DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA – SGSI–, PARA EMPRESAS DEL ÁREA TEXTIL EN LAS CIUDADES DE ITAGÜÍ, MEDELLÍN Y BOGOTÁ D.C. A TRAVÉS DE LA AUDITORÍA

ING. ALEXÁNDER GUZMÁN GARCÍA

Código: 1.030.548.291

ING. CARLOS ALBERTO TABORDA BEDOYA

Código: 98.639.837

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C. – COLOMBIA

ABRIL / 2015

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA – SGSI –, PARA EMPRESAS DEL ÁREA TEXTIL EN LAS CIUDADES DE ITAGÜÍ, MEDELLÍN Y BOGOTÁ D.C. A TRAVÉS DE LA AUDITORÍA

ING. ALEXÁNDER GUZMÁN GARCÍA

Código: 1.030.548.291

ING. CARLOS ALBERTO TABORDA BEDOYA

Código: 98.639.837

Trabajo de grado para optar el título de Especialización en Seguridad Informática

ING. FRANCISCO SOLARTE SOLARTE

Director del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ D.C. – COLOMBIA

ABRIL / 2015

CARTAS DE ACEPTACIÓN

CARTA ACEPTACIÓN Y ENTREGA TRABAJO DE GRADO

Bogotá, 21 de Marzo 2015

Señor(es)

COMITÉ DE TRABAJOS DE GRADO

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Universidad Nacional Abierta y a Distancia – UNAD –

Ciudad

Respetado(s) Comité de trabajos de Grado

Por medio de la presente, yo **Francisco Nicolás Javier Solarte Solarte**, Director del trabajo de grado titulado, **"DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA – SGSI –, PARA EMPRESAS DEL ÁREA TEXTIL EN LAS CIUDADES DE ITAGÜÍ, MEDELLÍN Y BOGOTÁ D.C. A TRAVÉS DE LA AUDITORÍA",** manifiesto mi conocimiento y **ACEPTACIÓN** del documento final del proyecto elaborado por los estudiantes **Alexander Guzmán García** y **Carlos Alberto Taborda Bedoya**, por tal motivo informo que dicho trabajo reúne los requisitos mínimos para la entrega a los jurados para las respectivas correcciones a que haya a lugar según su criterio en contenidos y forma, por consiguiente se hace entrega oficial del proyecto de grado al comité de trabajos de grado, para su respectiva verificación.

Cordialmente,

Francisco Solarte.

Ing. Francisco Solarte Solarte

C.C. 12989569 Pasto

Director del Proyecto

	FORMATO CONCEPTO ASESOR O JURADO	CODIGO: 7-PF-V-AC-004-009
	PROCEDIMIENTO RELACIONADO: TRABAJO DE GRADO	VERSION: 003-21-10-2009
		PAGINAS 1

Fecha: 19/04/2015	CEAD: José Acevedo y Gómez	Escuela: Escuela de Ciencias Básicas Tecnología e Ingeniería

DE: RAMSES RIOS LAMPARIELLO
PARA: Comité de Investigación Formativa

Asunto: Aval de proyecto para: Jurado ☐ Sustentación ☒ de Trabajo de Grado
periodo académico 2015

En cumplimiento de las funciones del Reglamento Académico **apruebo** ☒ **apruebo con correcciones** ☐ **rechazo** ☐ el proyecto "DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA – SGSI–, PARA EMPRESAS DEL ÁREA TEXTIL EN LAS CIUDADES DE ITAGÜÍ, MEDELLÍN Y BOGOTÁ D.C. A TRAVÉS DE LA AUDITORÍA", para ser presentado ante Jurado ☐ para Sustentación ☒.

Los integrantes del proyecto son:

PRIMER INTEGRANTE

Identificación		1.030.548.291	
Nombre Completo		ALEXÁNDER GUZMÁN GARCÍA	
Programa del que se graduará		Especialización en Seguridad Informática	
Celular	3214978252	Correo Electrónico:	alexander.guzman.garcia@gmail.com

SEGUNDO INTEGRANTE

Identificación		98.539.837	
Nombre Completo		CARLOS ALBERTO TABORDA BEDOYA	
Programa del que se graduará		Especialización en Seguridad Informática	
Celular	3046559734	Correo Electrónico:	taborda_carlos@hotmail.com

Atentamente,

Asesor

Jurado

Asegúrese de estar utilizando la versión actualizada de este formato. Consúltelo en: http://calidad.unad.edu.co

	FORMATO CONCEPTO ASESOR O JURADO	CODIGO: FP-VAC-004-003
	PROCEDIMIENTO RELACIONADO: TRABAJO DE GRADO	VERSION: 000-21-10-2009
		PAGINAS 1

Fecha: Popayán, 22 de Abril de 2015 **CEAD:** Popayán. **Escuela:** Ciencias Básicas Tecnología e Ingeniería.

DE: ELEONORA PALTA VELASCO
PARA: Comité de Investigación Formativa

Asunto: Aval de proyecto para: Jurado [ ] Sustentación [X] de Trabajo de Grado periodo académico 2015-I.

En cumplimiento de las funciones del Reglamento Académico **apruebo** [X] **apruebo con correcciones** [ ] **rechazo** [ ] el proyecto: "**DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA – SGSI–, PARA EMPRESAS DEL ÁREA TEXTIL EN LAS CIUDADES DE ITAGÜÍ, MEDELLÍN Y BOGOTÁ D.C. A TRAVÉS DE LA AUDITORÍA**", para ser presentado ante Jurado [ ] para Sustentación [X]

Los integrantes del proyecto son:

PRIMER INTEGRANTE

Identificación	1.030.548.291
Nombre Completo	ALEXÁNDER GUZMÁN GARCÍA
Programa del que se graduará	Especialización en Seguridad Informática
Celular 3214979252	Correo Electrónico: alexanderguzman.garcia@gmail.com

SEGUNDO INTEGRANTE

Identificación	98.639.837
Nombre Completo	CARLOS ALBERTO TABORDA BEDOYA
Programa del que se graduará	Especialización en Seguridad Informática
Celular 3046559734	Correo Electrónico: taborda_carlos@hotmail.com

Atentamente,

Francisco Solarte
Asesor

Eleonora Palta Velasco
Jurado

DEDICATORIA

Este proyecto de grado lo quiero dedicar:

A Dios, que es mi guía en todo momento, siempre está a mi lado guiándome por el camino de la vida, fortaleciendo cada uno de mis pasos día a día para salir adelante.

A mi Mamá Julia García Viatela, por brindarme en todo momento el apoyo que necesito para salir adelante y esos valores que me hacen único en mi forma de ser.

A mi Papá Álvaro Guzmán Vargas, por darme esa fuerza, esa sabiduría para afrontar los problemas, enseñándome las diferentes perspectivas de la vida.

A mi Hermana Julie Andrea Guzmán García, que siempre me apoya y ayuda en todo los momentos de mi vida.

A mis Abuelos y Abuelas, por darme esa fuerza para tomar decisiones.

A la Mujer que inspira mi vida con solo mirarla a sus hermosos ojos Martha Isabel Culma Soacha.

A Sofía, la niña más hermosa, dulce y tierna que con su sonrisa irradia felicidad.

A mis Familiares, por su apoyo incondicional.

Abril de 2015

A mis Maestros, por sus extraordinarios conocimientos sobre los temas explicados.

A mis Amigos, por sus enseñanzas y aportes profesionales.

A la Universidad Nacional Abierta y a Distancia – UNAD, Escuela de Ciencias Básicas Tecnología e Ingeniería, Especialización en Seguridad Informática, por permitirme desarrollar mis conocimientos.

A los Ingenieros Francisco Solarte Solarte, Eleonora Palta y Ramsés Ríos Lampariello, por su respaldo, apoyo, guía y orientación en el desarrollo del proyecto de grado.

Al Director Nacional, por todo el apoyo y colaboración en el desarrollo y culminación del proyecto de grado.

Al Comité proyectos de grado y sus colaboradores, por sus aportes de conocimiento y tiempo.

Alexánder Guzmán García

Abril de 2015

Este proyecto de grado lo quiero dedicar:

A mi esposa Silvia Marcela Oyuela Cano, quien es mi inspiración y apoyo constante, que con su paciencia, comprensión y dedicación, me ayuda cada día a lograr mis objetivos.

A mi hijo Juan David Taborda Palacio, que lo es todo para mí, y que aunque se encuentre distante sabe que está siempre en mi corazón y que todo lo que hago es para darle el mejor ejemplo y brindarle lo mejor de mí en todo momento.

A mis padres Rosalba Bedoya y Rafael Taborda (fallecido), que en medio de su humildad me brindaron la mejor enseñanza, y con lo poco que tenían me dieron el impulso para ir cada vez más allá.

A mis hermanos y hermanas, que siempre han estado presentes con su apoyo y aliento constante para que cada día pueda superar cada reto que me proponga.

A mis demás familiares y amigos, que son constantes ejemplo y apoyo para que no claudique en mis propósitos.

A todas aquellas personas y entidades que con su empeño, paciencia, dedicación, esfuerzo y compromiso, me han brindado las mejores herramientas para ir paso a paso avanzando en el camino del conocimiento.

Carlos Alberto Taborda Bedoya

Abril de 2015

AGRADECIMIENTOS

Agradezco a Dios por haberme permitido llegar a estos momentos tan maravillosos de mi vida, llenándome de salud, amor, paz y sabiduría para afrontar todos los retos de la vida.

Agradezco a mis padres: Julia García Viatela y Álvaro Guzmán Vargas por darme la vida, por brindarme en todo momento ese apoyo tan incondicional en mis decisiones y en mi crecimiento como profesional.

Agradezco a mi hermana: Julie Andrea Guzmán García por escucharme, apoyarme y estar siempre a mi lado en los momentos difíciles.

Agradezco a mi novia: Martha Isabel Culma Soacha y a su hija: Laura Sofía por apoyarme y brindarme la mano en los momentos difíciles, por llenarme de felicidad en instantes transcendentales de mi vida y por impulsarme a ser mejor cada día.

Agradezco a mis abuelos y abuelas maternas y paternas por mostrarme lo maravilloso que es la vida y lo importante que es dar paso a paso con firmeza.

Agradezco a mis familiares por sus enseñanzas y experiencias de la vida, por estar siempre pendiente participando directa o indirectamente de mis logros.

Agradezco a mis maestros por enriquecer con sus conocimientos mi aprendizaje intelectual hacia un enfoque profesional.

Abril de 2015

Agradezco a mis amigos por manifestar su apoyo y felicidad al estar culminando una etapa de mi vida tan importante, por apoyarnos en nuestra formación profesional.

Agradezco a la Universidad Nacional Abierta y a Distancia, Especialización en Seguridad Informática por permitirme desarrollar los conocimientos necesarios para desplegar la capacidad de diseñar, analizar, implementar, planificar y administrar un sistema de gestión de la seguridad informática, conforme a su infraestructura organizacional.

Expreso mis agradecimientos al ingeniero Francisco Solarte Solarte, Director del proyecto de grado, por su respaldo y orientación en la realización de la auditoría y diseño del sistema de gestión de la seguridad informática, también reitero mis agradecimientos al Comité trabajos de grado, al ingeniero José Miguel Herrán Suarez, a los jurados del proyecto Eleonora Palta y Ramsés Ríos Lampariello como a todos sus colaboradores que hicieron sus aportes de conocimiento y tiempo en el desarrollo del proyecto de grado.

Alexánder Guzmán García

Abril de 2015

AGRADECIMIENTOS

En primer lugar quiero reconocer y agradecer a todas aquellas personas, que durante mi vida me han brindado todo su conocimiento y apoyo, en los salones de clase y fuera de ellos, para que pueda cumplir con cada una de mis metas y estar en el lugar que estoy, si ellos esto no pudiese ser posible.

A Dios por permitirme tener la sabiduría y entendimiento para tomar el mejor camino para direccionar mi vida.

A mi esposa Silvia Marcela Oyuela Cano, quien día a día debe soportar largos momentos de ausencia, para yo poder cumplir con compromisos como mi educación.

A mi hijo Juan David Taborda Palacio, por comprender cuando está a mi lado, que todo el tiempo no se lo puedo dedicar a él, y a su vez entender que todo este esfuerzo es por ambos.

A mis padres Rosalba Bedoya y Rafael Taborda (fallecido), que siempre me llenaron de valores, que me permitieran ser una persona con principios y con objetivos claros en la vida.

A mis hermanos y hermanas, que con su apoyo y cariño, han logrado que me comprometa a ser ejemplo para todos y ser inspiración de nuestras siguientes generaciones.

Abril de 2015

A mis demás familiares y amigos, porque siempre han estado cuando los he necesitado.

A mi compañero de cursos y de trabajo de grado Alexander Guzmán García, que con su esfuerzo y compromiso en cada tarea que nos trazamos, hemos logrado realizar y culminar actividades de calidad para cumplir con lo solicitado en cada una de ellas.

Al ingeniero Francisco Solarte Solarte, que con su experiencia, conocimiento, y dedicación nos ha brindado la mejor de las asesorías para realizar un trabajo enmarcado en las normas y directrices requeridas para su presentación.

Por ultimo a la UNAD, que con el programa de Especialización en Seguridad Informática, me permite lograr un objetivo más en mi etapa cognitiva, y a todos los docentes de la especialización que me impartieron sus experiencias y saberes para apropiarme de ellos.

Carlos Alberto Taborda Bedoya

Abril de 2015

TABLA DE CONTENIDO

LISTAS ESPECIALES

Índice de tablas

Índice de figuras

Índice de ilustraciones

GLOSARIO

ACTIVIDADES: Conjunto de acciones, las cuales permiten desarrollar y cumplir una meta, a partir de un programa implementado o metodología de ejecución, poniendo en marcha cada uno de los procesos o tareas asignadas a cada colaborador.

AMENAZAS INFORMÁTICAS: Vulnerabilidades que se pueden presentar en un sistema de información, donde una mala configuración y un mal funcionamiento del sistema de control pueden denegar o no detectar las causas potenciales que pueden afectar la infraestructura.

AUDITOR: Es un grupo de personas naturales, jurídicas y/o personas independientes para evaluar los procesos de una empresa y un área específica a través de las listas de chequeo y monitoreo continuo.

AUDITORÍA: Proceso para evaluar cada una de las actividades y metodologías al interior de una organización, empresa, Pymes, etc., realizando una intervención de forma crítica, constructiva y sistemática en pro de la mejora de los procedimientos al interior del área examinada.

BASES DE DATOS: Conjunto de datos relacionados entre sí, con la misma estructura para ser utilizados, almacenados e indexados de forma sistemática para su posterior consulta estructurada y de acceso rápido.

BITS: Es el acrónimo Binary digit, para determinar el digito que inicia la numeración en los sistemas operativos binarios, por consiguiente puede representar un estado de (0 – 1).

BUGS: Fallas del sistema o errores del software

CALIDAD: Término que proviene del latín, la cual se encuentra asociada a cada uno de los conceptos o perspectivas de cada necesidad dentro de un mundo globalizado y puntual, comparando con otro componente.

CHECKLIST: Herramienta de apoyo en la verificación de cada uno de las metodologías, actividades y procedimientos que se deben llevar a cabo en el área, dirección, departamento u oficina evaluada, con el propósito de realizar una verificación objetiva sobre cada proceso.

CONFIDENCIALIDAD INFORMÁTICA: Medidas y herramientas que permiten a los sistemas de información, evitar el acceso de personas no autorizadas, con el fin de custodiar la información contenida en sus bases de datos.

DATOS: Representación metodológica de un conjunto de atributos, sucesos, hechos y variables para ser procesada, y así obtener la información requerida o solicitada conforme a las necesidades.

DIAGRAMA: (Del latín diagrama, diseño). Los diagramas son la representación de datos a través de una imagen, donde se muestra las relaciones existentes del sistema.

DISPONIBILIDAD INFORMÁTICA: La disponibilidad informáticas es la técnica para que los sistemas de información se puedan recuperar de fallos tecnológicos, con el propósito de mantener el acceso a las funcionalidades en la gran mayoría del tiempo.

ESTÁNDARES: Criterios, actividades y procesos claros, para establecer niveles de complejidad en cada uno de los procedimientos a implementar dentro de una organización o empresa puntual.

ESTRUCTURA SGSI: Metodología para implementar por medio de fases y pasos definidos como se puede construir un sistema de gestión de la seguridad de la informática.

FICHERO INFORMÁTICO: Está constituido por la agrupación de bits, los cuales almacenar información en los dispositivos para crear un archivo legible, por lo tanto cada archivo se identifica conforme a las características con la cual fue creado para proporcionar datos o información en otros momentos de tiempo.

GESTIÓN DE INCIDENTES: Conjunto de procesos con el fin de gestionar cada uno de los incidentes hallados, para recuperar el sistema y minimizar el impacto negativo en las empresas.

INTEGRIDAD INFORMÁTICA: Medidas y herramientas que permiten asegurar la procedencia de la información o datos, los cuales se identifican como datos seguros por que no se ha producido ninguna modificación o cambio desde su emisión y es exactamente igual al dato o información original.

ISO/IEC 27000: Estándares de seguridad, informados por la ISO - Organización Internacional para la Estandarización y la IEC - Comisión Electrotécnica Internacional, con el fin de estableces procedimientos claros frente a las actividades propuestas.

MODELOS INFORMÁTICOS: Los modelos informáticos proveen estrategias de gestión para el mejoramiento de los procesos, procedimientos y actividades al interior de una organización, promoviendo las soluciones informáticas.

NORMAS: Conjunto de elementos constituidos por reglas y pautas con el fin de ser ajustadas a un protocolo o procedimiento establecido por las organizaciones internacionales que lo rigen, estableciendo un orden de valores los cuales proporcionan una regulación entre los diversos comportamientos y estados que se pueden presentar dentro de una organización.

PROCEDIMIENTOS: "Según la definición de la Real Academia Española, el significado de esta palabra refiere a la acción y efecto de proceder. Este concepto se define como un método o sistema estructurado para ejecutar algunas cosas"[1]. "Es un conjunto de acciones u operaciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias"[2].

PROCESOS: Conjunto de fases sucesivas que se identifican a través de un diagrama de flujo, el cual permite la las operaciones lógicas a través de un protocolo establecido dentro de una organización.

PYMES: Medianas y pequeñas empresas que representan cierta cantidad de trabajadores en un sector específico, los cuales se encuentran registrados en el IMSS, desde sus características con los negocios que proporcionan alguna actividad económico dentro de un país pero que por su condición y constitución son locales pequeños.

RIESGOS: Término que proviene del italiano, adoptado de una palabra árabe, la cual representa el potencial de perjuicios que se pueden presentar en una organización, por la falta de una estrategia de seguridad, asociándose al peligro o daño de un acontecimiento, a través de la probabilidad de ocurrencia dentro de un instante de tiempo.

SGSI: Sistema de gestión de la seguridad informática.

TI: Tecnologías de la información

VULNERABILIDADES INFORMÁTICAS: Debilidad de un sistema, el cual permite a un hacker ingresar a un computador violentando la confidencialidad, integridad, disponibilidad de los datos y aplicaciones[3].

---

[1]QUEES.LA. *¿Qué es procedimiento?.* [en línea]. [09 de mayo del 2014]. Disponible en: http://quees.la/procedimiento/

[2]Ibíd., p. 1.

[3]ALEGSA. Definición de vulnerabilidad. [en línea]. [15 de mayo del 2014]. Disponible en: http://www.alegsa.com.ar/Dic/vulnerabilidad.php

RESUMEN

La presente investigación, desarrollara un sistema de gestión de la seguridad informática (SGSI) para empresas del sector textil de las Pymes en las ciudades de Medellín, Bogotá D.C. he Itagüí (Colombia): el diseño se elaborará basados en la norma ISO 27001, la cual provee prácticas apropiadas para el desarrollo e implementación de cada uno de sus componentes, estableciendo las fases, documentación y procedimientos requeridos y exigidos en el estándar para continuar con el diseño y ejecución del SGSI de manera adecuada.

En consecuencia, se debe realizar un análisis cualitativo y cuantitativo de los riesgos, vulnerabilidades y amenazas que se presentan en una Pyme, las cuales al poseer recursos económicos limitados para inversiones de este tipo, no pueden implementar un sistema de seguridad robusto, razón por la cual se debe implementar un mecanismo que satisfaga las necesidades de las pequeñas empresas, en el cual cada uno de los componentes informáticos juega un papel importante para la permanencia en el mercado de éstas.

Asimismo, se podrá salvaguardar el recurso más importante de la Pymes (datos – información), donde el diseño de un SGSI podrá proporcionar una metodología sencilla y muy completa para proteger cada uno de los activos informáticos y así establecer procesos de restauración y mitigación de riesgos, tomando las medidas correctivas y preventivas que sean necesarias.

Finalmente, cuando se establece un sistema de seguridad de la información, se logra detallar cada uno de los componentes y elementos que se encuentran asociados a la Pyme y así tener un mayor control sobre cada uno de los activos informáticos, por consiguiente durante la permanencia en el tiempo, podrá adaptarse a las necesidades de las pequeñas empresas, donde el ciclo de Deming, detalla el proceso de mejora continua proporcionando una realimentación constante de cada uno de los procesos.

Palabras claves

SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA, ISO 27001, PYME, VULNERABILIDADES INFORMÁTICAS, RIESGOS INFORMÁTICOS, AMENAZAS INFORMÁTICAS, CIBERDELINCUENTES, ESTÁNDARES DE SEGURIDAD, NORMAS, DISEÑO.

Abril de 2015

ABSTRACT

The current investigation will development a computer Security Management system (CSMS) for the companies in the textile sector of the PYMES in the city of Medellín, Bogota D.C and Itagüí (Colombia): The design is going to be based on ISO 27001, which provides appropriate practices for the development Implementing of every single component, establishing phases, documentation and all the required procedures and standards exacted to continue with (CSMS) design and implementation in the right way.

As a result, there should be a more qualitative analysis and quantitative risk assessment, susceptibility and threats on the posed in an PYME which by possessing limited financial resources for this type of investments, cannot implement a safety system robust, for that reason should be implement a mechanism to fulfill the small enterprise's need enterprises, where each solfware's component plays an important role in order to remain in the market of them.

Also, I'll safeguard the most important resource of the PYME (Data-Information) where the design of a (CSMS) will provide simple methodology and pretty complete to protect each one of software assets and this way develop process of restoration and mitigation of risks, taking the necessary corrective and preventive measures needed.

Finally, when establishes a security system information, reaches the detail of each one of the components and elements that are associated with PYME and take a greater control about in each one of software assets, Therefore during the lifetime, it will adapt to the needs of small companies in particular, in which the Deming cycle, detail the constant improvement process of the system, providing constant feedback from each of the processes.

Keywords

The safety management software system, ISO 27001, PYME, software vulnerabilities, IT risks or software risks, informatics threats, cybercriminals, safety standards, norms and design.

1. INTRODUCCIÓN

La seguridad informática es un mecanismo de control, el cual entre varias tareas, sirve para identificar cuáles son los usuarios que pueden hacer uso de la infraestructura tecnológica, los recursos informáticos, y la información de una organización, con el fin de hallar las vulnerabilidades, amenazas y riesgos que enfrenta una empresa en relación a los tres aspectos que enmarcan la seguridad de la información, y que hacen referencia a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y la información.

Actualmente, las empresas manejan una gran cantidad de información a través de diversos medios electrónicos, físicos, digitales y magnéticos, entre otros, que pueden ser susceptibles a ser interceptados o vulnerados, si no se posee un sistema de gestión de la seguridad informática y de la información SGSI que permite implementar políticas, técnicas, métodos, procesos y procedimientos de control bien definidos que contrarresten esas deficiencias de seguridad.

Es por eso que las empresas y su estructura organizacional, deben definir áreas responsables para la implementación y cuidado de la información que se almacena diariamente en los servidores o equipos de cómputo, y que permita evidenciar las vulnerabilidades, amenazas y riesgos de seguridad aplicando metodologías, pruebas y procedimientos de control que permitan mitigar esos riesgos.

En este sentido, el proyecto pretende hacer un diagnóstico del estado de la seguridad de la información en las Pymes del sector textil de las ciudades de Medellín, Itagüí y Bogotá, mediante procesos de auditoría que permita identificar las vulnerabilidades, amenazas y riesgos de seguridad informática y de la información, para proponer un SGSI de la información que pueda ser aplicado en cada una de ellas para mitigar los problemas de seguridad encontrados.

Para el proceso de auditoría se pretende realizar pruebas de seguridad informática, haciendo uso de los procesos especializados que permita identificar aquellos riesgos potenciales que se pueden presentar en los sistemas de información de las Pymes, de esta manera se establecerá por medio de las guías, metodologías y estándares de seguridad las mejores prácticas para implementar controles de seguridad, siguiendo a través de la mejora continua (ciclo PHVA) la retroalimentación de cada una de sus fases.

2. PLANTEAMIENTO DEL PROBLEMA

2.1. Descripción del problema

Al interior de las Pymes y de una manera generalizada, se detecta un alto grado de perdida y/o alteración de información propia del negocio, que en muchos casos es vital para el buen funcionamiento de la empresa.

La fuga de información se presenta debido a la falta de controles de acceso, para que los usuarios ingresen solo a los datos que deban acceder, motivo por el cual los competidores utilizan personal manipulado para sustraer información.

El borrado o destrucción de los datos se da por no contar con políticas para el manejo de dispositivos de almacenamiento externos, sistemas firewall y antivirus adecuados y actualizados, restricciones de navegación en internet y en general una infraestructura de protección acorde a las necesidades de hoy.

El daño a los sistemas hardware y software que interactúan con la información de la empresa, se presenta por pensar en una gestión de reparar y no en mantener los sistemas.

Un problema común es la falta o inadecuada gestión de la red, presentándose interceptación de datos cuando estos son transferidos por la misma este problema se presenta debido a la mala contratación de personal de sistemas, involucrando técnicos faltos de conocimientos en temas de seguridad en redes y en sistemas de información.

En la actualidad los sistemas informáticos se han convertido en uno de los activos más importantes para almacenar los datos relevantes de las empresas, Pymes y/u organizaciones, por lo tanto con las dinámicas y medios de almacenamiento para salvaguardar la información; se implementan métodos de seguridad para proteger cada uno de los datos confidenciales. Donde para algunas Pymes y/o empresas pequeñas se detecta un alto grado de pérdida, fuga y/o alteración de información computacional, debido a que los sistemas de cómputo no poseen protocolos y medidas de seguridad apropiadas para detectar a tiempo algunas vulnerabilidades, amenazas o riesgos informáticos que afectan la integridad, confidencialidad y disponibilidad de los datos.

Sin embargo proteger la información se ha convertido en uno de los aspectos más relevantes en los procesos para mitigar el riesgo informático, el cual es un suceso o acontecimiento relacionado con las condiciones cambiantes del ambiente por una serie de circunstancias que afectan los bienes o servicios informáticos, como equipos informáticos, periféricos, instalaciones, software, redes, etc.

Asimismo se tiene las vulnerabilidades informáticas, que son las debilidades de los sistemas, en el cual los atacantes como hackers pueden manipular la disponibilidad, integridad, confidencialidad y acceso a toda la información que se almacena en los equipos de cómputo, los cuales se pueden presentar como bugs o fallas de la arquitectura en el diseño de un sistema informático.

En consecuencia se puede encontrar las amenazas informáticas, las cuales son la eventualidad de que una acción puede producir un daño sobre los elementos periféricos de un sistema, causados por códigos maliciosos o desconocimiento humano de los diferentes ataques informáticos, como lo es la ingeniería social, entre otros tipos de amenazas permitiendo el acceso de hackers; dichas amenazas se pueden presentar de manera interna o externa.

Por consiguiente las amenazas, riesgos y vulnerabilidades informáticas, generan grandes costos y daños en los equipos de cómputo en su hardware y software para restablecer los sistemas de información, debido a que las Pymes no invierten en el capital humano para prevenir la perdida de información confidencial, por lo tanto se debe garantizar un flujo de protección de datos a través del diseño de un SGSI (Sistema de Gestión de la Seguridad Informática) que permita mejorar la seguridad informática en cuanto a las vulnerabilidades, amenazas y riesgos detectados por medio de la auditoría para controlar cada uno de los acontecimientos probables.

2.2. Formulación del problema

¿Cómo el diagnóstico de la seguridad de la información mediante procesos de auditoría permitirá mejorar la seguridad informática y la protección de la información en las Pymes del sector textil en la ciudad Medellín, Itagüí y Bogotá?

3. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Este proyecto abarca el diseño de un sistema de gestión de la seguridad informática (SGSI) para las Pymes del sector textil en Medellín, Itagüí y Bogotá, con el propósito de encaminar las buenas prácticas que proporciona la auditoría, la norma ISO 27000, más concretamente en los estándares ISO/IEC 27001, ISO/IEC 27002 y ISO/IEC 27005.

El diseño de un SGSI para las Pymes, se realizará basados en el uso de técnicas de auditoría con la aplicación de instrumentos de recolección de información en la ciudad de Bogotá D.C. y el municipio de Itagüí frente a las vulnerabilidades, amenazas y riesgos existentes en la seguridad de los activos y la información.

Con estas técnicas se pretende evaluar en las Pymes, la implementación existente de infraestructura física y lógica destinada a la protección de los activos de información, de los recursos humanos, de la infraestructura física de la compañía, del ambiente, de la transferencia de información, de las políticas de seguridad de la información, de los métodos de contratación para los sistemas informáticos, y del cumplimiento de la normativa para el aseguramiento, control y mantenimiento de los sistemas.

Asimismo el proyecto se desarrollará en el segundo semestre del año 2014 y el primer semestre del año 2015.

4. JUSTIFICACIÓN DEL PROYECTO

La seguridad informática es un aspecto importante dentro de las organizaciones y en las Pymes para tener en cuenta, ya que a partir de los procesos y procedimientos especializados se logra salvaguardar los datos a través de un Sistema de Gestión de la Seguridad Informática (SGSI), el cual permite mantener protegido los registros confidenciales de manera eficiente, gestionando un mecanismo que mantenga la confidencialidad, integridad y disponibilidad de la información dentro de los parámetros de seguridad que permite la ley, con el fin de lograr la permanencia en el tiempo y en un mundo globalizado y competitivo.

Las Pymes representan un porcentaje alto en el aporte al sistema económico de Colombia, por ende estas empresas aportan al crecimiento económico por su emprendimiento y desarrollo; abriendo puertas a diversas oportunidades, exportando nuevos productos, implementando tecnología, generando nuevos conocimientos y avances en diferentes entornos, para el progreso de la sociedad.

Por lo tanto, como son sociedades que están iniciando en sus procesos productivos y asentamiento, no conocen o no suelen invertir mucho sobre los temas de seguridad para sus sistemas de información, dejando vulnerable sus datos y sus procesos, sin tener en cuenta la importancia que es proteger la información de los equipos de cómputo.

De allí que algunas Pymes presenten falencias en su modelo informático y la forma como disponen la información a los usuarios, generando perdida de información, accesos no autorizados a datos confidenciales y alteración de información, por consiguiente se ve necesario un diseño de un SGSI, el cual tendrían la oportunidad de adoptar procesos basados en metodologías, normas y estándares internacionales de seguridad que les permitan mejorar la forma como se almacena, protege y dispone los datos dentro de las Pymes, lo cual implementa una barrera de protección ante los posibles ataques informáticos, mitigando las vulnerabilidades, amenazas y riesgos asociados al desconocimiento de metodologías robustas para no caer en una mala administración de los sistemas de información y canales de comunicación que se derivan en pérdidas importantes de información o re-procesos constantes.

Para tal efecto el diseño de un SGSI permite y proporciona ventajas claras sobre las necesidades en diferentes entornos, que a su vez reflejan un beneficio para las Pymes, por lo cual dichas ventajas pueden ser:

- Cambiar de una posición reactiva a una preventiva y proactiva ante la seguridad de la información.
- Disponer de verdaderas políticas y objetivos para darle tratamiento a la seguridad de la información en la empresa.
- Asignación real y formal de responsabilidades y funciones al personal involucrado en la seguridad.
- Se adecua la gestión de la seguridad, acorde a los riesgos presentes para la actividad.
- Permite aplicar los controles adecuados.
- Permite optimizar costos vinculados a la búsqueda constante de la seguridad.
- Salir al paso de los delincuentes y poder estar blindados ante sus actividades delictivas.
- Permite una mayor confianza de los clientes
- Tener una estructura estandarizada y aplicada de acuerdo a normas internacionales.

Como resultado el beneficio que trae el diseño de un SGSI, permitirá la implementación de elementos básicos para la seguridad informática en la Pymes del sector textil de Medellín, Itagüí y Bogotá D.C., generando confianza entre los usuarios internos y externos que sitúan la oportunidad de ofrecer un mejor producto, un mejor servicio, una mejor cobertura, unos mejores precios, etc., permitiendo ser más competitivos en el mercado, además de mantener protegido los datos del negocio, sus clientes, empleados y empleadores, proyectando y manteniendo una imagen en la cual ofrece garantías por que se compromete con ellos y con su información.

5. OBJETIVOS

5.1. Objetivo General

Diseñar un SGSI que mejore la seguridad informática y la protección de la información, basados en procesos de auditoría que permitan hacer un diagnóstico de la situación actual que enfrentan las Pymes del sector textil en Medellín, Itagüí y Bogotá D.C.

5.2. Objetivos Específicos.

- Recolectar información sobre las vulnerabilidades, amenazas y riesgos en la seguridad informática y de la información que permitan conocer el estado actual de la seguridad en las Pymes del sector textil en Medellín, Itagüí y Bogotá D.C.

- Diseñar instrumentos de recolección de información y un plan de pruebas que permitan hacer un diagnóstico de la seguridad de la información en las empresas del sector textil de Medellín, Itagüí y Bogotá D.C.

- Ejecutar las pruebas y aplicar los instrumentos diseñados para evidenciar la existencia de las vulnerabilidades, amenazas y fallas existentes tratando de buscar las posibles causas que los originan.

- Establecer controles, planes de mejoramiento y diseñar el SGSI que permita mitigar las causas que originan los riesgos de seguridad que se presentan en las Pymes de Bogotá e Itagüí

6. MARCO REFERENCIAL

6.1. Antecedentes

Para enfocar la investigación sobre el diseño de un sistema de gestión de la seguridad informática, se tomaron los siguientes proyectos a nivel nacional e internacional, con el propósito de identificar los avances y los hallazgos encontrados:

- En primer lugar se tiene, en febrero de 2013 fue presentado en la Facultad de Ingenierías de la Universidad Tecnológica de Pereira, el trabajo especial de grado: Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda, por Aguirre Cardona Juan David y Aristizabal Betancourt Catalina, como requisito para optar el título de Ingenieros de Sistemas y Computación.

  La investigación trata de diseñar un SGSI para el grupo empresarial la ofrenda, y busca generar una herramienta que le permita a esta mejorar los niveles de seguridad de sus activos de información y posteriormente lograr la certificación correspondiente a la seguridad de la información.

  Este trabajo aporta experiencias en el diseño de un SGSI para el proyecto que se está realizando, con elementos funcionales que permiten tener un mejor panorama acerca de este tipo de investigación.

- Igualmente en 2013 en su mes de febrero, es presentado en la Facultad de Ciencias e Ingeniería de la Pontificia Universidad Católica del Perú, el trabajo de grado: Diseño de un sistema de gestión de seguridad de información para un instituto educativo, por Aliaga Flores Luis Carlos, como requisito para optar el título de Ingeniero Informático. El proyecto presenta el diseño de un SGSI, que permita gestionar la seguridad de los activos de información que intervienen en diferentes procesos en las instituciones educativas de nivel superior.

Este proyecto sirve como guía para evidenciar la manera de afrontar las diferentes etapas del diseño de un SGSI, las técnicas utilizadas para la identificación de vulnerabilidades y riesgos, y la manera de definir controles a los diferentes hallazgos.

- En diciembre de 2009, es presentado en la Universidad Politécnica Salesiana de Ecuador en la Facultad de Ingenierías, el proyecto como trabajo de grado: Planeación y Diseño de un Sistema de Gestión de Seguridad de la información, basado en la norma ISO/IEC 27001 - 27002, por Buenaño Quintana José Luis y Granda Luces Marcelo Alfonso, para optar al título de Ingenieros de Sistemas.

  Dicho proyecto enmarca el diseño de un SGSI, basándose en la norma ISO 27000, en sus estándares 27001 y 27002, y enfocándolo a las necesidades directas de la misma Universidad en la que estudiaban, describen todas las etapas realizadas desde la necesidad puntual de tener un sistema que mejore la seguridad de la información, hasta los controles aplicables a los riesgos y vulnerabilidades hallados.

  Es un aporte que permite indagar y adentrarse en el manejo y la aplicabilidad de la norma ISO 27001 y 27002, como base del diseño de un SGSI, con todas sus recomendaciones y buenas prácticas, para obtener a través de los análisis, el más adecuado resultado con información de los riesgos encontrados y los controles que se pueden aplicar a estos.

6.2. Marco contextual

Las Pymes que se enfocan en procesos textiles como confecciones, están muy sectorizadas en la ciudad de Bogotá y el municipio de Itagüí, estas empresas se dedican al diseño, corte y fabricación de prendas de vestir masculinas y femeninas, con una alta gama de artículos que permiten cubrir las necesidades del mercado local, e incluso de algunos países de la región y de otros continentes.

En el aspecto tecnológico, es muy generalizado el manejo de equipos de cómputo para actividades de diseño, administración de información del personal, calidad, contabilidad y la información correspondiente a clientes y proveedores.

Es notable la ausencia de tecnologías o infraestructura que permita tener copias de seguridad o equipos destinados para mantener la información resguardada de una forma más segura, tampoco se manejan sistemas de contingencia contra caídas de energía, o desastres naturales.

Algunas cuentan con servicios informáticos contratados con personal poco apto en conocimientos informáticos seguros y profesionales, los cuales no cuentan con los procedimientos adecuados para el manejo apropiado de la información y los sistemas.

6.3. Marco Teórico

En la actualidad la información se ha convertido en el activo más valioso de las empresas, es por esto que las empresas deben implementar estrategias, no solo a nivel lógico, como la protección de las bases de datos y archivos de gestión, si no que se debe complementar con la contratación de personal calificado, con alto grado de pertenencia institucional y ética profesional.

6.3.1. Vulnerabilidad informática

Son las posibilidades del mismo ambiente, en el cual las características propician y se vuelve susceptible a una potencial amenaza, por lo tanto se puede considerar como la capacidad de reaccionar ante la presencia de una amenaza o un daño.

Se es vulnerable a cualquier evento, sin importar su naturaleza, sea esta interna o externa, pero aplicando los controles adecuados es posible minimizar las posibilidades de que estas se materialicen, por lo tanto los tipos de vulnerabilidades son:

6.3.1.1. Vulnerabilidad Física

Es la vulnerabilidad del entorno físico del sistema de información, equipos de cómputo y servidores, debido a que algún hacker ha violentado el acceso a la información de manera persuasiva para robar, modificar o eliminar información confidencial.

6.3.1.2. Vulnerabilidad Natural

Las vulnerabilidades naturales, son las ocasionadas por los desastres o eventos fortuitos en el medio ambiente, el cual ocasiona daños en los sistemas de cómputo por medio de los picos eléctricos, inundaciones, terremotos, temperatura alta y todos aquellos desastres naturales que son ocasionados por las variaciones atmosféricas y rozamiento de las placas tectónicas.

6.3.1.3. Vulnerabilidad del Hardware y del software

6.3.1.3.1. Hardware

Las vulnerabilidades de hardware, hace referencia a las probabilidades de que las piezas físicas y/o dispositivos presenten fallas por descuido, mal uso o por que se ha dejado desprotegido los equipos de cómputo sin la seguridad adecuada para su manipulación.

6.3.1.3.2. Software

Las vulnerabilidades de software son conocidas como bugs del sistema o errores del software, el cual permite acceder a la funcionalidad y aplicación sin mayor esfuerzo por parte del hacker, ya que conoce el código fuente, tiene un mal diseño el software, o ha encontrado una puerta trasera para adherirse y conseguir información.

6.3.1.4. Vulnerabilidad de los Medios o Dispositivos

Las vulnerabilidades de los dispositivos y medios, son los daños, robos y descuidos humanos que permiten a terceras personas apoderarse de los discos duros, impresoras, equipos de cómputo, memorias USB y demás medios extraíbles que no posean un medio de seguridad adecuado.

6.3.1.5. Vulnerabilidad de las Comunicaciones

Las vulnerabilidades de comunicación se encuentran asociadas a las redes y tipologías de conexión a través de diferentes puntos de red, esto quiere decir que si no se posee un método o herramienta que monitoree el tráfico de paquetes de datos por internet, los datos pueden ser capturados mientras el mensaje viaja por el internet.

6.3.1.6. Vulnerabilidad Humana

Las vulnerabilidades humanas radican en la falta de conocimiento sobre los métodos para proteger los datos y el acceso completo a las configuraciones del sistema informático, sin tener las restricciones adecuadas para identificar por medio de roles y usuarios el acceso conforme a la auditoría de cambio en el sistema de cómputo.

6.3.1.7 Vulnerabilidad Económica

Las vulnerabilidades económicas se enmarcan en la falta de recursos económicos, que permitan la adecuada inversión en sistemas, metodologías y demás elementos físicos y lógicos, para garantizar que los activos de información puedan protegerse de la mejor manera posible.

6.3.2. Amenazas informáticas

Es la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial, sobre los sistemas de información, por lo tanto se puede clasificar en:

- Amenaza criminal: son aquellas acciones en las que intervienen seres humanos violando las normas y las leyes.
- Sucesos de origen físico: son los eventos naturales que se pueden presentar, o aquellos eventos en los que el ser humano propicia las condiciones para determinar un hecho físico.
- Negligencia: son las omisiones, decisiones o acciones que pueden presentar algunas personas por desconocimiento, falta de capacitación y/o abuso de autoridad porque tienen influencia sobre los sistemas de información, algunos porque no tienen ética para el desarrollo de la profesión.

Las amenazas a los sistemas de información están latentes cada que se interactúa con los mismos, desde la utilización de dispositivos de almacenamiento externos, hasta el ingreso a sitios web, o la inconformidad de empleados insatisfechos dentro de la misma compañía, por lo tanto los tipos de amenazas según el efecto causado en el sistema:

6.3.2.1. Intercepción

Es cuando un hacker o grupo de personas, logran ingresar a los sistemas de información sin autorización para escuchar, visualizar y copiar archivos confidenciales de las empresas, organizaciones y/o Pymes.

6.3.2.2. Modificación

Es cuando un hacker o grupo de personas, han logrado ingresar al sistema de información y además pueden modificar los archivos y/o líneas de código del software para ocasionar perdida de información, mal funcionamiento de los equipos de cómputo o programar cambios en los contenidos de las bases de datos.

6.3.2.3. Interrupción

La interrupción se da cuando los sistemas de información son saturados por medio de inyección SQL, código malicioso, virus, troyanos, gusanos y todas las aplicaciones que pueden ocasionar entorpecimiento en el sistema de información para un mal funcionamiento.

6.3.2.4. Generación

La generación de amenazas se da cuando se añade información en las bases de datos, registros y programas confidenciales, ocasionando daños internos y externos en los equipos de cómputo y prestación del servicio, ya que introduce mensajes no autorizados en cada uno de los comandos, registros y datos requeridos para un buen funcionamiento.

Por otro lado se tiene las amenazas según el punto de vista:

6.3.2.5. Amenazas Involuntarias

Las amenazas involuntarias son aquellas que se producen por desconocimiento sobre las medidas de seguridad mínimas que se deben tener al manipular cualquier tipo de información, asimismo los casos más comunes se encuentran en la eliminación de archivos básicos del sistema sin darse

cuenta, dejar la contraseña de acceso en lugares visibles o simplemente no bloquean el equipo cuando salen de la oficina o se desplazan a otro lugar por alguna razón.

6.3.2.6. Amenazas Naturales o Físicas

Las amenazas naturales son aquellas que se producen por los efectos naturales y cambios ambientales en el entorno, ocasionando un desastre tales como el polvo, las inundaciones, terremotos, etc.

6.3.2.7. Amenazas Intencionadas

Las amenazas intencionadas son aquellas en la cual un grupo de hackers o una sola persona quiere conocer, modificar, eliminar y/o robar información para sus fines personales, por lo tanto se puede clasificar en dos tipos:

6.3.2.7.1. Intencionadas internas

Las amenazas intencionadas internas, se dan por personas que en algún momento trabajaron en la empresa, Pyme u organización y se quieren vengar porque ya no tienen trabajo, o se encuentran descontento del trabajo o quieren su propio beneficio al sacar información confidencial.

6.3.2.7.2. Intencionadas externas

Las amenazas intencionadas externas, se dan cuando un grupo de hackers y/o hacker a través de los conocimientos informáticos, aprovecha las fallas del software o conexiones de red para ingresar al sistema de manera no autorizada para obtener la información requerida, o pueden ingresar a las oficinas sin ser detectados.

Dentro de este tipo de amenazas se pueden ver:

- La ingeniería social. Se presenta cuando el atacante se aprovecha del eslabón más débil de la cadena que representa la seguridad de la información(los usuarios), y con técnicas de engaño, donde a través del teléfono, o el correo electrónico se hace creer a la víctima que se es un compañero de trabajo, un empleado bancario, un administrador del sistema, entre otros, buscando obtener datos personales como usuarios y claves de diferentes sistemas de información de los cuales pueden obtener beneficios económicos o de otra índole.

- La ingeniería social inversa. En este caso, se da cuando una vez el atacante pone la trampa de ingeniería social, es el usuario quien busca la ayuda del atacante, el cual se ha ganado su confianza y aprovechará esta para sacar toda la información necesaria al usuario.

6.3.3. Riesgos informáticos

Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información u ordenadores, si no se poseen las medidas adecuadas para salvaguardar los datos, dichos riesgos informáticos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, por lo tanto los riesgos se pueden clasificar en:

6.3.3.1. Riesgos de integridad

Son aquellos que se relacionan con el acceso, autorización y procesamiento de las aplicaciones que integran los reportes de las organizaciones, aplicados en cada uno de sus sistemas de operaciones como por ejemplo:

- Interfaz del usuario
- Procesamiento, procesamiento de errores
- Interfaz
- Administración de cambios

- Información[4]

6.3.3.2. Riesgos de relación

Son aquellos que se relacionan con la toma de decisiones de manera oportuna a partir de la información recolectada y en momento preciso, integrada a través de las aplicaciones para tomar decisiones.

6.3.3.3. Riesgos de acceso

Son aquellos que por una inadecuada configuración del sistema, en el cual no se poseen las metodologías apropiadas para salvaguardar la integridad y confidencialidad de la información, los datos podrían estar expuestos y son vulnerables a cualquier hacker, dependiendo del nivel de estructura en el cual se encuentra la seguridad de la información, de los cuales se pueden mencionar:

- Procesos de negocio
- Aplicación
- Administración de la información
- Entorno de procesamiento
- Redes
- Nivel físico

6.3.3.4. Riesgos de utilidad

Los riesgos de utilidad se enfocan desde 3 sectores, en primer lugar se tienen los backups y/o planes de contingencia para la seguridad informática, en segundo lugar se tiene las técnica para recuperar el sistema cuando existen caídas de los sistemas operativos y en tercer lugar los procesos que acompañan las posibles problemáticas debido al entorno para mitigar o minimizar la ocurrencia del hecho (amenaza y/o vulnerabilidad informática).

[4] EBILIO UNAD. *Lección 11: Riesgos informáticos*. [en línea]. [12 de diciembre del 2014]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_11_riesgos_informticos.html

6.3.3.5. Riesgo de infraestructura

Son aquellos que no poseen una estructura tecnológica efectiva a la hora de enfrentar alguna eventualidad en sus sistemas de información, en el cual el software, hardware, personal, procesos, redes y canales de comunicación son los elementos que soportan las necesidades de operación, desarrollo, mantenimiento y procesamiento de la información de una organización, los cuales se deben determinar a partir de:

- Planeación organizacional
- Definición de las aplicaciones
- Administración de seguridad
- Operaciones de red y operaciones computacionales
- Administración de sistemas de bases de datos
- Información / Negocio
- Riesgos de seguridad general
- Riesgos de choque de eléctrico
- Riesgos de incendio
- Riesgos de niveles inadecuados de energía eléctrica
- Riesgos de radiaciones
- Riesgos mecánicos

6.3.4. Seguridad informática

La seguridad informática, es el área que se enfoca en las metodologías, proceso y procedimientos para mantener salvaguardada la información y datos confidenciales de una organización, Pyme y empresa al interior de las herramientas informáticas. Dichos procesos se estructuran a través de estándares, normas, protocolos y metodologías para mitigar y minimizar los riesgos asociados a la infraestructura tecnológica.

Por ende la seguridad informática es uno de los grandes retos a implementar, ya que no es posible implementarla en un 100%, por lo tanto la aplicación de metodologías, infraestructura y estándares adecuados, permiten obtener un mayor grado de seguridad para cualquier compañía, mitigando algunos errores que se pueden prever.

6.3.5. Seguridad de la información

La seguridad de la información es un agregado de medidas preventivas, con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad, en este sentido la información se puede presentar en diferentes características; no solamente en los medios electrónicos, sino también en los medios físicos. En consecuencia la información se ha convertido en el activo más valioso para las compañías, donde se ejecutan metodologías para proteger los registros y mantener una infraestructura adecuada para la custodia y salvaguardar la información, por consiguiente la seguridad de la información abre el campo a la auditoría informática y a muchas áreas afines que apoyan la seguridad de los datos manteniendo los principios de la seguridad.

6.3.5.1. Integridad

La integridad garantiza la modificación, manipulación, borrado y almacenamiento de archivos solo por el personal autorizado de forma controlada, en este sentido provee metodologías de seguridad por niveles y logs de auditoría para salvaguardar la información de las organizaciones, Pymes, empresas y/o compañías. Igualmente el sistema de información, proporcionara accesos a las configuraciones, conforme a los roles o privilegios otorgados por los administradores del sistema.

6.3.5.2. Disponibilidad

Es la capacidad del sistema de información para mantener el acceso en cualquier instante de tiempo, por lo tanto se controla los intentos de eliminar archivos o modificar registros, por medio de la identificación de usuario y clave de acceso.

6.3.5.3. Confidencialidad

La confidencialidad provee las garantías, para identificar los usuarios que acceden al sistema de información, identificando la hora y fecha a través de los controles adecuados.

6.3.6. SGSI

Un sistema de gestión de la seguridad informática es el enfoque sistemático, con el propósito de establecer los mecanismos de gestión, para la confidencialidad integridad y disponibilidad de la información dentro de un conjunto de estándares seguros, teniendo como objetivo identificar cada una de las personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a la compañía.

De esta manera se pueden establecer controles de seguridad de manera adecuada para cada componente y/o elemento que conforma los activos informáticos tangibles e intangibles.

6.3.6.1. Activos intangibles

Son los bienes inmateriales como:

- Relaciones inter-empresas
- Capacitaciones empresariales
- Habilidades y motivación de los empleados y/o trabajadores
- Bases de datos, Herramientas tecnológicas
- Know How (Conocimiento - Experiencia)
- Procesos operativos

6.3.6.2. Activos tangibles

Son los bienes de naturaleza material, los cuales son perceptibles a la vista del ser humano[5], como:

- Mobiliario, capital
- Infraestructura y área de terreno
- Material, elementos de trabajo
- Equipos informáticos
- Teléfonos, cableado de red
- Entre otros.

[5] WEB AND MACROS. *Los activos tangibles e intangibles - ejemplos*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.webandmacros.com/activos_cuadro_mando_integral.htm

6.3.7. Norma ISO 27001[6]

La norma ISO 27001, es la norma principal para adecuar los requisitos del sistema de gestión de la seguridad informática en las organizaciones, por lo tanto esta norma es certificable para los auditores externos, los cuales evalúan las Pymes, empresas, etc., dentro de los 11 dominios que existen en la norma ISO 27001, con el propósito de organizar y gestionar la seguridad cuyos objetivos son:

- Mantener una imagen excelente tanto interna, como externa (cliente – proveedor).
- Cumplimiento de la legislación vigente.
- Permear con claridad las directrices a seguir para mantener la seguridad de la información y datos.
- Identificación, análisis y mitigación de los riesgos asociados al sistema de información actual de la empresa o Pyme.
- Conocimiento de la importancia que tiene la información para la empresa, con el fin de armonizar la seguridad.
- Mejora procesos, procedimientos y actividades con que se desarrolla la gestión en cuanto a la información.

Por consiguiente sus 11 dominios y/o pilares para gestionar la información e implementar el sistema de gestión de seguridad de la información son:

6.3.7.1. Política de seguridad de la información

Este dominio articula los objetivos del negocio y la razón social de la Pyme, empresa u organización con las necesidades de la seguridad informática, para salvaguardar los datos, registro y demás información confidencial que se desee proteger, por lo tanto el documento debe contemplar todos los niveles y acciones a seguir en determinado caso.

- Clasificación de la información
- Naturaleza del negocio
- Información de uso interno y externo
- Necesidades técnicas y operativas

[6] ISOTOOLS. *ISO 27001: Dominios Tecnológicos de Seguridad de la Información*. [en línea]. [22 de enero del 2015]. Disponible en: http://www.isotools.org/2013/10/03/iso-27001-dominios/

6.3.7.2. Aspectos administrativos[7]

Es este dominio se asignan las responsabilidades en cuestión de seguridad informática, donde se conocen las funciones de cada persona con el fin de establecer los acuerdos de confidencialidad y asignación de los privilegios y roles para el uso de las aplicaciones.

- Asignación de responsabilidades
- Acuerdos de confidencialidad
- Riesgos de acceso de terceros

6.3.7.3. Gestión de activos

Este dominio se encarga de organizar los activos informáticos conforme a las características y componentes que lo integran dentro de una organización, realizando el respectivo inventario, con el propósito de establecer las directrices para el uso de los activos informáticos.

- Inventario de activos informáticos
- Clasificación de los activos informáticos

6.3.7.4. Recurso humano y seguridad de la información

En este dominio se establecen los lineamientos de los contratos, cláusulas de confidencialidad, accesos a las áreas de la organización, programas de capacitación, formación procesos y procedimientos en cada uno de los ámbitos laborales antes, durante y después de cada actividad.

- Contratación de personal idóneo[8]
- Capacitaciones constantes sobre las normas y riesgos de la organización
- Suspensión de credenciales cuanto termina el contrato

---

7 Gutiérrez, C. (2012). *WELIVESECURITY: Los 10 pilares básicos de la norma ISO 27001.* [en línea]. [22 de enero del 2015]. Disponible en: http://www.welivesecurity.com/la-es/2012/10/22/10-pilares-basicos-norma-iso27001/

[8] BLOOGER. (2010).*Seguridad de la información en Colombia*. [en línea]. [22 de enero del 2015]. Disponible en: (http://seguridadinformacioncolombia.blogspot.com/2010/04/iso-27001-e-iso-27002-dominio-11.html

6.3.7.5. Seguridad física

Este dominio establece las áreas seguras y seguridad de los equipos de cómputo que se deben tener en cuenta para cada uno de los perímetros o lugares donde se encuentran los activos informáticos tanto interno como externos, ofreciendo una seguridad para garantizar que el cableado, redes y demás activos y/o periféricos se encuentren protegidos, conforme a la técnicas de control.

- Áreas seguras
- Seguridad física
- Seguridad en los activos (equipos de cómputo)

6.3.7.6. Gestión de comunicaciones

Este dominio establece las metodologías para la seguridad en redes y sistemas de restauración que soporten las caídas del sistema cuando han tenido algún fallo grave, implementando procedimientos operativos y responsabilidades.

- Copias de seguridad
- Seguridad en redes

6.3.7.7. Control de accesos

Este dominio establece y proporciona las herramientas para la implementación de una política de acceso a los sistemas de información de una organización, con el propósito de identificar por medio de auditorías sistematizadas la trazabilidad de los cambios efectuados.

- Política control de acceso
- Gestión de acceso de usuarios
- Acceso a redes
- Acceso a las aplicaciones de la organización

6.3.7.8. Gestión de sistemas de información

Este dominio establece las técnicas y mecanismos para la seguridad en los sistemas informáticos, aplicando las metodologías de clave pública y clave privada para encriptar los mensajes, datos e información confidencial, asimismo se disminuyen las vulnerabilidades, riesgos y amenazas por utilizar adecuadamente las herramientas de comunicación.

- Controles criptográficos

6.3.7.9. Gestión de incidentes

Este dominio monitorea y propone recomendaciones cuando se presentan acontecimientos, notificaciones, fallas o puertas traseras en el sistema, con el fin de asignar por medio de procedimiento las acciones a seguir en casos fortuitos o inesperados.

- Gestión de incidentes
- Mejoras de seguridad

6.3.7.10. Continuidad del negocio[9]

Este dominio ayuda ajustar las necesidades de seguridad informática que no se pudieron tener en cuenta en la implementación de la organización, como su nombre lo indica (BCP, Business Continuty Planning), contempla las actividades que se deben seguir y realizar para restaurar los procesos después de incidentes críticos, garantizando la normalización de manera progresiva con un tiempo prudencial para dar respuesta a cualquier eventualidad, por ende avala la confidencialidad, integridad y disponibilidad de la información.

- Procedimientos
- Proceso
- Políticas
- Restauración de actividades
- Gestión de seguridad

[9] Gutiérrez, C. (2012). *Continuidad del negocio: ¿Cómo responder ante una contingencia?.* [en línea]. [18 de enero del 2015]. Disponible en: http://blogs.eset-la.com/laboratorio/2012/07/18/continuidad-negocio-como-responder-ante-emergencia/

6.3.7.11. Requisitos legales

Este dominio establece las normas legales y evalúa el estricto cumplimiento conforme a los requisitos establecidos.

- Normal legales en seguridad informática
- Requisitos políticos
- Requisitos legales
- Norma técnica en seguridad informática

6.3.8. Norma ISO 27002:2013[10]

La norma ISO 27002:2013[11], establece un conjunto de actividades y directrices bien definidas para la implementación de la seguridad informática, a fin de proteger los activos informáticos, generando confianza tanto al cliente interno como al cliente externo, de esta manera se empieza a implementar los procesos de seguimiento en cada una de las áreas, estableciendo e identificando cada uno de los potenciales riesgos que se pueden presentar en la empresa.

Por con consiguiente, apoya el análisis y valoración de los riesgos clasificando los activos de las Pymes u organizaciones, donde cada grupo de activo posee sus propias amenazas, vulnerabilidades y riesgos, proporcionando en prospectiva su impacto y la probabilidad de ocurrencia. Con esa finalidad se establecen los 14 dominios, 35 objetivos y 114 controles[12] para cada uno de los hallazgos encontrados a través de la auditoría, actualizada el 25 de septiembre del 2013 los cuales son:

[10] El portal ISO. (2015). *ISO 27000.es.* [en línea]. [20 de enero del 2015]. Disponible en: http://www.iso27000.es/iso27000.html

[11] ISO. (2015).*ISO/IEC 27002:2013.* [en línea]. [24 de enero del 2015]. Disponible en: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

[12] El portal ISO. (2015).*ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES.* [en línea]. [22 de enero del 2015]. Disponible en: http://www.iso27000.es/download/ControlesISO27002-2013.pdf

6.3.8.1. A5 Política de seguridad

(5.1.) Directrices de la dirección en seguridad de la información: En este dominio las Pymes, empresas u organizaciones deben establecer la política de seguridad conforme a la razón social y/u objetivo de la sociedad, con el fin de mantener los lineamientos de seguridad informática para el manejo de la información, dando respuesta los 2 controles:

- 5.1.1. Conjunto de políticas para la seguridad de la información.
- 5.1.2. Revisión de las políticas para la seguridad de la información

6.3.8.2. A6 Aspectos organizativos de la seguridad de la información

En este dominio, se establece la distribución organizacional a través de la infraestructura y los accesos de terceras partes, para la implementación de los controles de seguridad, conforme a:

(6.1) Organización interna: Establece la organización de gestión, con el propósito de implementar los controles:

- 6.1.1 Asignación de responsabilidades para la seguridad de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

(6.2.) Dispositivos para movilidad y teletrabajo: Registrar y mantener seguro las conexiones móviles y de teletrabajo, debido a los controles:

- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

6.3.8.3. A7 Seguridad ligada a los recursos humanos

En este dominio se debe amparar las capacitaciones, formación profesional y actividades para concientizar al recurso humano sobre los términos y condiciones de uso de la información, antes, durante y después de la relación laboral durante el periodo de tiempo que se labore, el cual se divide en:

(7.1) Seguridad en la definición del trabajo y los recursos o definición de los puestos de trabajo (Antes de la contratación): Suministra el manual de funciones de cada cargo, donde se especifican las actividades y funciones, con el fin de proveer las responsabilidades asignadas y así desarrollen pertenencia por la empresa, pro que conocen la importancia de su trabajo, donde se establecen los controles:

- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.

(7.2) Seguridad en el desempeño de las funciones del empleo (Durante la contratación): Conforme a las capacitaciones, formación laboral y profesional, los trabajadores conocen las amenazas, riesgos y vulnerabilidades que puede tener el sistema de información, por ende se encuentran instruidos para cumplir con la política de seguridad, teniendo como controles:

- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en seguridad de la información.
- 7.2.3 Proceso disciplinario.

(7.3) Finalización o cambio del puesto de trabajo (cese o cambio de puesto de trabajo): Contempla el debido cambio, traslado y finalización del contrato, con las garantías de que se ha entregado y dejado todo organizado conforme a las políticas de seguridad, donde los controles a implementar son:

- 7.3.1 Cese o cambio de puesto de trabajo.

6.3.8.4. A8 Gestión de activos

En este dominio las Pymes, empresas y organizaciones deben clasificar y tener inventariado los activos informáticos que poseen a su disposición, los cuales son controlados por el personal asignado para su manipulación y uso, gestionando los controles de:

(8.1) Responsabilidad sobre los activos: Proporcionar una adecuado protección sobre cada activo informático de la organización, manteniendo el compromiso con cada elemento y sus controles son:

- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.

- 8.1.4 Devolución de activos.

(8.2) Clasificación de la información: Proporciona los niveles adecuados de seguridad para cada uno de las clasificaciones de la información, implementando los controles de:

- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

(8.3.) Manejo de los soportes de almacenamiento: Proporciona mecanismos para la manipulación de los periféricos que se manejen dentro de una organización, adecuando los controles:

- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

6.3.8.5. A9 Control de Accesos

Este dominio se encarga de mantener el acceso a los sistemas de información, únicamente al personal autorizado, implementados en los siguientes controles de entrada.

(9.1) Requerimientos de negocio para el control de accesos: Registra los accesos autorizados al sistema de información conforme a la política de seguridad:

- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

(9.2) Gestión de acceso de usuario: Registrar los accesos autorizados y los no autorizados por medio del sistema, donde se instituyen los controles:

- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

(9.3) Responsabilidades del usuario: Se generan los logs de auditoría, manteniendo, a trazabilidad de las operaciones y acciones realizadas en el sistema de información, debido a sus controles de acceso:

- 9.3.1 Uso de información confidencial para la autenticación.

(9.4) Control de acceso a sistemas operativo y aplicaciones: Integrar por medio de privilegios y roles, los usuarios autorizados para ingresar a los sistemas de información, conforme a los controles:

- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

6.3.8.6. A10 Cifrado

Este dominio permite cifrar la información por medio de las metodologías de clave pública y clave privada en las organizaciones, Pymes y empresas.

(10.1) Controles criptográficos: Potencializar las metodologías criptográficas para mantener los datos confidenciales de manera segura, los cuales se asocian al uso de claves encriptados y controles como:

- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

6.3.8.7. A11 Seguridad física y ambiental

Este dominio permite establecer los controles de las instalaciones y la forma como se manipula la información, donde se desprende las áreas seguras y la seguridad de los equipos de cómputo.

(11.1) Áreas seguras: garantizar el acceso de personal autorizado, donde se implementan los controles:

- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.

- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga

(11.2) Seguridad de los equipos: Prevenir daños, pérdida y robo de los activos informáticos, donde se implementan los controles:

- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

6.3.8.8. A12 Seguridad en la operativa

Este dominio determina y asignan las operaciones y la forma como se desarrollan los procesos que se encuentran asociados a la ejecución de las actividades de forma adecuada, al interior de cada subdivisión

(12.1) Responsabilidades y procedimientos operación: Certifica los pasos de manera segura en cada uno de los activos involucrados, manteniendo los controles necesarios para su funcionamiento:

- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.

(12.2) Protección contra código malicioso: a través de los riesgos, vulnerabilidades y amenazas se establecen estrategias para mitigar los códigos maliciosos implementando:

- 12.2.1 Controles contra el código malicioso

(12.3) Copias de seguridad: Mantener los logs de auditoría, registro de fallas y copias de seguridad para salvaguardar la integridad de la información, por medio del control:

- Backup – Copias de seguridad de la información

(12.4) Registro de actividad y supervisión: Evaluar las actividades en cada uno de los procesos, procedimientos que se desarrollan con:

- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes

(12.5) Control del software en explotación: Implementación de las instalaciones y configuraciones necesarias en los equipos de cómputo del control:

- 12.5.1 Instalación del software en sistemas en producción.

(12.6) Gestión de las vulnerabilidades técnicas: Mitigar los riesgos que se generan por medio de aprovechamiento pública, implementando el control:

- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.

(12.7) Consideraciones de las auditorías de los sistemas de información: Maximizar los procesos de auditoría para gestionar e identificar las mejores prácticas y metodologías en los sistemas de información, aplicando el control:

- 12.7.1 Controles de auditoría de los sistemas de información.

6.3.8.9. A13 Seguridad en las telecomunicaciones

Este dominio establece la seguridad entre los canales de comunicación y conexiones, tanto internas como externas.

(13.1) Gestión de la seguridad en redes: Proporciona medidas para defender los canales de comunicación, como lo son las redes e infraestructura que soporta las telecomunicaciones, apoyada en los controles:

- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

(13.2) Intercambio de información: Cuando se va a distribuir o entregar información a personas de la misma empresa o empresas diferentes, se debe garantizar la seguridad en cada uno de los intercambios, manteniendo la confidencialidad e integridad de los datos, por medio de los controles:

- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

6.3.8.10. A14 Adquisición, desarrollo y mantenimiento de los sistemas de información

Este dominio se orienta a las empresas que se dedican al desarrollo de software, donde se deben establecer los requisitos en cada etapa definiendo las necesidades requeridas en cada período.

(14.1) Requisitos de seguridad de los sistemas de información: La seguridad es una de los requisitos para integrar los sistemas de información, donde se aplica el control:

- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

(14.2) Seguridad en los procesos de desarrollo y soporte: Implementar las técnicas de seguridad en las aplicaciones, software e información a través de los controles:

- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

(14.3) Datos de prueba: Implementa las técnicas para mantener salvaguardado los datos y la información requerida, aplicando pruebas en su desarrollo y efectuando el control:

- 14.3.1 Protección de los datos utilizados en pruebas.

6.3.8.11. A15 Relaciones con suministradores

Este dominio contempla los planes que se deben llevar a cabo para llevar y tener una buena comunicación entre los suministradores

(15.1) Seguridad de la información en las relaciones con suministradores: Proporciona los pasos y metodologías para mantener una buena armonía entre las necesidades y los servicios ofrecidos, teniendo en cuenta los controles:

- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

6.3.8.12. A16 Gestión de incidentes de la seguridad de la información

Este dominio aplica los hallazgos encontrados sobre la seguridad para dar cavidad a la mejora continua, implementando soluciones en pro de la seguridad informática y los procesos de gestión.

(16.1) Gestión de incidentes de seguridad de la información y mejoras: Conforme a los hallazgos encontrados, se establecen medidas y acciones correctivas de manera oportuna para mitigar los riesgos y amenazas asociadas, aplicar y registrar los incidentes presentados a través de los controles:

- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

6.3.8.13. A17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Este dominio establece las medidas para la continuidad del negocio a través de las actividades que son recurrentes, para identificar las que no se pueden eliminar porque generan un gran impacto.

(17.1) Continuidad de la seguridad de la información: Mantener un plan de acción, con el fin de reaccionar a los procesos críticos o fallas del sistema, aplicando los controles:

- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

(17.2) Redundancia: Cruzar la información necesaria, a través de las bases de datos para establecer el control de:

- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

6.3.8.14. A18 Cumplimiento

Este dominio establece los pasos para dar cumplimiento a los requisitos legales en cuanto a la seguridad, diseñando, operatividad y gestión de los sistemas para mantener la seguridad informática.

(18.1) Cumplimiento de los requisitos legales y contractuales: Impedir el incumplimiento de las leyes, normas, decretos que regulan la seguridad informática, por medio de los controles:

- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.

(15.2) Revisiones de la seguridad de la información: Adecuar los estándares y políticas de seguridad a la razón y/u objetivo de las organizaciones, implementando los controles:

- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

6.3.9. Análisis de riesgos informáticos

Es el proceso mediante el cual se identifican los activos informáticos de una organización o Pyme, la cual permite indagar sobre las posibles vulnerabilidades y amenazas a las cuales se puede encontrar expuesta una empresa grande o pequeña, por lo tanto se identifica la probabilidad de ocurrencia y el impacto de cada una, con el fin de implementar los controles y medidas preventivas necesarias para aceptar, transferir, evitar, o mitigar el riesgo identificado. Asimismo se podrá realizar una presunción o estimación del impacto a través de la matriz de riesgo, con el fin de identificar el riesgo total por medio de la fórmula:

RT (Riesgo Total) = Probabilidad x Impacto Promedio

6.3.10. Control de Gestión

Es el proceso que permite organizar y guiar la gestión de las actividades empresariales, el cual inicia con el planteamiento de un objetivo para ser evaluado y medido a través del tiempo. De esta manera se centra en la verificación constante de cada proceso dentro de la organización, asimismo se podrá implementar los principios de control, los cuales pueden ser[13]:

- Control por responsabilidades
- Desarrollo económico
- Integración de sistemas informáticos
- Control de excepciones
- Indicadores de gestión
- Medidas de comparación
- Entre otras

[13] Gestion.ORG. (2002). *¿Qué es el control de gestión?.* [en línea]. [16 de mayo del 2014]. Disponible en: http://www.gestion.org/estrategia-empresarial/4594/que-es-el-control-de-gestion/

6.3.11. Mapa Estratégico

Un mapa estratégico, es el que determina a través de una ruta de navegación el camino a seguir durante cada uno de los instantes del tiempo, en el cual se establecen: a) objetivos estratégicos, b) perspectivas, c) líneas o temas estratégicos y d) relación de causa efecto (matriz DOFA). Asimismo permite comunicar y permear a toda la organización los procedimientos, procesos y actividades que se llevan a cabo para el mejoramiento continuo.

6.3.11.1. Metodología Estratégica

La metodología determina una serie de pasos para desarrollar cada una de las actividades que se han planteado, de esta manera se puede llevar un orden consecutivo de cómo se debe actuar frente a las acciones y situaciones adversas que se pueden presentar a través de los medios informáticos o sistema operativo de una organización, estableciendo:

- Indicadores
- Metas
- Iniciativas estratégicas

6.3.12. Ciberdelincuentes

Son aquellas personas que realizan de forma ilícita actividades en internet, medios electrónicos y herramientas informáticas que por su procedencia pueden llevar a su propio lucro, donde pueden robar información, acceder a redes privadas, delitos informáticos.

6.3.12.1. Delitos Informáticos

Los delitos informáticos se definen como toda actividad ilegal y ofensas que se pueden cometer ante cualquier individuo o grupo de personas con motivos criminales, asimismo dañar intencionadamente a la víctima. El término delito informático generalmente es usado indistintamente a la palabra crimen cibernético, a la cual en inglés se le conoce como cibercrimen, donde la Organización de las Naciones Unidas (ONU) lo divide en dos categorías con sus respectivas definiciones:

- Cibercrimen en un sentido reducido (crimen computacional): Cualquier comportamiento ilegal perpetrando por medio de operaciones electrónicas que comprometa la seguridad de los sistemas computacionales y los datos procesados por ellos.

- Cibercrimen en un sentido amplio (crimen relacionado a las computadoras): Cualquier comportamiento ilegal cometido por cualquier medio o relacionado, a un sistema de computadoras o red, incluyendo crímenes como posesión ilegal y/u oferta o distribución de información por medio de un sistema de computadoras o red.

Los delitos informáticos son ejecutados en diversas modalidades y sus objetivos son la violación de los tres pilares fundamentales de la Seguridad Informática como lo son la confidencialidad, integridad y disponibilidad de la información (datos). Dentro de estas modalidades se encuentran los ataques de:

- Denegación de Servicios (DOS, Denial of Service)
- Instalación o propagación de software de Código Malicioso (Malware)
- Alteración y/o modificación de contenido mediante ataques de Secuencias de Comandos de Sitios Cruzados (XSS, Cross-Site Scripting)
- Inyecciones SQL (SQL Injection)
- Envío masivo de correo fraudulento (Spamming)
- Suplantaciones de Identidad (Phising)
- Ingeniería Social (Social Engineering)
- Interceptación de tráfico (Man in theMiddle)
- Entre otros

6.3.13. Auditoría

La auditoría es la herramienta para diagnosticar el sistema de información de una empresa y/o Pyme, el cual proporciona metodologías en la toma de decisiones sobre los sistemas auditados, por lo tanto se debe tener en cuenta que no todas las empresas manejan y manipulan la información de la misma manera, esto quiere decir que la auditoría puede diagnosticar y examinar diferentes aspectos conforme al área a inspeccionar, para determinar:

- Herramientas para la planeación y el control.
- Resultados, pronósticos, planes e informes de control adecuados.
- Propuestas para mejorar el control de los sistemas de información.

Asimismo el diagnostico se convierte en un examen sistemático que lo lleva a cabo un grupo de personas, empresas, organizaciones o una sola persona para revisar e intervenir los requisitos básicos para el funcionamiento del sistema de la Pyme.

6.3.13.1. Auditoría Interna

Según el Instituto de Auditores Internos (The Institute of Internal Auditors - IIA), definieron la auditoría interna como "*La actividad independiente y objetiva de aseguramiento y consulta concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno*"[14]. Asimismo se realizan los controles internos de la Pyme u organización para mejorar los procesos y procedimientos mitigando los riesgos, vulnerabilidades y amenazas que se puedan presentar.

Por consiguiente el objetivo principal de la auditoría interna se convierte en direccionar y proporcionar herramientas para la toma de decisiones conforme a las funciones y actividades a realizar en cada una de las áreas, analizando y evaluando cada proceso para determinar las recomendaciones y medidas necesarias. Favoreciendo los intereses de las empresas para proteger de manera global el funcionamiento de la Pyme y la permanencia en el sector donde desarrolla la actividad económica, por ende se adquiere el conocimiento necesario para profundizar en las operaciones de la empresa y así desarrollar los controles necesarios.

6.3.13.2. Auditoría Externa

La auditoría externa son los métodos utilizados por una empresa ajena para examinar sistemáticamente las herramientas que soportan la gestión de la empresa, como por ejemplo: el sistema de información administrativo, el sistema de información contable y aquellos sistemas que soportan algún procedimiento que pueda ser auditado para determinar la integridad del estado actual de los documentos, expedientes e información que ocasiono el ingreso de información.

Como resultado se emite un concepto independiente sobre los sistemas de información y se realizaran sugerencias conforme a los hallazgos y evidencias encontradas, con el objetivo de:

[14] Instituto de auditores internos. *¿Qué es la auditoria interna?*. [en línea]. [15 de enero del 2015]. Disponible en: http://www.iaiperu.org/index.php?option=com_content&view=article&id=80:ique-es-auditoria-interna&catid=49:preguntas-frecuentes&Itemid=40

- Dar fe pública sobre el procedimiento desarrollado para examinar los procesos.
- Validar las evidencias ante terceros.
- Formular los procedimientos de mejora continua.

En síntesis la auditoría externa la desarrolla un grupo de personas, organización o empresa que no están adscritas a la Pyme auditada para determinar un concepto e informe que justifique los hallazgos y las recomendaciones de mejora.

6.3.13.3. Diferencias entre auditoría interna y externa

Tabla 1 Cuadro comparativo auditoría interna y externa

Auditoría Interna	**Autoría Externa**
La realiza un auditor adscrito a la empresa o que tiene algún vínculo con la empresa.	La realiza un auditor o ente de control, que tenga alguna relación de tipo civil.
El diagnóstico de la auditoría es para la empresa y así desarrollar las mejoras necesarias.	El diagnóstico de la autoría es para terceros y así implementar planes de contingencia.
Conforme a la vinculación contractual laboral, la información y/o hallazgos son de carácter interno para las mejoras.	Conforme a la faculta legal y principios éticos, se puede hacer público los hallazgos para implementar mejoras.
La auditoría es de carácter ipso facto, esto quiere decir en el momento en que se realiza la inspección.	La auditoría es de carácter ex post facto, esto quiere decir después de que los hechos ya ocurrieron.
Los controles son evaluados continuamente.	Los controles se evalúan recurrentemente a nivel interno.
Los hallazgos poseen independencia solo interna y son de reserva de la empresa.	Los hallazgos poseen independencia absoluta y pueden ser publicados.

6.3.13.4. El auditor

El auditor es la persona encargada de realizar el proceso de verificación y validación de la información, a través de la herramienta para diagnosticar los hallazgos y las evidencias encontradas, para lograr y proponer un concepto de eficacia y eficiencia en las operaciones y actividades que desarrolla las empresas y/o Pymes. Como complemento el auditor debe poseer las siguientes características:

- Conocer el procedimiento auditor bajo los estándares legales y marco legal actual.
- Poseen un dominio del tema para proponer diálogos y acuerdos entre las partes.
- Ser una persona íntegro, objetivo, confiable, creativo, crítico, educado y con diplomacia para realizar una evaluación confiable e imparcial para proponer las mejores alternativas.
- Realizar un informe ético profesional, conforme a los hallazgos y las evidencias encontradas.
- Mantener una percepción positiva en cuanto a la empresa donde va a desarrollar las actividades de auditoría.
- Dar respuesta a las inquietudes y actividades desarrolladas conforme a la ética profesional realizando acuerdos.
- Ser una persona responsable, honesta y discreta con la información adquirida.

6.3.14. Auditoría informática

La auditoría informática es el procedimiento y conocimiento para analizar las normas, técnicas y buenas prácticas para determinar por medio de un sistema de gestión de la seguridad informática los mecanismos de control y así salvaguardar la información de las organizaciones, manteniendo la integridad, disponibilidad y seguridad de la información; con el propósito de aumentar la eficiencia y eficacia de los recursos físicos y humanos asociados a las tecnologías de la información (TI).

Por ende se realiza un examen crítico, sistemático y objetivo para evaluar los recursos informáticos y así verificar que se encuentren desarrollando la gestión en pro del cumplimiento de los objetivos propuestos y la seguridad de la información, a fin de tomar de forma adecuada las decisiones frente a las amenazas, riesgos y vulnerabilidades informáticas.

6.3.14.1. Objetivos de la auditoría informática

- Evaluar los procedimientos, procesos y actividades de cada elemento informático, diagnosticando las entradas, controles, archivos, seguridad y la forma como se obtiene la información.
- Proponer los controles y las medidas adecuadas para la seguridad informática, conforme a las necesidades de las organizaciones y/o Pymes, al interior del hardware y software.
- Verificar el cumplimiento de la normatividad vigente.

6.3.14.2. Beneficios de la auditoría informática

- Genera confianza ante los usuarios y personal que labora en la empresa, frente a los servicios de las tecnologías de la información (TI).
- Efectuar el diseño de un mapa estratégico o sistema de gestión de la seguridad informática para establecer los controles de seguridad.
- Reduce los costos de re-procesos, reclamos y procedimientos de baja calidad.

6.3.14.3. Alcance de la auditoría informática

Concretar los lineamientos para el desarrollo de la auditoría, conforme a los objetivos de la misma auditoría; identificando las fronteras y los puntos que se han alcanzado con la implementación de las preguntas adecuadas frente a los controles de gestión en los sistemas de información.

6.3.14.4. Herramientas para efectuar la auditoría informática

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Muestreo estadístico
- Flujo gramas
- Listas de chequeo
- Mapas conceptuales

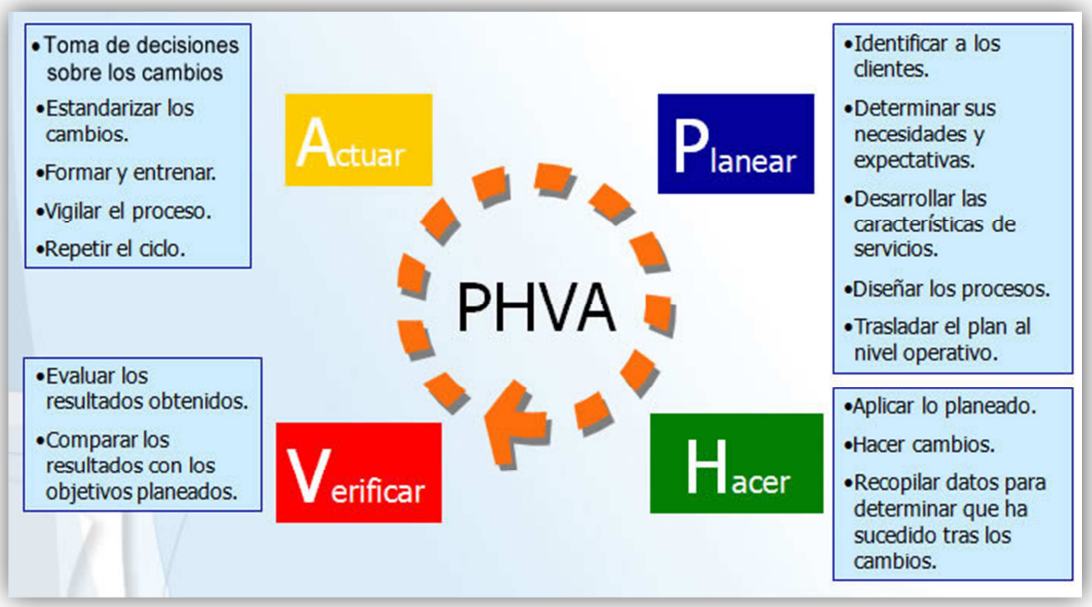
6.3.15. Ciclo PHVA

Es la herramienta de mejora continua a través del ciclo propuesto por Deming en 1950, el cual permite estableces 4 fases o etapas para el desarrollo de las actividades con el fin de ser retroalimentadas para mejorar en los aspectos que se pudieron quedar cortos en un principio y así ser más competitivos en el mundo, de esta manera se establecen las fases que son:

- Planear
- Hacer
- Verificar
- Actuar

Ilustración 1 Actividades ciclo PHVA

Fuente: Tomado de Implementación SIG[15]



[15] Implementación SIG. (2014). *El ciclo de Deming.* [ilustración 1]. [en línea]. [16 de mayo del 2014]. Disponible en: http://www.implementacionsig.com/index.php/generalidades-sig/55-ciclo-de-

6.3.15.1. Planificar (Plan)

En esta fase se establecen la planeación de las actividades, procesos y procedimientos a seguir en un tiempo determinado, proyectando en prospectiva los objetivos y metas.

6.3.15.2. Hacer (Do)

En esta fase se da inicio a la implementación de los objetivos, con el fin de alcanzar las metas proyectadas y trazadas en la planeación, poniendo en marcha las propuestas y actividades que cada uno de los integrantes de la organización debe implementar.

6.3.15.3. Verificar (Check)

En esta fase, a partir de la implementación, se debe realizar un monitoreo constante de las actividades para saber el estado en que se encuentran y así brindar un acompañamiento más oportuno, eficiente y eficaz en el desarrollo de las actividades, donde se destacan los:

- Objetivos
- Políticas de seguridad
- Requisitos
- Actividades

Asimismo realizar un análisis de los resultados que se van llevando hasta el momento, teniendo en cuenta la lista de chequeo.

6.3.15.4. Actuar (Act)

En esta fase, a través de los resultados obtenidos, se sugieren y proponen acciones de mejora continua para dar inicio nuevamente al ciclo de Deming, con el fin de realizar las acciones de mejora que sean necesarias para mantener un desempeño óptimo.

6.3.16. Pasos a seguir para desarrollar la auditoría

6.3.16.1. Estudio preliminar – Fase de reconocimiento

Para realizar el estudio preliminar se debe identificar las funciones del área a auditar, con el fin de identificar y conocer la distribución de los equipos de cómputo, infraestructura y métodos de seguridad existentes, indagando sobre:

- Organización: Permite conocer el organigrama, la áreas con sus respectivas funciones y relaciones entre cada área.
- Canales de información: Permite conocer los medios como se manipula la información y como se transmite a las diferentes áreas.
- Flujos de información: Permiten verificar los procesos en cada área para no generar redundancia en los procedimientos, identificando los cargos y las funciones.
- Ambiente de operaciones: Permite conocer la estructura y el entorno donde se va a realizar la auditoría teniendo en cuenta: a) ubicación geográfica, b) arquitectura de hardware y software, c) redes de comunicación y d) sistemas operativos.
- Aplicaciones informáticas: Permite conocer los procesos informáticos realizados al interior de la Pyme, recolectando:
    - Inventario de hardware
    - Inventario de software
    - Aplicaciones para salvaguardar y utilizar la información.
    - Metodología del diseño para almacenar la documentación e información
    - Recolección de información a través de documentos
- Recursos: Permite identificar los recursos humanos y físicos requeridos para la auditoría.

6.3.16.2. Técnicas de trabajo – Diseño de los instrumentos

- Diseño de la encuesta de auditoría para las Pymes.
- Análisis de la información recolectada en la primera etapa de reconocimiento de la organización y/o Pymes.
- Investigación de la información recolectada.

6.3.16.3. Herramientas de trabajo

- Estándares ISO
- Checklist
- Encuesta inicial
- Matrices de riesgo

6.3.16.4. Aplicación de la auditoría – Informe final

Informe final de la auditoría realizada en las Pymes, el cual debe contener:

- Objetivo de la auditoría
- Alcance de la auditoría
- Desarrollo de la auditoría en el cual se define
    - Situación actual
    - Hallazgos
    - Recomendaciones
    - Planes de acción – Sistema de gestión de la seguridad informática (SGSI)

Tabular las encuestas y los hallazgos para determinar los riesgos, vulnerabilidades y amenazas y así diseñar el sistema de gestión de la seguridad informática.

6.4. Marco Conceptual

6.4.1. Seguridad

El concepto de seguridad se aplica a los entornos de la vida cotidiana, de manera tal que el hombre siempre ha tenido la necesidad de imaginar mecanismos que le aseguren sus datos, los cuales viajan a través de una red informática o un medio de almacenamiento electrónico de forma segura, los cuales deben llegar sus respectivos receptores.

6.4.2. Estándares de seguridad

"*Si bien los estándares nos proporcionan una base importante para llegar a crear un modelo de seguridad, ésta se basa en las políticas de seguridad de la organización, las cuales determinan los procedimientos, los estándares y las herramientas que ayudarán a estas labores*"[16].

6.4.3. Modelo de seguridad

Son los mecanismos, protocolos, estándares, procesos, procedimientos y actividades que se enmarcan en un conjunto de pasos para desarrollar y mantener el control frente a los diversos dinamismos que se presentan en una organización frente a los avances tecnológicos.

6.4.4. Pymes

Son las empresas medianas o pequeñas, las cuales se catalogan dentro de este parámetro, cuando cumple con ciertos criterios y características definidas de acuerdo a la dinámica y comportamiento del mercado y lo financiero. En principio las características más relevantes son la cantidad de trabajadores y el balance general de productividad al año, como por ejemplo:

[16] Gómez, J. *Seguridad de la Información*. [en línea]. [09 de diciembre del 2013]. Disponible en: http://www.slideshare.net/hvillas/seguridaddela-informacion-17506228

Tabla 2 Categorías Empresarial[17]

Fuente: Tomado de ¿Qué es una Pyme?

Categoría	No. Trabajadores	Cantidad de Capital
Mediana	Menor de 250	≤ 50 millones
Pequeña	Menos de 50	≤ 10 millones
Microempresa	Menos de 10	≤ 2 millones

Por consiguiente las Pymes poseen una mayor flexibilidad para adaptarse a las diferentes medidas que puede proveer el mercado de los negocios y así implementar proyectos de innovación para poner en marcha propuestas que enriquezcan la productividad del país.

6.4.5. Norma ISO 27000

Es la norma establecida para dar a conocer por medio de las buenas prácticas los estándares y normas de seguridad frente a cada uno de los activos informáticos de una organización o Pymes, de esta manera se establecerá un sistema de control para los componentes y elementos que conforman los sistemas informáticos, salvaguardando el activo más importante de las empresas, (información – datos).

6.4.6. Norma ISO 27001

La norma ISO 27001, fue emitida por la Organización Internacional de Normalización (ISO), la cual describe la forma como se debe gestionar la seguridad de la información para las organizaciones. Por lo tanto al ser una norma internacional, las empresas se pueden certificar para garantizar a sus clientes y/o usuarios que cumplen con los estándares de seguridad internacionales debido a sus mejores prácticas.

[17]Comisión Europea. *¿Qué es una Pyme?.* [en línea]. [15 de mayo del 2014]. Disponible en: http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_es.htm

6.4.7. Norma ISO 27002

La ISO 27002 es un estándar para gestionar la seguridad de la información, debido a las recomendaciones para desarrollar las mejores prácticas entre los administradores que deseen implementar los sistemas de gestión de la seguridad informática, por lo tanto la integridad, confidencialidad y disponibilidad de los datos es el elemento para preservar a través de los diferentes controles dentro de sus dominios para la seguridad informática.

6.4.8. Norma ISO 27005

La ISO 27005 es un estándar internacional que se enfoca en la gestión de los riesgos, por lo tanto la norma establece directrices para gestionar los riesgos con referencia a la seguridad informática, implementando la metodología conforme a las necesidades y experiencias adquiridas, en el cual se determina el soporte para el diseño de un SGSI de conformidad con la norma 27001.

6.4.9. Escalas de medición

Las escalas de medición son el proceso por el cual se asigna un valor a un elemento en observación, y este elemento se desplaza en diferentes escalas para su interpretación e identificación, por lo tanto cada vulnerabilidad y amenaza será clasificada en la matriz de riesgo para su respectivo control.

6.4.10. Concepto de vulnerabilidad

El concepto de vulnerabilidad es muy importante porque demuestra el grado de incapacidad para anticipar, asimilar, resistir y recuperarse de un suceso ya sea por una catástrofe natural o un acto humano; todo esto producido por factores internos.

6.4.11. Concepto de amenaza

Amenaza se llama a todo aquello que genera la posibilidad de que ocurra un evento o fenómeno que puede o no causar daño (material o inmaterial) sobre un objeto animado o inanimado, causado por el factor externo.

6.4.12. Concepto de riesgo

Riesgo es lo que puede llegar a pasar cuando están de la mano la vulnerabilidad y la amenaza juntas las cuales generaran un daño o pérdida de la estructura física, material o humana.

6.4.13. Escala de medición probabilidad

Escala de medición probabilidad es un proceso de medición numérica que se encuentra en un intervalo de 0 a 1 para observar la posibilidad que ocurra un evento aun teniendo matrices y escalas de la clasificación de los elementos.

6.4.14. Escala de medición de impacto

La escala de medición del impacto tiene presente los elementos observados para que la colisión tenga un control de la matriz de riesgo que llegue a generar el proceso.

6.4.15. Hallazgo

Un hallazgo es un proceso evaluativo frente a un dato evidenciado ya sea novedoso u original de un aspecto natural considerándose una debilidad o fortaleza.

6.4.16. Concepto de control

Control es la regulación del funcionamiento de un sistema para realizar feedback correspondientes al desempeño logrado a lo largo permitiendo que las metas y objetivos propuestos sean cumplidos en un conjunto de acciones, procedimientos, normas y técnicas estipuladas.

6.4.17. Concepto de política

La política está basada en la toma de decisiones de un grupo para lograr que los objetivos sean culminados satisfactoriamente, desde la orientación, liderazgo e intervención de disputas de interés.

6.4.18. Concepto de procedimiento

Procedimiento es la ejecución de una determinada tarea, por medio de un proceso consecutivo y sistemático, llegando al descenso del objetivo trazado desde el comienzo del proceso.

6.5. Marco Legal

Cuando se piensa en la implementación de un sistema de gestión, en este caso el de seguridad informática, es necesario y obligatorio tener en cuenta desde el diseño, que se cumplan todas las leyes, decretos, normas, entre otras que apliquen durante el desarrollo de las actividades, buscando establecer la manera adecuada de proteger a las organizaciones y sus activos, sus colaboradores, a terceros, y a las personas en general de cualquier delito, infracción, proceso, procedimiento o acto mal ejecutado, que vulnere sus derechos, y ponga en riesgo su integridad, su buen nombre, sus activos y cualquier otro bien al que tengan pertenencia.

Durante el diseño del SGSI para las Pymes, se debe tener en cuenta que elementos de infraestructura hardware y software, políticas, sistemas y metodologías de gestión del riesgo, procesos, procedimientos, planes de seguridad y demás elementos serán necesarios para la implementación de SGSI, estos elementos durante su aplicación o implementación son susceptibles a que se pueda omitir el cumplimiento de alguna ley, y tener consecuencias sobre la organización o sobre una o más personas en particular, por eso es necesario conocer algunas leyes, decretos y normas que rigen sobre estos elementos buscando la protección del bien individual o colectivo, algunas de estas leyes, decretos o normas son:

- "Decreto 1360 de 1989, donde se reglamenta el soporte lógico (software) en el registro nacional del derecho de autor, considerando al software como una creación del dominio literario en conformidad a la ley 23 de 1982 sobre derechos de autor"[18].
- "Ley 527 de 1999, que establece y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales, además de establecer las entidades de certificación y otras disposiciones"[19].

[18]Jaramillo, A. *Manual de derecho de autor*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.derechodeautor.gov.co/documents/10181/331998/Cartilla+derecho+de+autor+(Alfredo+Vega).pdf/e99b0ea4-5c06-4529-ae7a-152616083d40

[19]Cuervo, J. *Aspectos jurídicos de internet y el comercio electrónico.* [en línea]. [13 de mayo del 2014]. Disponible en: http://www.informatica-juridica.com/trabajos/Aspectos_juridicos_de_Internet_y_el_comercio_electronico.asp

- “Decreto 1747 de 2000, que reglamenta parcialmente la ley 527 de 1999, con lo relacionado a las entidades de certificación, los certificados y las firmas digitales”[20].
- “Resolución 26930 de 2000, la cual fija los estándares para la autorización y el funcionamiento de las entidades de certificación y sus auditores”[21].
- “Ley estatutaria 1266 de 2008, que establece las disposiciones generales del habeas data y regula el manejo de la información que se contiene en las bases de datos personales, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”[22].
- “Ley 1273 de 2009, con la que se modifica el código penal, se crea u nuevo bien jurídico denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de información y de comunicaciones”[23].

[20] Decreto. Artículo 160 del Decreto ley 19 de 2012. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.sic.gov.co/documents/10165/2142817/DECRETO+333+DEL+19+DE+FEBRERO+DE+2014+VIG+ENTES+ACREDITAC.pdf/3dcd1c36-533a-48fa-a72c-7fcb2181e771

[21] Resolución. *Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5793

[22] Concepto. *Oficina juridicial nacional*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.legal.unal.edu.co/sisjurun/normas/Norma1.jsp?i=42011

[23] DELTA. (2014). *Ley de delitos informáticos en Colombia*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

7. DISEÑO METODOLÓGICO

Se realizara una investigación de tipo factible, que consiste en el análisis y desarrollo de una propuesta acerca del diseño de un SGSI para las Pymes, basado en estándares y normas internacionales, utilizando metodologías de desarrollo de proyectos, acordes a las buenas prácticas para la implementación y mejora continua del mundo actual. Atendiendo a esta modalidad de proyecto, se introducirán tres fases para el estudio con el fin de determinar que se cumpla con los requisitos del proyecto factible.

En la primera etapa se desarrolla una evaluación de los riesgos actuales y potenciales, así como las vulnerabilidades que enfrentan las Pymes, ante los intentos constantes de los ciberdelincuentes por apropiarse de la información confidencial o tratar de dejar sus sistemas inutilizados temporal o permanentemente, en esta etapa también se evaluará la situación actual de dichas empresas en cuanto a los métodos y herramientas utilizadas para defenderse de los posibles ataques informáticos internos y externos.

En la segunda etapa y de acuerdo a los resultados de la evaluación de las situaciones que generan riesgos, vulnerabilidades y procesos implementados en la actualidad, se propondrá un diseño del SGSI acorde a las necesidades de las empresas y a las que el medio trae de manera implícita, por consiguiente se realizara una ponderación de cada uno de los ataques evidenciados, para determinar la probabilidad de ocurrencia a partir de las veces en que se repite un suceso de ataque informático, clasificando en la matriz de riesgos, donde se evidencia una probabilidad alta, media y baja, dependiendo de la cantidad de veces en suceder el hecho, asimismo se determinara el impacto a través del peor escenario propuesto en un instante de tiempo en el que se pueda presentar el hecho, con el fin de clasificarla en un aspecto de leve impacto, moderado impacto y catastrófico impacto; por consiguiente se identificaran las acciones y procesos a realizar para el diseño del SGSI.

7.1. Línea y Tipo de Investigación

La línea de investigación corresponde: gestión de sistemas, los cuales representan un gran campo de indagación debido a sus dinamismos a través de la evolución de las tecnologías de la información, dicha investigación se verá representada en el diseño de un sistema de gestión de la seguridad informática.

7.2. Diseño de la Investigación

En función a los objetivos propuestos para el proyecto y dentro de la modalidad de investigación definida, se implementaran la auditoría y técnicas de recolección de información, para tal efecto se cumplirá con tres etapas, la primera de ellas hace referencia a la delimitación del objeto de estudio y la elaboración del marco teórico, la segunda determina la realización de la evaluación de los riesgos, vulnerabilidades y situación actual de las Pymes en el tema de seguridad informática, la tercera se enfoca en el diseño de un SGSI que permita minimizar dichos riesgos, e implementar procesos adecuados con estándares de calidad, los riesgos que se analizarán son de tipo interno y externo y los procesos que están implementados para su mitigación o prevención.

7.3. Instrumentos de Recolección de Información

Para efectos de la investigación se hará uso de todas las fuentes bibliográficas posibles, textos, manuales, tesis, internet, revistas técnicas, ponencias de expertos, y demás elementos documentales, que permitan recopilar a su vez, antecedentes relacionados con la investigación.

De este modo también se utilizará la observación directa y las entrevistas, de tal manera que permitan complementar las evaluaciones a realizar.

7.4. Población y Muestra (Universo)

La población total del tema de estudio se estima entre 2 o 3 empresas y/o Pymes del sector textil en las ciudades de Medellín, Itagüí y Bogotá D.C., correspondiente a algunas asociaciones de Colombia que registran en cámara de comercio de las diferentes zonas del país.

La población que servirá como objeto de investigación, puede identificarse en personas, equipos, procedimientos y procesos en las Pymes Colombianas, por lo tanto se podrá tomar muestras a través de la entrevista y la auditoría a profesionales de sistemas, directivos u operadores de los sistemas de cómputo de cada Pyme, así como de procedimientos implementados, procesos ejecutados, equipos involucrados en los procesos y herramientas locales y externas.

Para el cálculo de la muestra de tal manera que sea representativa al total de la población, se tendrá en cuenta los siguientes factores:

- El tamaño de la muestra (n)
- El nivel de confianza (Z)
- Desviación estándar de la población (σ)
- El tamaño de la población (N)
- El margen de error que se acepta(e)

Estos factores se denotan en la siguiente fórmula y a continuación se exponen los valores reales para determinar la muestra del total de la población que será representativa para conocer la situación generalizada de la población que es objeto de estudio o investigación.

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Tamaño de la población: 3
Margen de error: 5%
Nivel de confianza: 90%
Desviación estándar o variabilidad: 50%

7.5. Fases Metodológicas o Metodología de la Investigación

Fase I: Esta se basará en la descripción de los riesgos, vulnerabilidades y sistemas implementados actualmente para su mitigación en las Pymes abordadas.

En esta fase se utilizaran herramientas como:

- La observación directa, cuya finalidad es verificar de una manera visual la implementación de seguridad informática vigente en las empresas, a su vez visualizar los métodos de trabajo y control del personal y los planes de contingencia establecidos ante eventuales ataques.
- Las entrevistas a los profesionales del área de sistemas, quienes son los más documentados y experimentados en la ejecución de procesos informáticos, de esta manera conocer las medidas de prevención con las que cuenta la organización, por ende son los más indicados para ofrecer información relevante para el estudio.

Fase II: Está basada en la selección de herramientas de evaluación que servirán para diagnosticar el nivel de riesgo por procesos, las herramientas utilizadas son:

- Auditoría, que se pueden realizar inclusive a algunos usuarios diferentes al área de sistemas, y pueden ayudar a evaluar las actividades realizadas por estas personas y conocer que riesgos se afrontan de acuerdo a dicha actividad.
- Lista de chequeo, permiten evaluar la capacidad de respuesta que tienen estas empresas ante un eventual ataque informático.

Fase III: Se trata de la generación de propuestas de un diseño de SGSI para la organización.

- La generación de las alternativas se realiza de acuerdo a los resultados y el estudio de las evaluaciones realizadas, y aunque pueden variar de una empresa a otra se hará una propuesta que pueda ser adoptada por cualquier Pyme, tomando en cuenta los riesgos existentes y generalizados al interior y exterior de este tipo de empresas.

8. NOMBRE DE LAS PERSONAS QUE PARTICIPARAN EN EL PROCESO

Tabla 3 Responsables del Proyecto

Nombre	Cargo
Ing. Carlos Alberto Taborda Bedoya	Ingeniero investigador del proyecto
Ing. Alexánder Guzmán García	Ingeniero de Sistemas investigador del proyecto.
Ing. Francisco Solarte Solarte	Director del proyecto de investigación

9. DESARROLLO DE LA AUDITORÍA

9.1. Plan de auditoría

9.1.1. Objetivo de la auditoría

Diagnosticar los sistemas de información de las 2 empresas visitadas, identificando los hallazgos encontrados para establecer decisiones sobre las evidencias y diseñar el sistema de gestión de la seguridad informática - SGSI para las Pymes del sector textil en Medellín, Itagüí y Bogotá D.C.

9.1.2. Alcance de la auditoría

Determinar a través de los hallazgos encontrados, los controles y las recomendaciones para la implementación y diseño de un sistema de gestión dela seguridad informática – SGSI.

9.1.3. Metodología para desarrollo de la auditoría

- Pasos para cumplir cada uno de los objetivos propuestos
- Recursos para llevarla a cabo
- Recursos humanos, tecnológicos para llevar a cabo la auditoría
- Cronograma de actividades
- Diagrama de Gantt

9.2. Programa de auditoría

9.2.1. Estándares ISO

Conforme a la norma ISO 27001:2013 se seleccionaron los siguientes controles y dominios para aplicar la auditoría en cada empresa, Pyme u organización.

Tabla 4 Dominios y procesos seleccionados [24]

Fuente: Tabla estructurada con los dominios y procesos seleccionados

DECLARACIÓN DE APLICABILIDAD	
REF.	CONTROL
5. POLÍTICA DE SEGURIDAD	
5.1. Política de Seguridad de la Información	
5.1.1	Conjunto de políticas para la seguridad de la información
5.1.2	Revisión de las políticas para la seguridad de la información
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1. Organización Interna	
6.1.1	Asignación de responsabilidades para la seguridad de la información
6.1.2	Segregación de tareas
6.1.5	Seguridad de la información en la gestión de proyectos
6.2. Dispositivos para movilidad y teletrabajo	
6.2.1.	Política de uso de dispositivos para movilidad
6.2.2.	Teletrabajo
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
7.2. Seguridad en el desempeño de las funciones del empleo (Durante la contratación)	
7.2.1	Responsabilidades de gestión
7.2.2	Concienciación, educación y capacitación en seguridad de la información
8. GESTIÓN DE ACTIVOS	
8.1. Responsabilidad sobre los activos	
8.1.1	Inventario de Activos
8.1.2	Propiedad de los activos
8.1.3.	Uso aceptable de los activos
8.1.4.	Devolución de activos
8.2. Clasificación de la información	
8.2.1.	Directrices de clasificación
8.2.2.	Etiquetado y manipulado de la información
8.2.3.	Manipulación de activos
9. CONTROL DE ACCESO	
9.1 Requerimientos de negocio para el control de acceso	
9.1.1	Política de control de acceso
9.2. Gestión de acceso de usuario	
9.2.1	Gestión de altas/bajas en el registro de usuarios
9.2.3	Gestión de los derechos de acceso con privilegios especiales
9.3. Responsabilidades de usuario	
9.3.1	Uso de información confidencial para la autenticación
9.4. Control de acceso a sistemas operativo y aplicaciones	

[24] Fuente: Tabla estructurada con los dominios y procesos seleccionados

9.4.1	Restricción del acceso a la información
9.4.2	Procedimientos seguros de inicio de sesión
9.5.4	Uso de herramientas de administración de sistemas
10. CIFRADO	
10.1 Controles criptográficos	
10.1.1	Política de uso de los controles criptográficos
10.1.2	Gestión de claves
11. SEGURIDAD FÍSICA Y DEL ENTORNO	
11.1. Áreas seguras	
11.1.2	Controles físicos de entrada
11.1.3	Seguridad de oficinas, despachos y recursos
11.1.4	Protección contra las amenazas externas y ambientales
11.2. Seguridad de los equipos	
11.2.1	Emplazamiento y protección de equipos
11.2.2	Instalaciones de suministro
11.2.3	Seguridad del cableado
11.2.4	Mantenimiento de los equipos
12. SEGURIDAD EN LA OPERATIVA	
12.2. Protección contra código malicioso	
12.2.1	Controles contra el código malicioso
12.3. Copias de seguridad	
12.3.1	Copias de seguridad de la información
12.4. Registro de actividad y supervisión	
12.4.1	Registro y gestión de eventos de actividad
12.4.3	Registros de actividad del administrador y operador del sistema
12.6 Gestión de las vulnerabilidades técnicas	
12.6.1	Gestión de las vulnerabilidades técnicas
12.6.2	Restricciones en la instalación de sistema operativo (S.O.)
12.7 Consideraciones de las auditorías de los sistemas de información	
12.7.1	Controles de auditoría de los sistemas de información
13. SEGURIDAD EN LAS TELECOMUNICACIONES	
13.2 Intercambio de información	
13.2.3	Mensajería electrónica
13.2.4	Acuerdos de confidencialidad y secreto
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	
14.1 Requisitos de seguridad de los sistemas de información	
14.1.1	Análisis y especificación de los requisitos de seguridad
14.3 Datos de prueba	
14.3.1	Protección de los datos utilizados en pruebas
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
16.1. Gestión de incidentes de seguridad de la información y mejoras	
16.1.6	Aprendizaje de los incidentes de seguridad de la información
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	

17.1. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio	
17.1.1	Planificación de la continuidad de la seguridad de la información
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
18. CUMPLIMIENTO	
18.1. Cumplimiento de los requisitos legales y contractuales	
18.1.1	Identificación de la legislación aplicable
18.1.2	Derechos de propiedad intelectual (DPI)
18.1.3	Protección de los registros de la organización
18.1.4	Protección de datos y privacidad de la información personal
18.2. Revisiones de la seguridad de la información	
18.2.2	Cumplimiento de las políticas y normas de seguridad

9.3. Etapas de la auditoría - etapa de conocimiento de las empresas

9.3.1. Informe director Guille Sport:

Realizado por:

Carlos Alberto Taborda Bedoya

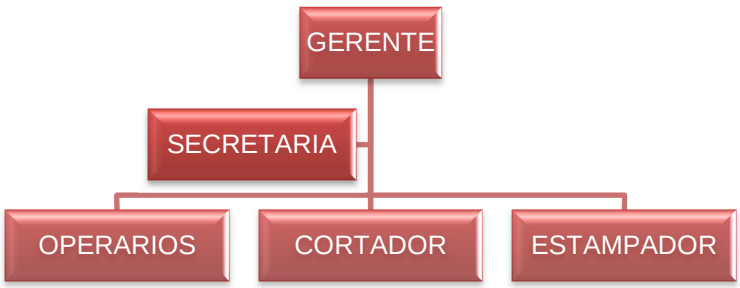
Alexander Guzmán García

9.3.1.1. Tema Guille Sport:

Visita inicial a Pymes del sector textil en Medellín y su área metropolitana y Bogotá.

Figura 1 Organigrama Guille Sport[25]

Fuente: Estructura organizacional tomada de la empresa Guille Sport



9.3.1.2. Objetivo Guille Sport:

Conocer a través de una primera visita, los recursos de infraestructura y de informática utilizados en las Pymes para gestionar y mantener su información.

9.3.1.3. Descripción general Guille Sport:

Se realizó una primera visita a la microempresa Guille Sport, ubicada en el municipio de Bello-Antioquia, empresa que se dedica al corte, confección y venta de prendas deportivas masculinas y femeninas, buscando obtener información sobre la infraestructura que manejan para dar gestión a la información concerniente a desarrollo de actividades propias del negocio.

[25] Fuente: Estructura organizacional tomada de la empresa Guille Sport

El proceso se constituyó a través de una visita de observación avalada por el propietario de la empresa, y después de realizar dicha visita, se presenta a continuación la infraestructura hallada:

9.3.1.4. Activos de información Guille Sport

Para el manejo de información, la empresa cuenta con los siguientes activos:

Tabla 5 Inventario de activos Guille Sport[26]

Fuente: Tomado de UNAD. Inventario de activos

Inventario de activos	
Tipos de activos	**Nombre de activos empresa Guille Sport**
Activo de información	Datos de clientes y proveedores (Archivos en Excel)
	Documentos Físicos (Libro contable, facturas… entre otros)
Software o aplicación	El software no está licenciado
Hardware	PC1 Computador de escritorio Clon. Utilizado por el propietario de la empresa.
	PC2 Computador portátil. Utilizado por la secretaria o por su reemplazo.
	Impresora multifuncional
	Disco duro extraíble de 1 Tera
Instalación	Cables para el fluido eléctrico
Servicios	Conectividad a internet
Personal	Empleados de las diferentes líneas de producción, secretaria y propietario

[26] UNAD. Inventario de activos. [en línea]. [09 de febrero del 2015]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321_paso_1_inventario_de_activos.html

9.3.1.5. Infraestructura física Guille Sport

La empresa Guille Sport se encuentra ubicada en el municipio de Bello-Antioquia, en un sector residencial, en un edificio compuesto por varios locales destinados al comercio, el local es un área abierta donde se encuentran zona de corte, zona de confección, zona de estampado, escritorio de secretaria y oficina del propietario de la empresa, en esta empresa laboran generalmente entre 6 y 10 empleados, dependiendo de temporadas del año donde se trabaja con mayor o menor producción.

Ilustración 2 Zona Corte Guille Sport[27]

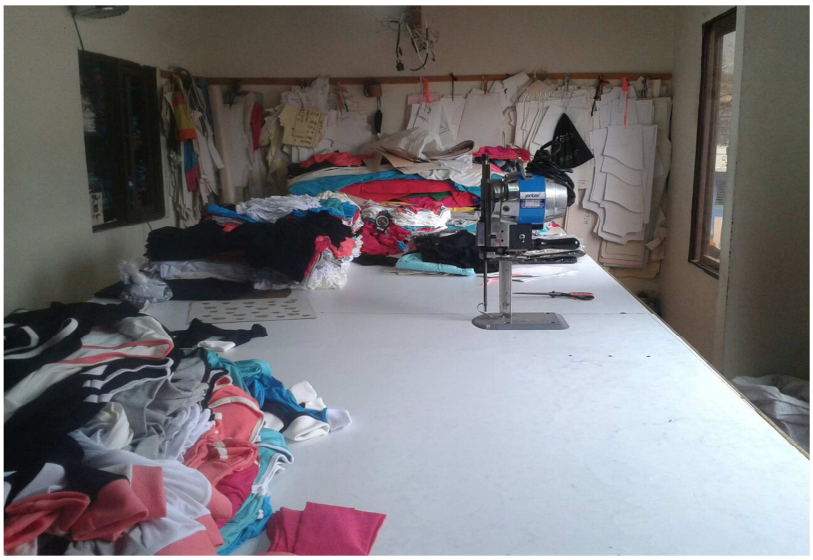


Ilustración 3 Zona confección Guille Sport[28]

[27] Fotografía de la empresa Guille Sport
[28] Fotografía de la empresa Guille Sport

9.3.1.6. Infraestructura informática Guille Sport

La infraestructura informática se basa en un servicio de conexión a internet banda ancha de 20 megas, con un modem inalámbrica para brindar conexión a otros equipos dentro de la empresa.

La empresa cuenta con dos equipos de cómputo con sistema operativo Windows 7(no licenciado), uno destinado para el propietario de la misma, y el otro para el uso de la secretaria, también poseen una impresora multifuncional, cuentan con un modem instalado por un proveedor ISP, conectado por cable al equipo del propietario de la empresa y por vía inalámbrica al equipo de la secretaria. A su vez, el propietario de la empresa cuenta con un disco duro portable conectado a su PC.

Ilustración 4 Máquina estampado Guille Sport[29]

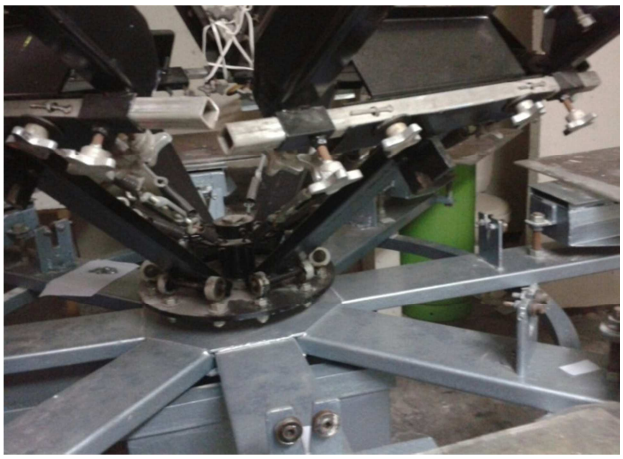
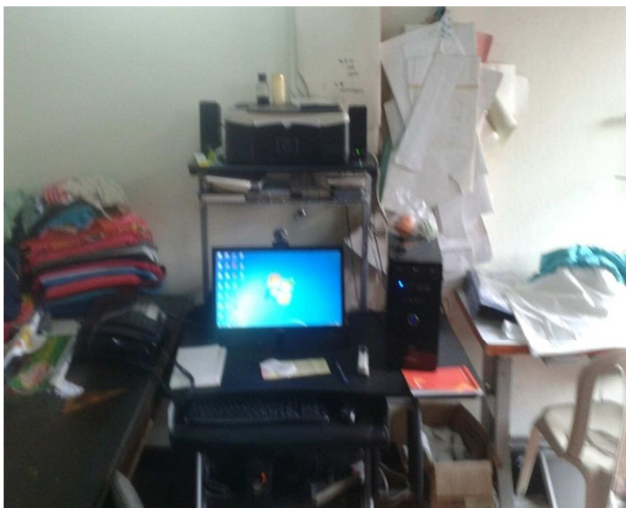


Ilustración 5 Equipo PC Guille Sport[30]



[29] Fotografía de la empresa Guille Sport
[30] Fotografía de la empresa Guille Sport

Tabla 6 Valoración para activos Guille Sport[31]

Fuente: Tomado de UNAD. Valoración de los activos

Escala de valoración cualitativa y cuantitativa para los activos		
Valoración Cualitativa	Escala de valor cuantitativo	Valor cuantitativo
Muy Alto (MA)	> $ 15.000.000	$ 16.000.000
Alto (A)	$ 15.000.000 <valor> $ 6.000.000	$ 7.500.000
Medio (M)	$ 6.000.000 <valor> $ 1.000.000	$ 3.000.000
Bajo (B)	$ 1.000.000 <valor> $ 100.000	$ 500.000
Muy Bajo (MB)	$ 100.000 <valor> $ 30.000	$ 50.000

Tabla 7 Criterio de valoración de activos Guille Sport[32]

Fuente: Tomado de seguridad informática. pilar - herramienta para análisis y gestión de riesgos

Valor	**Criterio**
10	Daño muy grave
7-9	Daño grave
4-6	Daño importante
1-3	Daño menor
0	Irrelevante

[31] UNAD. Valoración de los activos. [en línea]. [25 de febrero del 2015]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/322__paso_2_valoracin_de_los_activos.html.

[32] SEGURIDAD INFORMÁTICA. PILAR - Herramienta para Análisis y Gestión de Riesgos. [en línea]. [25 de febrero del 2015]. Disponible en: https://seguridadinformaticaufps.wikispaces.com/PILAR+-+Herramienta+para+An%C3%A1lisis+y+Gesti%C3%B3n+de+Riesgos

Valoración de activos de acuerdo a la dimensiones de seguridad y criterios para activos.

Tabla 8 Dimensiones de los riesgos Guille Sport[33]

Fuente: Tomado de UNAD. Dimensiones de Seguridad

		Dimensiones				
Tipo	**Nombre De Activo**	**Confidencialidad ¿Qué daño**	**Integridad ¿Qué perjuicio causaría que**	**Disponibilidad ¿Qué perjuicio causaría no**	**Autenticidad ¿Qué perjuicio causaría no saber**	**Trazabilidad ¿Qué daño causaría no**
Activo de información	Datos de clientes y proveedores(Archivos en Excel)	[9][A]	[9][A]	[6][M]	[8][A]	
	Documentos Físicos	[10][MA]	[1][MB]	[1][MB]		
Software o aplicación	El software no está licenciado		[10][MA]			
Hardware	PC1 Computador de escritorio Clon. Utilizado por el propietario de la empresa.	[9][A]	[9][A]	[6][M]	[6][M]	
	PC2 Computador portátil. Utilizado por la secretaria o por su reemplazo.	[8][A]	[6][M]	[6][M]	[6][M]	

[33] UNAD. Dimensiones de Seguridad. [en línea]. [05 de febrero del 2015]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3221_dimensiones_de_seguridad.html

	Impresora multifuncional			[3][MB]		
	Disco duro extraíble de 1 Tera	[8][A]	[8][A]	[6][M]	[6][M]	
Instalación	Cables del fluido eléctrico			[7][M]		
Personal	Empleados de las diferentes líneas de producción, secretaria y propietario			[9][A]		

Tabla 9 Dimensiones de valoración del impacto Guille Sport[34]

Fuente: Tomado de introducción a la seguridad informática

Cód.	**Nombre Dimensiones de valoración**
[D]	Disponibilidad
[I]	Integridad de los datos
[C]	Confidencialidad de la información
[A]	Autenticidad
[T]	Trazabilidad

[34] Mifsud, Elvira. Introducción a la seguridad informática. [en línea]. [25 de febrero del 2015]. Disponible en: http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

Tabla 10 Amenazas Guille Sport[35]

Fuente: Tomado de UNAD. Identificación de amenazas

Cód.	Amenazas	Impacto
[N] Desastres Naturales		
[N.1]	Incendio	[D][I]
[N.2]	Inundación	[D][I]
[I] De origen industrial		
[I.5]	Avería de origen físico	[D]
[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
[I.9]	Interrupción de otros servicios o suministros esenciales	[D]
[E] Errores y fallos no intencionados		
[E.1]	Errores de los usuarios	[D][I][C]
[E.16]	Introducción de falsa información	[I]
[A] Ataques deliberados		
[A.11]	Acceso no autorizado	[D][I][C][A][T]
[A.15]	Modificación deliberada de la información	[I]
[A.16]	Introducción de falsa información	[I]
[A.18]	Destrucción de la información	[D][I]
[A.25]	Robo de equipos	[D][I][C][A][T]
[A.30]	Ingeniería social	[D][I][C][A][T]

[35] UNAD. Identificación de amenazas. [en línea]. [25 de febrero del 2015]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3231_identificacin_de_amenazas.html

Tabla 11 Escala de valoración de rango porcentual de impacto en los activos Guille Sport[36]

Fuente: Tomado de UNAD. Valoración de amenazas

Impacto	Valoración del impacto
Muy Alto (MA)	100%
Alto (A)	75%
Medio (M)	50%
Bajo (B)	20%
Muy bajo (MB)	5%

Tabla 12 Escala de rango de frecuencia de amenazas Guille Sport[37]

Fuente: Tomado de UNAD. Valoración de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

[36] UNAD. Valoración de amenazas. [en línea]. [17 de febrero del 2015]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/3232_valoracin_de_amenazas.html
[37] Ibíd., p. 1.

Tabla 13 Valoración de las amenazas Guille Sport[38]

Fuente: Tomado de UNAD. Valoración de amenazas

Cód.	Amenazas	Frecuencia	Impacto	Causas
[N] Desastres Naturales				
[N.1]	Incendio		100%	Acumulación de gases, tormentas eléctricas.
[N.2]	Inundación	5	50%	Lluvia
[I] De origen industrial				
[I.5]	Averías de origen físico	5	20%	Cortos circuitos, variación eléctrica, apagado incorrecto
[I.7]	Condiciones inadecuadas de temperatura o humedad	5	20%	Humedades en paredes
[I.9]	Interrupción de otros servicios o suministros esenciales	50	5%	Interrupción del fluido eléctrico o acceso a internet
[E] Errores y fallos no intencionados				
[E.1]	Errores de los usuarios	50	5%	Falta de conocimiento en manejo de sistemas de información.
[E.16]	Introducción de falsa información	50	20%	Personal poco idóneo para ingresar o actualizar la información
[A] Ataques deliberados				

[38] Ibíd., p. 1.

[A.11]	Acceso no autorizado	5	5%	Equipos sin controles para el acceso a los mismos
[A.15]	Modificación deliberada de la información	5	20%	Intención de daños a la empresa
[A.16]	Introducción de falsa información	50	20%	Intención de dañar y afectar la empresa o sus procesos
[A.25]	Robo de equipos	5	5%	Poca seguridad de la zona geográfica
[A.30]	Ingeniería social	5	5%	Desconocimiento o exceso de confianza de algunos empleados

9.3.2. Informe director Color Shop:

Realizado por:

Carlos Alberto Taborda Bedoya

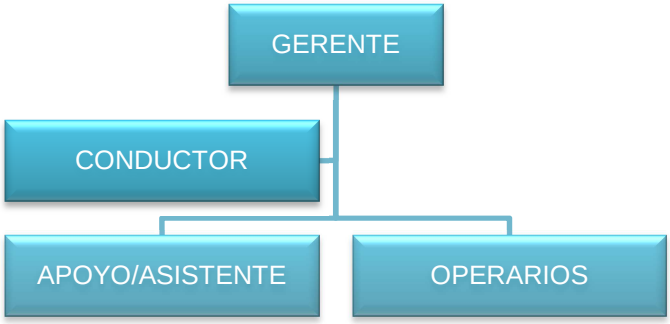
Alexander Guzmán García

9.3.2.1. Tema Color Shop:

Visita inicial a Pymes del sector textil en Medellín y su área metropolitana y Bogotá.

Figura 2 Organigrama Color Shop[39]

Fuente: Estructura organizacional tomada de la empresa Color Shop



9.3.2.2. Objetivo Color Shop:

Conocer a través de una primera visita, los recursos de infraestructura informática utilizados en las Pymes para gestionar y mantener su información.

9.3.2.3. Descripción General Color Shop:

Se realizó una primera visita a la microempresa Color Shop, ubicada en el municipio de Medellín-Antioquia, en el barrio Sagrado Corazón, empresa que se dedica a la terminación de procesos industriales para prendas de vestir, especialmente pantalones (jeans), con la visita se pretende obtener información sobre la infraestructura que manejan para dar gestión a la información concerniente al desarrollo de actividades propias del negocio.

[39] Fuente: Estructura organizacional tomada de la empresa Color Shop

El proceso se constituyó a través de una visita de observación avalada por el propietario de la empresa, y después de realizar dicha visita, se presenta a continuación la infraestructura hallada:

9.3.2.4. Activos de información Color Shop

Para el manejo de información, la empresa cuenta con los siguientes activos:

Tabla 14 Inventario de activos Color Shop[40]

Fuente: Tomado de UNAD. Inventario de activos

INVENTARIO DE ACTIVOS	
Tipos de activos	**Nombre de activos empresa Guille Sport**
Activo de información	Datos de clientes, proveedores y personal (Archivos de Microsoft Excel)
	Documentos Físicos (Libro contable, facturas)
Software o aplicación	Sistema Operativo Windows 7 Home Edition licencias OEM
	Office 2007 licencias OEM
	Antivirus Microsoft Security Essentials
Hardware	PC1 Computador de escritorio marca HP. Utilizado por el propietario de la empresa.
	PC2 Computador de escritorio marca HP. Utilizado por algunos de los empleados para informar procesos realizados.
	Impresora multifuncional HP 1515 deskjet
	2 memorias USB de 16 GB
Instalación	Cables para el fluido eléctrico
Servicios	Conectividad a internet

[40] UNAD. Inventario de activos, op. cit, p.1.

Personal	Empleados y propietario
Otros	Sistema de video vigilancia Cctv

9.3.2.5. Infraestructura Física Color Shop

La empresa Color Shop se encuentra ubicada en el municipio de Medellín-Antioquia, en un sector industrial, el edificio donde se encuentra ubicado cuenta con diferentes locales para el comercio y fabricación de distintas líneas de productos, el local se divide en varias áreas separadas donde se realizan procesos como estampado y tintorería, además de la oficina del propietario de la empresa, la empresa tiene un total de 10 empleados, pero en temporadas de mayor producción se puede tener hasta 16.

Ilustración 6 Zona Producción Color Shop[41]

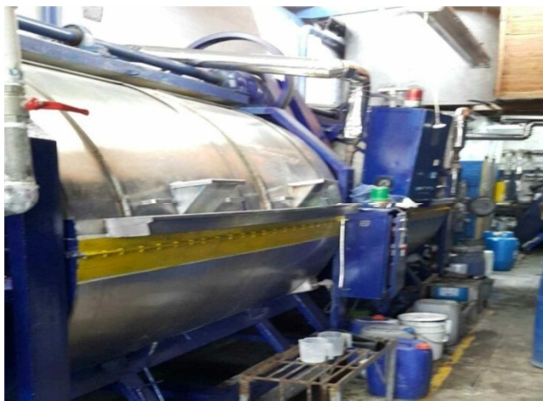
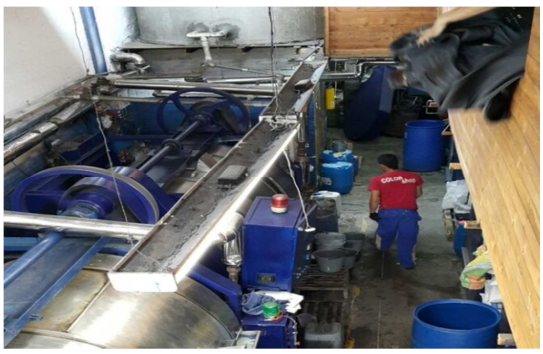


Ilustración 7 Zona Producción 2 Color Shop[42]



[41] Fotografía de la empresa Color Shop
[42] Fotografía de la empresa Color Shop

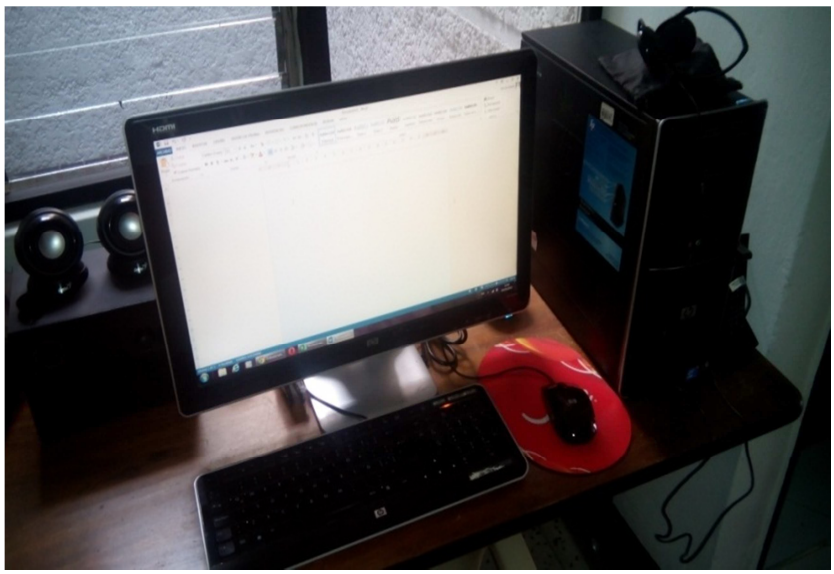
9.3.2.6. Infraestructura Informática Color Shop

La infraestructura informática se compone de un servicio de conexión a internet banda ancha de 10 megas, con un modem inalámbrico para brindar conexión a otros equipos dentro de la empresa.

La empresa cuenta con dos equipos de cómputo marca HP con sistema operativo Windows 7 licencia OEM, y con el software de ofimática Office 2007 cuya licencia también es OEM, los equipos cuentan con el antivirus propio de Microsoft(Microsoft Security Essentials), que se descarga de manera gratuita para este tipo de licencias del S.O, los equipos se utilizan así: uno destinado para el propietario de la empresa, y el otro para el uso de algunos de los empleados para datar procesos realizados en determinados espacios de tiempo, también poseen una impresora multifuncional marca HP, cuentan con un modem instalado por un proveedor ISP, conectado por cable al equipo del propietario de la empresa y por vía inalámbrica al otro equipo el cual posee una tarjeta de red inalámbrica para este fin.

El local cuenta con un sistema de video vigilancia Cctv con dos cámaras que apuntan una hacia el interior y otra hacia el exterior del mismo, el cual guarda la información en un disco duro de 160GB.

Ilustración 8 Equipo PC Color Shop[43]



[43] Fotografía de la empresa Color Shop

Tabla 15 Valoración para activos Color Shop[44]

Fuente: Tomado de UNAD. Valoración de los activos

ESCALA DE VALORACIÓN CUALITATIVA Y CUANTITATIVA PARA LOS ACTIVOS		
Valoración Cualitativa	Escala de valor cuantitativo	Valor cuantitativo
Muy Alto (MA)	> $ 15.000.000	$ 16.000.000
Alto (A)	$ 15.000.000 <valor> $ 6.000.000	$ 7.500.000
Medio (M)	$ 6.000.000 <valor> $ 1.000.000	$ 3.000.000
Bajo (B)	$ 1.000.000 <valor> $ 100.000	$ 500.000
Muy Bajo (MB)	$ 100.000 <valor> $ 30.000	$ 50.000

Tabla 16 Criterio de Valoración de activos Color Shop[45]

Fuente: Tomado de seguridad informática. PILAR - Herramienta para análisis y gestión de riesgos

Valor	Criterio
10	Daño muy grave
7-9	Daño grave
4-6	Daño importante
1-3	Daño menor
0	Irrelevante

[44] UNAD. Valoración de los activos, op. cit, p.1.
[45] SEGURIDAD INFORMÁTICA. PILAR - Herramienta para Análisis y Gestión de Riesgos, op. cit, p.1.

Valoración de activos de acuerdo a la dimensiones de seguridad y criterios para activos

Tabla 17 Dimensiones de los riesgos Color Shop[46]

Fuente: Tomado de UNAD. Dimensiones de Seguridad

		Dimensiones				
Tipo	**Nombre de Activo**	**Confidencialidad ¿Qué daño**	**Integridad ¿Qué perjuicio causaría que**	**Disponibilidad ¿Qué perjuicio no causaría**	**Autenticidad ¿Qué perjuicio**	**Trazabilidad ¿Qué daño no causaría**
Activo de información	Datos de clientes, proveedores y personal (Archivos de Microsoft Excel)	[9][A]	[9][A]	[8][M]	[8][A]	
	Documentos Físicos (Libro contable, facturas)	[10][MA]	[1][MB]	[9][A]		
Software o aplicación	Sistema Operativo Windows 7 Home Edition licencias OEM	[6][M]	9][A]	[8][A]	9][A]	
	Office 2007 licencias OEM		9][A]	[6][M]	9][A]	
	Antivirus Microsoft Security Essentials	[8][A]	[8][A]	[8][A]		
Hardware	PC1 Computador de escritorio marca HP. Utilizado por el propietario de la empresa.	[9][A]	[9][A]	[6][M]	[6][M]	

[46] UNAD. Dimensiones de Seguridad, op. cit, p.1.

	PC2 Computador de escritorio marca HP. Utilizado por algunos de los empleados para informar procesos realizados.	[8][A]	[8][M]	[6][M]	[6][M]	
	Impresora multifuncional HP 1515 deskjet			[3][MB]		
	2 memorias USB de 16 GB	[8][A]	[8][A]	[6][M]	[6][M]	
Instalación	Cables del fluido eléctrico			[7][M]		
Personal	Empleados y propietario			[9][A]		
Otros	Sistema de video vigilancia Cctv	[9][A]		[9][A]		

Tabla 18 Dimensiones de valoración del impacto Color Shop[47]

Fuente: Tomado de Fuente: Tomado de introducción a la seguridad informática

Cod.	Nombre Dimensiones de valoración
[D]	Disponibilidad
[I]	Integridad de los datos
[C]	Confidencialidad de la información
[A]	Autenticidad
[T]	Trazabilidad

Tabla 19 Amenazas Color Shop[48]

Fuente: Tomado de UNAD. Identificación de amenazas

Cod.	Amenazas	Impacto
[N] Desastres Naturales		
[N.1]	Incendio	[D][I]
[N.2]	Inundación	[D][I]
[I] De origen industrial		
[I.5]	Avería de origen físico	[D]
[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
[I.9]	Interrupción de otros servicios o suministros esenciales	[D]
[E] Errores y fallos no intencionados		
[E.1]	Errores de los usuarios	[D][I][C]
[E.16]	Introducción de falsa información	[I]

[47] Mifsud, Elvira, op. cit, p.1.
[48] UNAD. Identificación de amenazas, op. cit, p.1.

[A] Ataques deliberados		
[A.11]	Acceso no autorizado	[D][I][C][A][T]
[A.15]	Modificación deliberada de la información	[I]
[A.16]	Introducción de falsa información	[I]
[A.18]	Destrucción de la información	[D][I]
[A.25]	Robo de equipos	[D][I][C][A][T]
[A.30]	Ingeniería social	[D][I][C][A][T]

Tabla 20 Escala de valoración de rango porcentual de impacto en los activos Color Shop[49]

Fuente: Tomado de UNAD. Valoración de amenazas

Impacto	**Valoración del impacto**
Muy Alto (MA)	100%
Alto (A)	75%
Medio (M)	50%
Bajo (B)	20%
Muy bajo (MB)	5%

[49] UNAD. Valoración de amenazas, op. cit, p.1.

Tabla 21 Escala de rango de frecuencia de amenazas Color Shop[50]

Fuente: Tomado de UNAD. Valoración de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Tabla 22 Valoración de las amenazas Color Shop[51]

Fuente: Tomado de UNAD. Valoración de amenazas

Cód.	Amenazas	Frecuencia	Impacto	Causas
[N] Desastres Naturales				
[N.1]	Incendio		100%	Acumulación de gases, tormentas eléctricas.
[N.2]	Inundación	5	50%	Lluvia
[I] De origen industrial				
[I.5]	Averías de origen físico	5	20%	Cortos circuitos, variación eléctrica, apagado incorrecto
[I.7]	Condiciones inadecuadas de temperatura o humedad	5	20%	Humedades en paredes
[I.9]	Interrupción de otros servicios o suministros	50	5%	Interrupción del fluido eléctrico o acceso a

[50] UNAD. Valoración de amenazas, op. cit, p.1.
[51] UNAD. Valoración de amenazas, op. cit, p.1.

	esenciales			internet
[E] Errores y fallos no intencionados				
[E.1]	Errores de los usuarios	50	5%	Falta de conocimiento en manejo de sistemas de información.
[E.16]	Introducción de falsa información	50	20%	Personal poco idóneo para ingresar o actualizar la información
[A] Ataques deliberados				
[A.11]	Acceso no autorizado	5	5%	Equipos sin controles para el acceso a los mismos
[A.15]	Modificación deliberada de la información	5	20%	Intención de daños a la empresa
[A.16]	Introducción de falsa información	50	20%	Intención de dañar y afectar la empresa o sus procesos
[A.25]	Robo de equipos	5	5%	Poca seguridad de la zona geográfica
[A.30]	Ingeniería social	5	5%	Desconocimiento o exceso de confianza de algunos empleados

10. TÉCNICAS DE TRABAJO – DISEÑO DE LOS INSTRUMENTOS

10.1. Diseño de la encuesta de auditoría para las Pymes

Para el desarrollo e implementación de la técnica de trabajo y diseño de los instrumentos de auditoría, se tomó como base la apreciación de cada uno de los dominios identificados, por lo tanto a partir del modelo de madurez de COBIT se estableció la clasificación para conceptuar cada dominio evaluado, y así identificar los riesgos asociados a cada proceso emparejando la calificación como:

- 0 = No se aplica la gestión de procesos[52]
- 1 = Los procesos son “ad hoc” y desorganizados[53]
- 2 = Los procesos siguen un cierto patrón[54]
- 3 = Los procesos están documentados y comunicados[55]
- 4 = Los procesos se monitorizan y se miden[56]
- 5 = Los procesos se mejoran y optimizan[57]

[52] Senén, J. Gestión de riesgo COBIT. [en línea]. [25 de febrero del 2015]. Disponible en: http://www.revistadintel.es/Revista1/DocsNum32/SISA/SISA32.pdf
[53] Ibíd., p. 2.
[54] Ibíd., p. 2.
[55] Ibíd., p. 2.
[56] Ibíd., p. 2.

Tabla 23 Auditoría de evaluación de la seguridad de la información Anexo 1

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son “ad hoc” y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A5: EVALUACIÓN QUE PERMITE EVALUAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN									
A5.1.	**Política de Seguridad de la Información**								
	Conjunto de políticas para la seguridad de la información								
1	¿Está definida la política de seguridad para la empresa?								
2	¿Se encuentran definidos los objetivos generales y el alcance de seguridad informática, como mecanismo para compartir información?								
3	¿Se tiene la estructura necesaria para establecer los objetivos de control, evaluando los riesgos?								
4	¿Se tiene la estructura necesaria para establecer la gestión de								

[57] Ibíd., p. 2.

	los riesgos?								
5	¿Se realizan capacitaciones constantes sobre las vulnerabilidades, riesgos y amenazas que tiene una organización?								
	Revisión de las políticas para la seguridad de la información.								
1	¿Se realizan acciones preventivas y correctivas?								
2	¿Se realizan revisiones periódicas de la política de seguridad?								
3	¿Los incidentes de seguridad se reporta?								
4	¿Se realizan revisiones periódicas de la política de seguridad?								
OBSERVACIONES:									

Tabla 24 Auditoría de evaluación de la seguridad de la información Anexo 2

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A6: EVALUACIÓN QUE PERMITE EVALUAR LOS ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN									
A6.1.	**Organización interna**								
	Asignación de responsabilidades para la seguridad de la información								
1	¿Documentar las metas de seguridad, verificando que satisface los requisitos de la empresa?								
2	¿Revisar y probar la política de seguridad de la información?								
3	¿Definir las iniciativas de seguridad?								
4	¿Proporciona los recursos requeridos para la seguridad de la información?								
5	¿Se asignan funciones conforme a las necesidades de la información?								
6	¿Se asignan las responsabilidades a								

	cada proceso de seguridad?								
7	¿Se documentan los procesos de asignación y seguridad?								
	Segregación de tareas								
1	¿Los activos informáticos se encuentran definidos claramente?								
2	¿Se garantizan las actividades de seguridad, siguiendo la política de seguridad?								
3	¿Se identifican los cambios, cuando existen amenazas?								
4	¿Se evalúan y coordinan los controles de seguridad?								
	Seguridad de la información en la gestión de proyectos								
1	¿La dirección se compromete con la seguridad de la información?								
2	¿Autorización por la dirección para la inversión de recursos, tiempos y formaciones?								
3	¿Existen los procedimientos documentados para contactar a las								

	autoridades competentes?								
4	¿Existen los procedimientos documentados para contactar a las entidades públicas?								
5	¿Existen los procedimientos documentados para contactar a las empresas proveedoras de telecomunicaciones?								
A6.2.	**Dispositivos para movilidad y teletrabajo**								
	Política de uso de dispositivos para movilidad								
1	¿Se tiene definida la política de seguridad para dispositivos móviles?								
2	¿Los controles aseguran la protección de los canales de comunicación?								
3	¿Los controles aseguran la protección contra código malicioso?								
4	¿Los controles aseguran la disponibilidad, integridad y								

	confidencialidad de la información?								
	Teletrabajo								
1	¿Se tiene la estructura clara para la presentación de informes?								
2	¿Se cuenta con unos procesos específicos para la gestión de cambio?								
3	¿La política de acceso, cuenta con los módulos permitidos para la identificación de usuario?								
4	¿Se cuenta con los privilegios de acceso?								
OBSERVACIONES:									

Tabla 25 Auditoría de evaluación de la seguridad de la información Anexo 3

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A7: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS									
A7.2.	**Seguridad en el desempeño de las funciones del empleo**								
	Responsabilidades de gestión								
1	¿Se tienen las directrices sobre las funciones de seguridad en el sistema de información?								
2	¿Se poseen las habilidades y calificaciones apropiadas?								
3	¿Logran un grado de concientización sobre la seguridad dentro de la organización?								
4	¿Están de acuerdo con los términos y las condiciones laborales?								
	Concienciación, educación y capacitación en seguridad de la información								

1	¿Se utiliza una formación en el uso correcto de los servicios de procesamiento de información?								
2	¿Se realizan capacitaciones sobre las amenazas, riesgos y vulnerabilidades?								
3	¿Se establecen los procesos de formación y concientización, diseñado para presentar las políticas de seguridad de la organización?								
OBSERVACIONES:									

Tabla 26 Auditoría de evaluación de la seguridad de la información Anexo 4

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A8: EVALUACIÓN QUE PERMITE EVALUAR LA GESTIÓN DE ACTIVOS									
A8.1.	**Responsabilidad sobre los activos**								
	Inventario de activos								
1	¿Se establece un inventario de activos informáticos por categoría?								
2	¿Se incluyen los requisitos para mantener seguro los activos informáticos?								
	Propiedad de los activos								
1	¿Los activos informáticos mantienen un código de ingreso a la organización, cada vez que se adquiere uno nuevo?								
2	¿Se clasifican los activos, conforme a sus características?								
3	¿Los activos se								

	clasifican por niveles?								
	Uso aceptable de los activos								
1	¿Se informa a los empleados el uso de los activos?								
	Devolución de activos								
1	¿Existe un proceso de terminación para incluir la devolución del software?								
2	¿Existe un proceso de terminación para incluir la devolución de los documentos?								
3	¿Existe un proceso de terminación para incluir la devolución de los equipos móviles?								
4	¿Existe un proceso de terminación para incluir la devolución de los equipos de cómputo?								
5	¿Existe un procedimiento que garantice la transferencia de información al finalizar su contratación?								
A8.2.	**Clasificación de la información**								

	Directrices de clasificación								
1	¿Se tienen las directrices sobre cómo se clasifican los activos informáticos?								
2	¿Existe la clasificación de seguridad por niveles?								
	Etiquetado y manipulado de la información								
1	¿Se capacita sobre cómo se debe enviar, y manipular las bases de información confidencial?								
2	¿Existe una marca para identificar las fuentes de información?								
	Manipulación de activos								
1	¿Los activos informáticos poseen una documentación adecuada?								
2	¿Existen manuales de configuración de los activos informáticos?								

Tabla 27 Auditoría de evaluación de la seguridad de la información Anexo 5

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A9: EVALUACIÓN QUE PERMITE EVALUAR EL CONTROL DE ACCESO									
A9.1.	**Requerimientos de negocio para el control de acceso**								
	Política de control de acceso								
1	¿Se tiene implementado la política de control de acceso conforme a la política de seguridad?								
2	¿Se atiende la legislación vigente, conforme a las normas actuales?								
3	¿Identificar la información relacionada con las aplicaciones?								
4	¿Identificar los riesgos asociados a la información?								
A9.2.	**Gestión de acceso de usuario**								
	Gestión de altas/bajas en el registro de usuarios								

1	¿Se establecen los repositorios donde se registran los usuarios que ingresan al sistema operativo?								
2	¿Se establecen los contadores para identificar cuantas sesiones están abiertas por usuario?								
3	¿Se verifica el nivel de acceso otorgado a cada usuario periódicamente?								
4	¿Se verifica que el usuario tenga autorización del dueño del sistema para el uso de la información?								
	Gestión de los derechos de acceso con privilegios especiales								
1	¿Se establece para cada tipo de activo los privilegios otorgados de acuerdo a la evaluación de riesgos asociada?								
2	¿Se promueve el desarrollo de rutinas del sistema para evitar la necesidad de otorgar privilegios innecesarios?								
A9.3.	**Responsabilidades de usuario**								
	Uso de información confidencial para la								

	autenticación								
1	¿Está definida la políticas de seguridad para usuarios de los equipos?								
2	¿Las contraseñas predeterminadas por el proveedor se cambian inmediatamente después de la instalación de los sistemas o del software?								
3	¿Las contraseñas temporales se suministran de forma segura a los usuarios?								
A9.4.	**Control de acceso a sistemas operativo y aplicaciones**								
	Restricción del acceso a la información								
1	¿El control de acceso se realiza de acuerdo a la política del control de accesos?								
2	¿Se controla los derechos de acceso de otras aplicaciones?								
3	¿Se garantiza que los datos de salida de los sistemas de aplicación que manejan información sensible solo contienen la información pertinente								

	para el uso de la salida y que se envía únicamente a terminales o sitios autorizados.								
	Procedimientos seguros de inicio de sesión								
1	¿Se establece la política de autenticación a los equipos, con contraseñas personales y perfiles definidos?								
2	¿Se valida la información de registro con la base de datos para el acceso?								
3	¿Los controles de acceso se aplican al personal de soporte técnico?								
4	¿Los controles de acceso se aplican a los operadores?								
5	¿Los controles de acceso se aplican a los administradores de red?								
6	¿Los controles de acceso se aplican a los programadores de sistemas?								
7	¿Los controles de acceso se aplican a los administradores de bases de datos?								

	Uso de herramientas de administración de sistemas								
1	¿Se regula la instalación de software en los equipos personales?								
2	¿Se lleva un registro de todo uso de las utilidades del sistema?								
3	¿Se utilizan procedimientos de identificación, autenticación y autorización para las utilidades del sistema?								
OBSERVACIONES:									

Tabla 28 Auditoría de evaluación de la seguridad de la información Anexo 6

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A10: EVALUACIÓN QUE PERMITE EVALUAR EL CIFRADO									
A10.1.	**Controles criptográficos**								
	Política de uso de los controles criptográficos								
1	¿Se establece la política de cifrado para las claves públicas y privadas en el manejo de información confidencial?								
2	¿Se verifica periódicamente la política de cifrado conforme a la norma actual?								
	Gestión de claves								
1	¿Se valida las metodologías para cifrar las claves y uso en los mensajes emitidos?								

2	¿Se controla los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?								
3	¿Se asigna los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?								
OBSERVACIONES:									

Tabla 29 Auditoría de evaluación de la seguridad de la información Anexo 7

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A11: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD FÍSICA Y DEL ENTORNO									
A11.1.	**Áreas seguras**								
	Controles físicos de entrada								
1	¿Se definen los controles físicos para cada activo?								
2	¿Se definen los controles técnicos para cada activo?								
3	¿Se definen los controles organizacionales para cada activo?								
4	¿Se dicta la política de control de accesos conforme al SGSI?								
	Seguridad de oficinas, despachos y recursos								
1	¿Se dicta la política de uso de las oficinas acorde a la política de gestión								

	de acceso y del SGSI?								
2	¿Se establece el reglamento sobre las actividades y procesos informáticos?								
3	¿Se establece las normas sobre las actividades y procesos informáticos?								
	Protección contra las amenazas externas y ambientales								
1	¿Definir un plan de respuesta para cada tipo de efecto que pudiera causar amenaza externa?								
2	¿Se suministran equipos apropiados contra las amenazas ambientales y son ubicados adecuadamente?								
A11.2.	**Seguridad de los equipos**								
	Emplazamiento y protección de equipos								
1	¿Monitorear el uso de equipos personales a través								

	de la política de uso de equipos personales?								
2	¿Los equipos están distribuidos de tal forma que no pueda acceder cualquier usuario?								
3	¿Los elementos que requieren protección especial están aislados?								
	Instalaciones de suministro								
1	¿Se establece el plan de continuidad para este tipo de riesgos?								
2	¿Se instalan las UPS para suministrar energía a los equipos de cómputo?								
3	¿Las UPS y plantas de energía son revisadas con frecuencia?								
	Seguridad del cableado								
1	¿El cableado se encuentre canalizado por conductos específicos del suelo técnico instalado en las oficinas?								

2	¿Existe un control de acceso en los cuartos de cableado que soportan los sistemas críticos?								
3	¿Tienen rótulos de equipos y de cables claramente identificables para minimizar los errores en el manejo?								
	Mantenimiento de los equipos								
1	¿Se realiza el mantenimiento acorde a los procesos de gestión de activos?								
2	¿La información confidencial es retirada periódicamente de los equipos de cómputo?								
3	¿El personal de mantenimiento es suficientemente confiable?								
4	¿Se lleva un registro de todas las fallas reales y sospechosas?								
OBSERVACIONES:									

Tabla 30 Auditoría de evaluación de la seguridad de la información Anexo 8

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A12: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LA OPERATIVA									
A12.1.	**Protección contra código malicioso**								
	Controles contra el código malicioso								
1	¿Se establece la política de seguridad de equipos personales en la que se previene el uso de programas no autorizados por la empresa?								
2	¿Se regula el uso de software antivirus y su actualización?								
3	¿Se lleva a cabo revisiones mensuales sobre el contenido del software y los datos que soportan los procesos críticos del negocio?								
4	¿Se investiga la aparición de archivos o códigos no								

	autorizados por el desarrollador del software?								
A12.2.	**Copias de seguridad**								
	Copias de seguridad de la información								
1	¿Se realizan copias de seguridad de manera periódica sobre la información registrada en las oficinas – Backup?								
2	¿Las copias de seguridad se almacenan en un sitio seguro?								
3	¿Se puede consultar de las copias de seguridad los archivos y la información está completa?								
A12.4.	**Registro de actividad y supervisión**								
	Registro y gestión de eventos de actividad								
1	¿Se monitorea los cambios de configuración del sistema?								
2	¿Supervisar los controles definidos al								

	uso de equipos personales?								
	Registros de actividad del administrador y operador del sistema								
1	¿Se monitorea el ingreso de usuarios a las diferentes aplicaciones?								
2	¿Se registran las alertas o fallas del sistema, como mensajes de consola?								
A12.6.	**Gestión de las vulnerabilidades técnicas**								
	Gestión de las vulnerabilidades técnicas								
1	¿Se establece el cuadro de control que evidencie los riesgos asociados a la organización?								
	Restricciones en la instalación de sistema operativo (S.O.)								
1	¿Se tiene instalado un corta fuego en el sistema operativo?								
2	¿Se asignan privilegios a los								

	usuarios conforme a su perfil o cargo?								
A12.7.	**Consideraciones de las auditorías de los sistemas de información**								
	Controles de auditoría de los sistemas de información								
1	¿Se realiza mensualmente y trimestralmente una auditoría interna por los procesos de seguridad que se han implementado en la organización?								
OBSERVACIONES:									

Tabla 31 Auditoría de evaluación de la seguridad de la información Anexo 9

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A13: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LAS TELECOMUNICACIONES									
A13.2.	**Intercambio de información**								
	Mensajería electrónica								
1	¿Se establecen los protocolos para enviar la información por los canales de comunicación?								
2	¿Se verifica los canales de comunicación mensualmente identificando los canales de transmisión por el internet?								
	Acuerdos de confidencialidad y secreto								
1	¿Se documenta donde se establecen los acuerdos de confidencialidad?								

2	¿Se documenta donde se establecen las políticas de confidencialidad?								
3	¿Se monitorea el cumplimiento de los acuerdos?								
OBSERVACIONES:									

Tabla 32 Auditoría de evaluación de la seguridad de la información Anexo 10

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A16: EVALUACIÓN QUE PERMITE EVALUAR LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN									
A16.1.	**Gestión de incidentes de seguridad de la información y mejoras**								
	Aprendizaje de los incidentes de seguridad de la información								
1	¿Se verifican las amenazas, riesgos y vulnerabilidades asociados a la empresa?								
2	¿De acuerdo a las amenazas, riesgos y vulnerabilidades se debe establecer una propuesta para disminuir el riesgo?								
A14.3.	**Datos de prueba**								
	Protección de los datos utilizados en pruebas								

1	¿Se realizan pruebas a los activos informáticos, estableciendo las mejores alternativas para mitigar los riesgos?								
2	¿Se realizan pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial?								
OBSERVACIONES:									

Tabla 33 Auditoría de evaluación de la seguridad de la información Anexo 11

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A14: EVALUACIÓN QUE PERMITE EVALUAR LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN									
A16.1.	**Gestión de incidentes de seguridad de la información y mejoras**								
	Aprendizaje de los incidentes de seguridad de la información								
	¿Se establecen procesos de resolución de incidentes de seguridad de la información?								
	¿Se evalúan los incidentes de seguridad?								
OBSERVACIONES:									

Tabla 34 Auditoría de evaluación de la seguridad de la información Anexo 12

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son “ad hoc” y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A17: EVALUACIÓN QUE PERMITE EVALUAR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO									
A17.1.	**Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**								
	Planificación de la continuidad de la seguridad de la información								
1	¿Se define el proceso de gestión de continuidad del negocio?								
2	¿Se define las directrices de continuidad del negocio de conformidad con la política de seguridad de la información?								
3	¿Se garantiza la seguridad del personal, la								

	protección de los servicios y procesos de información?								
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información								
1	¿Se define los planes de continuidad del negocio de acuerdo al orden de prioridades?								
2	¿Se implementa los planes de continuidad del negocio de acuerdo al orden de prioridades?								
OBSERVACIONES:									

Tabla 35 Auditoría de evaluación de la seguridad de la información Anexo 13

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	**1 = Los procesos son "ad hoc" y desorganizados**	**2 = Los procesos siguen un cierto patrón**	**3 = Los procesos están documentados y comunicados**	**4 = Los procesos se monitorizan y se miden**	**5 = Los procesos se mejoran y optimizan**	**Verbal**	**Documental**
A18: EVALUACIÓN QUE PERMITE EVALUAR EL CUMPLIMIENTO									
A18.1.	**Cumplimiento de los requisitos legales y contractuales**								
	Identificación de la legislación aplicable								
1	¿Se identifica la legislación aplicable para los procesos que intervienen en el manejo de la información?								
	Derechos de propiedad intelectual (DPI)								
1	¿Se identifica la legislación aplicable y los términos contractuales en las licencias utilizadas?								
2	¿Se hace un								

	inventario de software para garantizar la idoneidad de su uso?								
3	¿Se dictan políticas de cumplimiento?								
	Protección de los registros de la organización								
1	¿Se mantienen disponibles los documentos del Sistema de gestión de la seguridad informática - SGSI?								
2	¿Los documentos se mantienen editables para los usuarios autorizados?								
3	¿Se clasifica la información en función de su importancia?								
4	¿Se establecen copias de seguridad de la información relevante?								
5	¿Se protege la información física sensible?								
	Protección de datos y privacidad de la								

	información personal								
1	¿Se establece el documento de seguridad de conformidad con la legislación de protección de datos personales?								
A18.2.	**Revisiones de la seguridad de la información**								
	Cumplimiento de las políticas y normas de seguridad								
1	¿Se dicta y acuerda la política del sistema de gestión de la seguridad informática - SGSI?								
OBSERVACIONES:									

10.2. Análisis de la información recolectada

10.2.1. Análisis de resultados Guille Sport

En la investigación que se realizó, se puede determinar que un 80% de las personas son poco conocedores de los sistemas informáticos, de las consecuencias generadas del mal uso de estos y del impacto que genera en la empresa la alteración o pérdida de información relevante.

Se desconoce las normativas de derechos de autor y propiedad intelectual, en cuanto al software utilizado para el manejo de la información en los equipos de cómputo.

Se desestima casi en un 100% del personal, la importancia de mantener buenas prácticas en el manejo de los equipos y de la información allí almacenada, además de tener reglas claras y políticas establecidas para la manipulación de la misma información, por ende se estableció la siguiente tabla de vulnerabilidades, amenas y riesgos de la empresa.

Tabla 36 Descripción de las posibles vulnerabilidades, amenazas y riesgos Guille Sport

Cód.	Vulnerabilidad	Amenazas Ligadas	Riesgos Potenciales
Hardware			
V1	Control a dispositivos de almacenamiento externos	Virus informáticos, malware.	Mal funcionamiento de los sistemas, destrucción de sistemas operativos, aplicativos e información.
V2	Manipulación de los equipos sin control alguno	Ataques insiders	Alteración de archivos, registros, robo o destrucción de información, robo o destrucción de equipos de cómputo, fuga de información.
V3	Falta de equipos UPS's para contingencias	Cortes de energía o sobrecargas en los equipos.	Perdida de información, daños en los equipos, perdida de tiempos en los procesos y actividades del negocio.

Software			
V4	Software no licenciado	Virus informáticos, malware, utilización de exploit.	Mal funcionamiento de los sistemas, destrucción de sistemas operativos, aplicativos e información.
V5	Software con problemas de desarrollo	Ataques de Inyección SQL, información inconsistente	Modificación de información, robo de datos de los usuarios del sistema, bases de datos a merced del atacante.
V6	Sistemas sin restricciones de acceso	instalación de programas keylogger	Sustracción de información de la empresa o datos personales.
V7	Algunos equipos no tiene el sistema operativo actualizado	Utilización de exploit	Intrusión no autorizada en los equipos, modificación, borrado o robo de información, ataques de DOS, consecución de privilegios.
V8	Falta de control a las actualizaciones del proveedor	Utilización de exploit, propagación de código malicioso	Robo alteración y destrucción de datos, mal funcionamiento de los equipos y servicios.
Seguridad física			
V9	Instalaciones físicas sin medidas de seguridad	Intrusión de delincuencia común, saboteo al interior	Robo de equipos de cómputo, telecomunicaciones, papelería, archivos, elementos de almacenamiento de información, daño a la información y a los equipos que la contienen.
V10	Instalaciones con deficiencias en planes de contingencia ante desastres naturales o provocados.	Ataques deliberados a los equipos e instalaciones, desastres naturales.	Inundaciones, incendios, terremotos, tormentas, destrucción parcial o total de equipos y datos.
V11	Control de acceso físico a las oficinas no existente	Manipulación de información si control de acceso, ataques intencionados a los	Robo, destrucción, modificación o borrado de información, destrucción física de

		equipos, desastres provocados.	equipos, incendios.
V12	Instalaciones físicas con control ambiental inapropiado	Destrucción de los equipos, degradación o inutilización de los mismos.	Perdida de información, equipos o partes asociadas a su gestión.
Seguridad lógica			
V13	Control en el recambio y destrucción de medios de almacenamiento	Entrega de medios obsoletos o dañados a terceros sin la adecuada destrucción o proceso de borrado de información.	Sustracción de información sensible de la compañía a través de personas externas.
V14	Control de acceso deficiente o faltante	Suplantación de contenido	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios.
Redes de comunicaciones			
V15	Vulnerabilidades de los navegadores utilizados	Inyección de código SSI, ataques con código XSS	Alteración en el funcionamiento del código, programas y sitios, apropiación de información sin autorización.
V16	Uso de aplicaciones poco confiables para compartir archivos o para asistencia remota	Inyección SQL	Robo de información de bases de datos.
Personal			
V17	Falta de una política de seguridad clara	Ataques no intencionados, ingeniería social, phishing.	Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal.
V18	Personal inconforme en la compañía	Ataques insiders	Alteración de archivos, registros, robo o destrucción de información, robo o destrucción de equipos de cómputo, fuga de información.
V19	Usuarios con pocos conocimientos en	Ataques con ingeniería social	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de

	informática		usuarios.
V20	Falta de conciencia en los funcionarios para el uso de las tecnologías	Abuso de permisos, divulgación de contraseñas, instalación de software y complementos no autorizados.	Sustracción de información sensible de la compañía y los usuarios, daño en aplicativos, bases de datos y repositorios.
V21	Soportes técnicos con deficiencias en capacitación y experiencia	Dejar pasar instalaciones críticas en los equipos, como: Antivirus, Parches de seguridad o configuraciones seguras que causarían propagación de código malicioso o ingeniería social.	Sustracción de datos personales y su posterior uso en actividades delictivas, mal funcionamiento de los equipos, robo de información, o destrucción premeditada de la misma.

10.2.1.1. Evaluación de la auditoría para Guille Sport

A continuación se presentan los resultados de la visita a la empresa Guille Sport aplicando el instrumento de auditoría frente a la calificación de los procesos:

Ilustración 9 Política de seguridad de la información Guille Sport

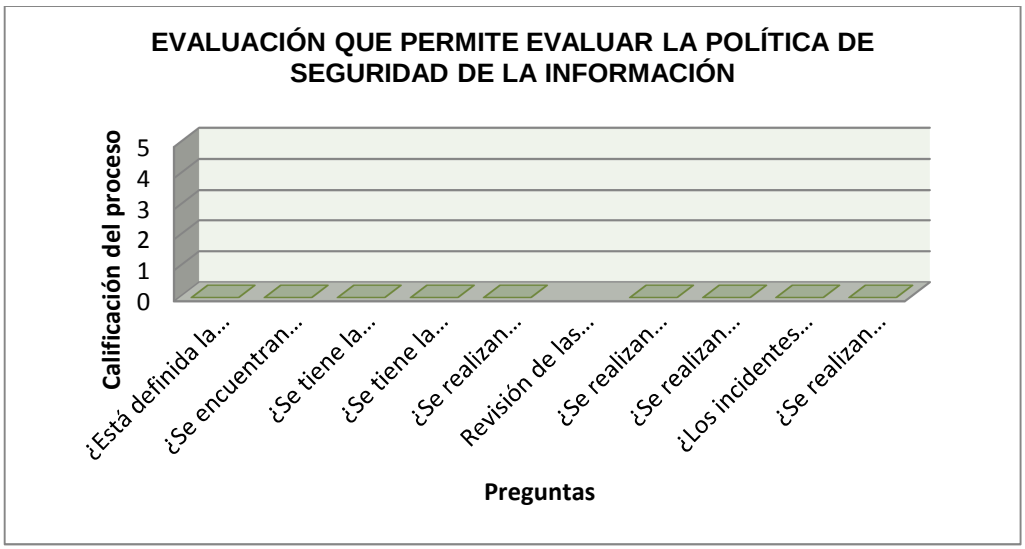


Ilustración 10 Aspectos organizativos de la seguridad de la información Guille Sport

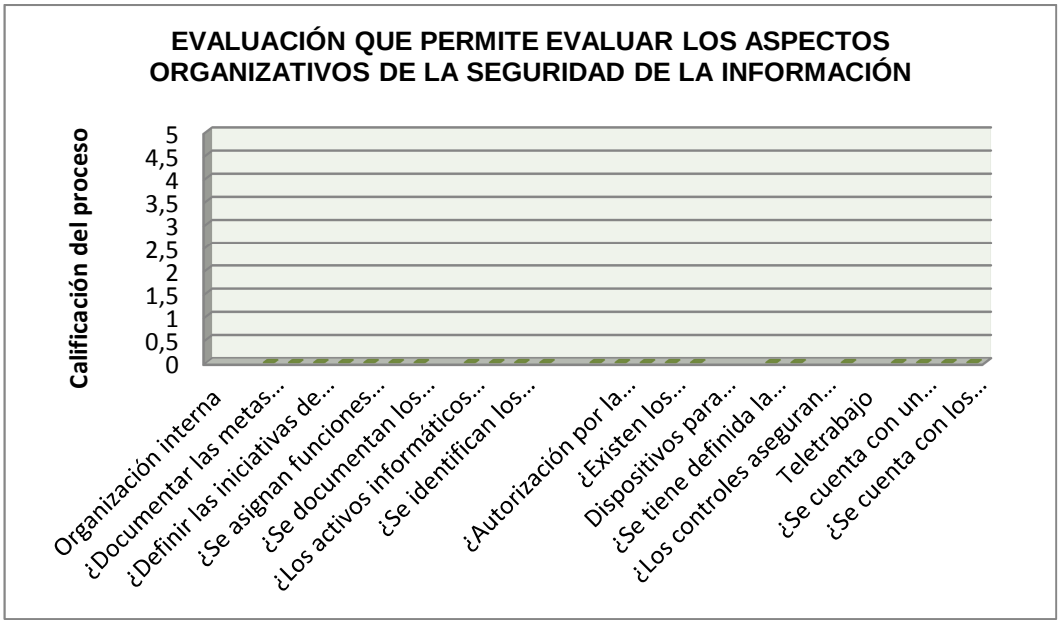


Ilustración 11 Seguridad ligada a los recursos humanos Guille Sport

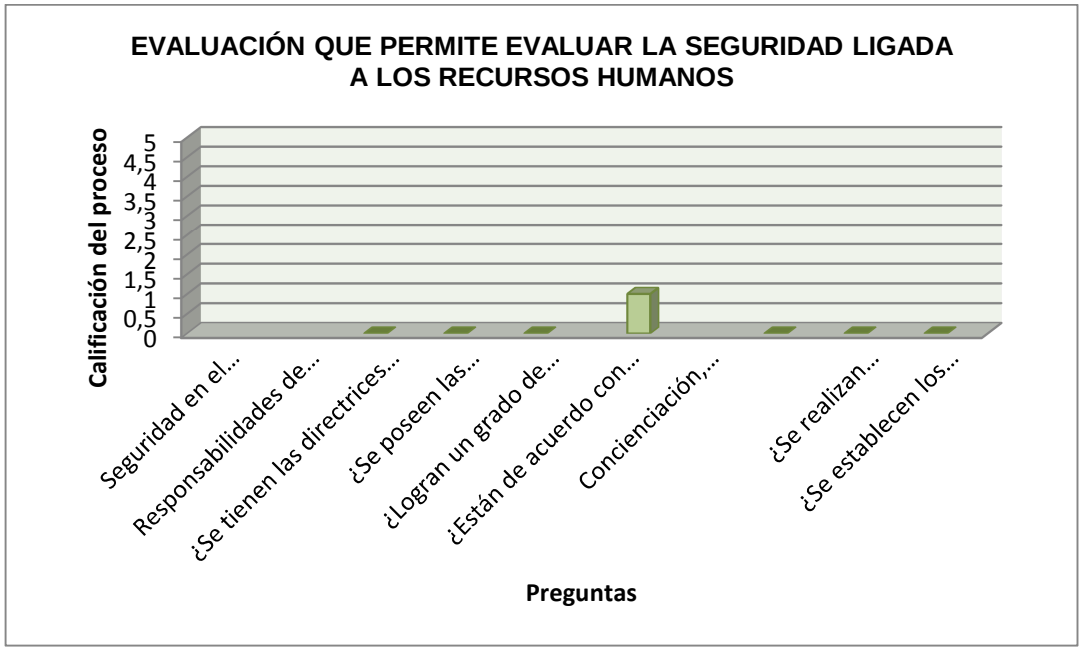


Ilustración 12 Gestión de activos Guille Sport

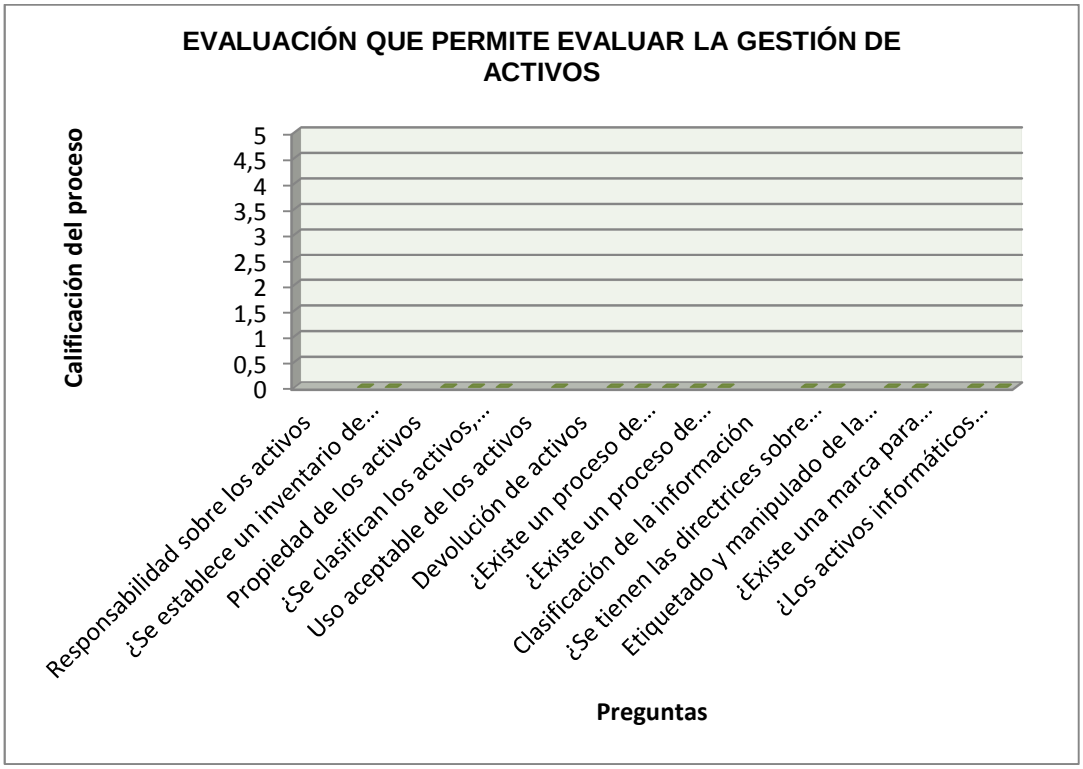


Ilustración 13 Control de acceso Guille Sport

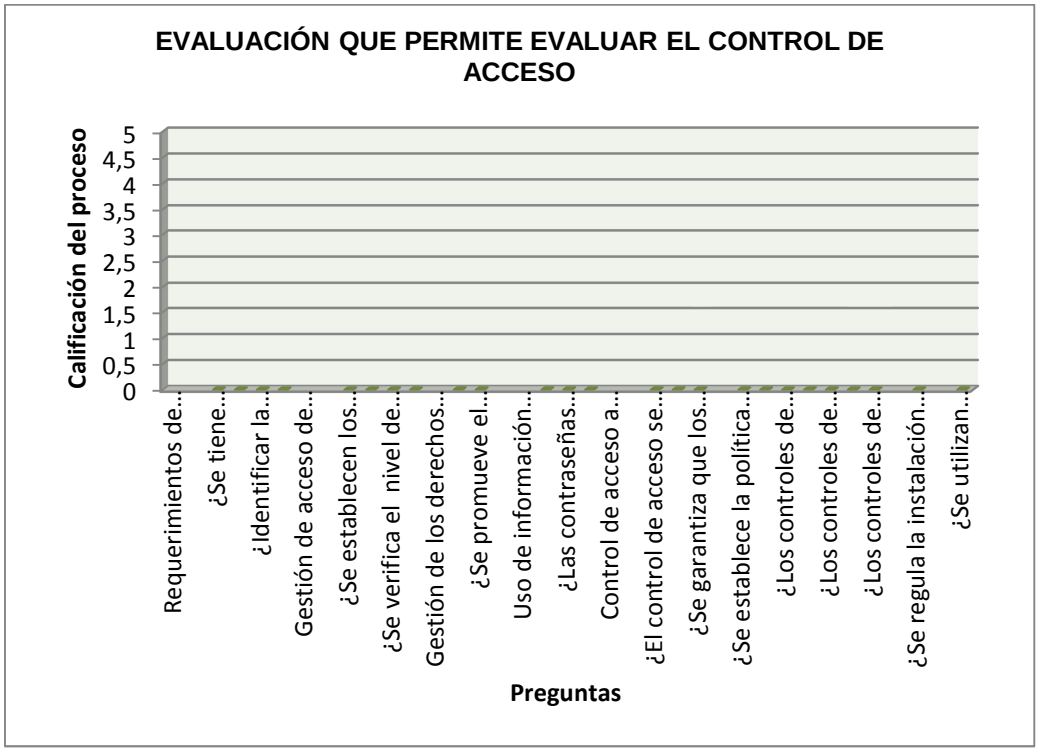


Ilustración 14 Cifrado Guille Sport

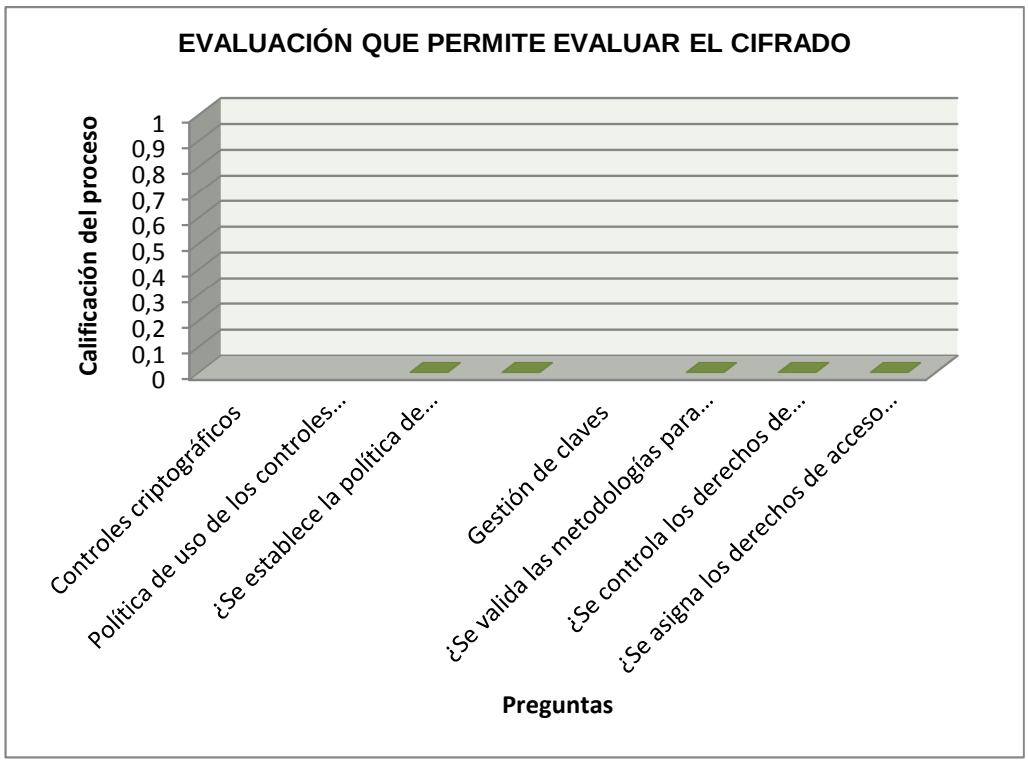


Ilustración 15 Seguridad física y del entorno Guille Sport

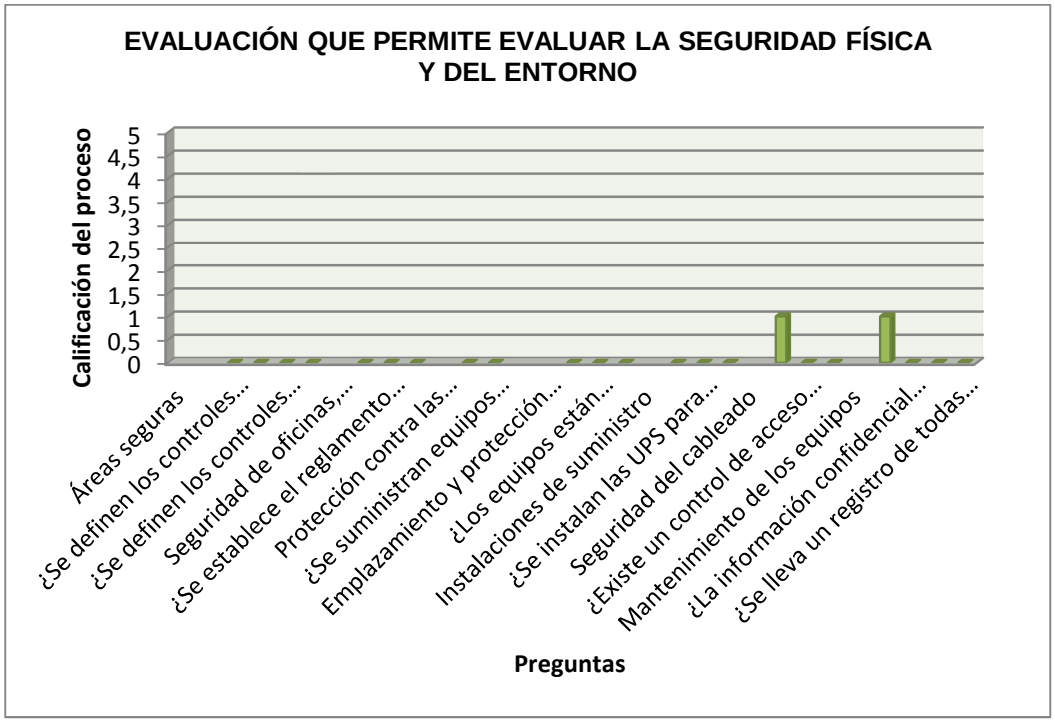


Ilustración 16 Seguridad en la operativa Guille Sport

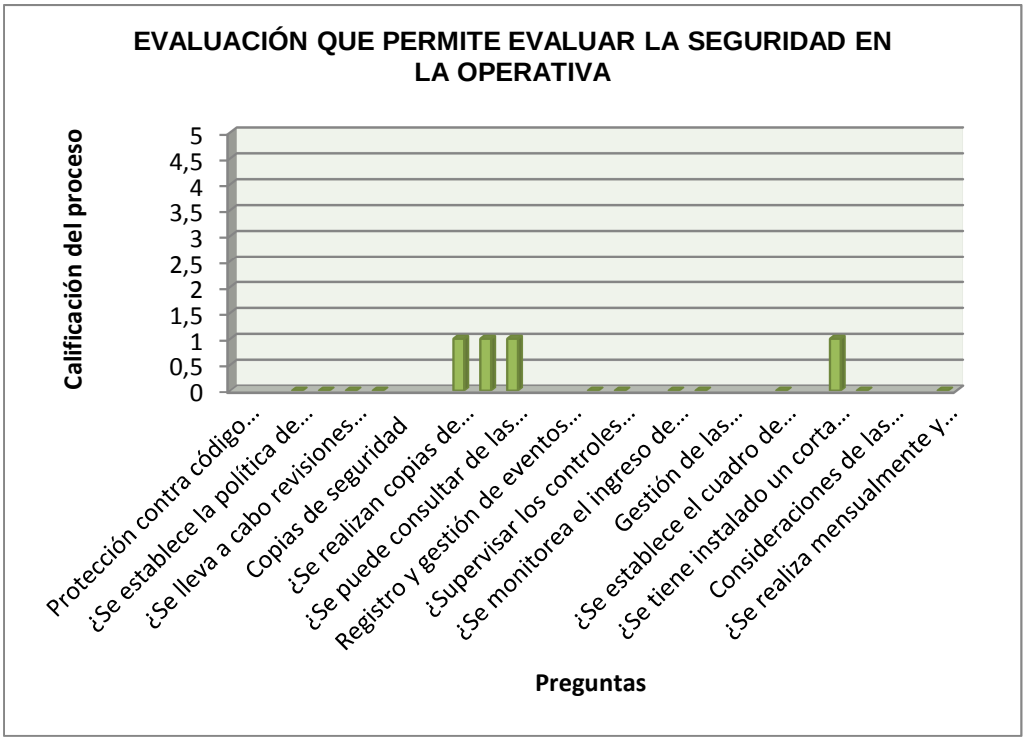


Ilustración 17 Seguridad en las telecomunicaciones Guille Sport

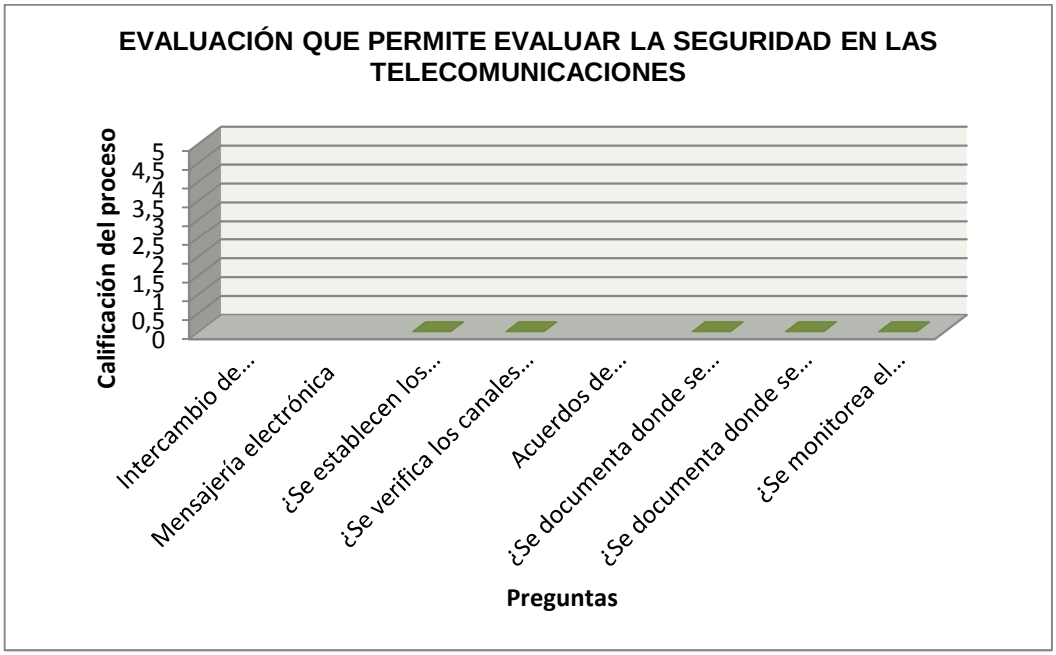


Ilustración 18 Gestión de incidentes en la seguridad de la información Guille Sport

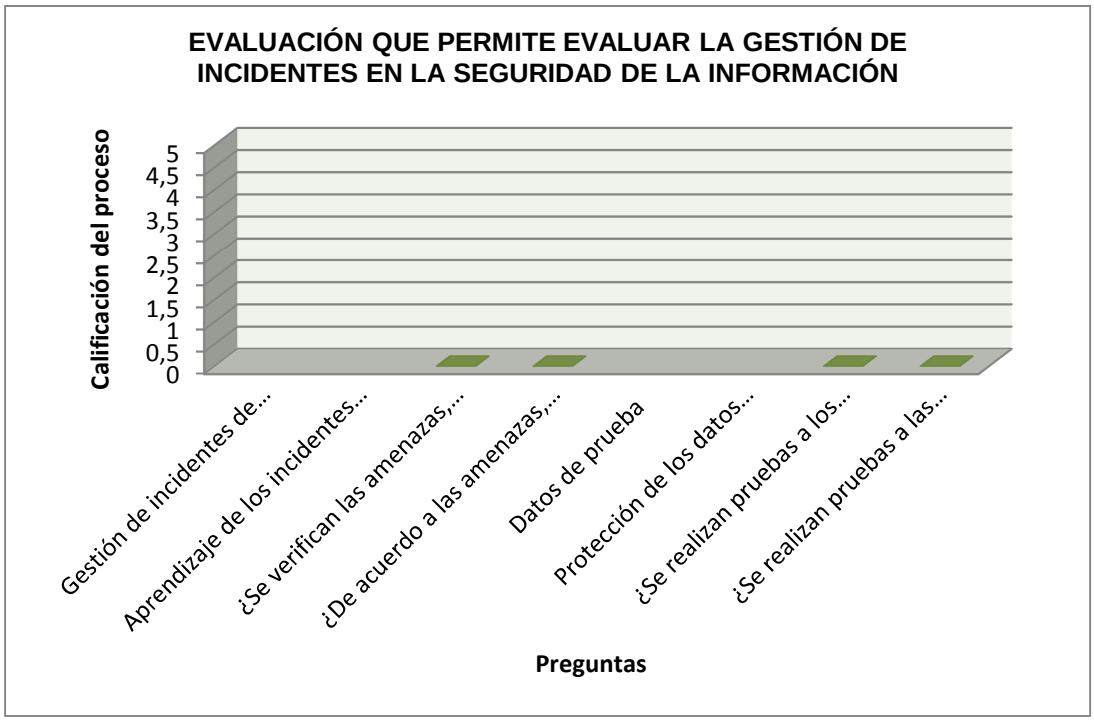


Ilustración 19 Adquisición, desarrollo y mantenimiento de los sistemas de información Guille Sport

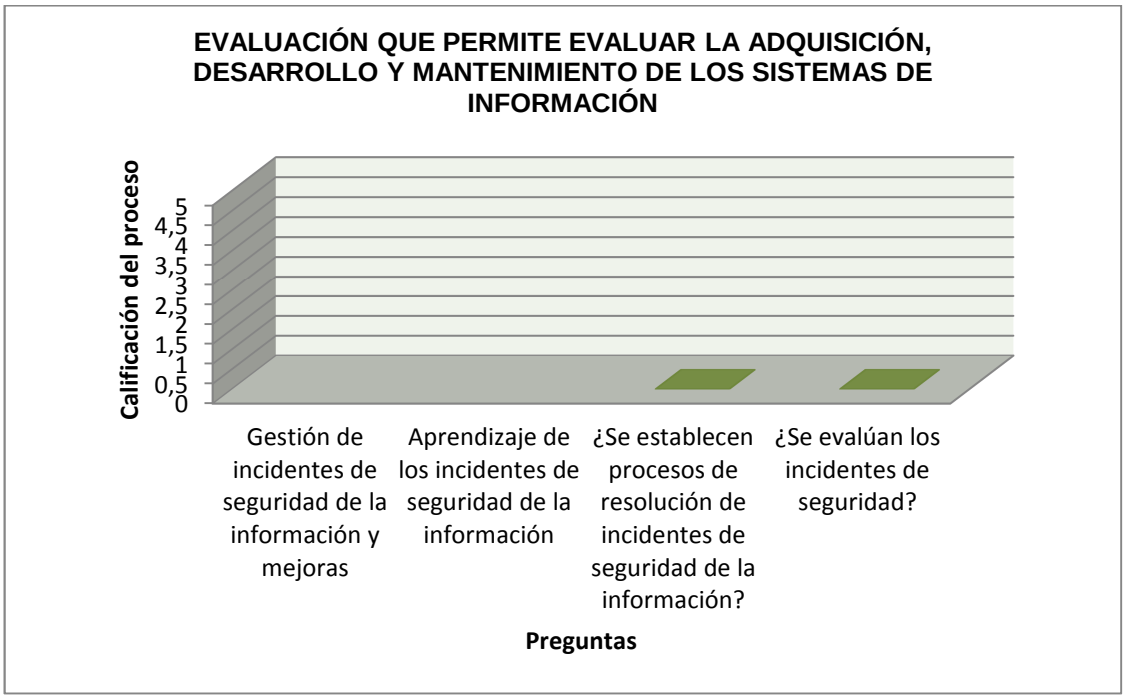


Ilustración 20 Aspectos de seguridad de la información en la gestión de la continuidad del negocio Guille Sport

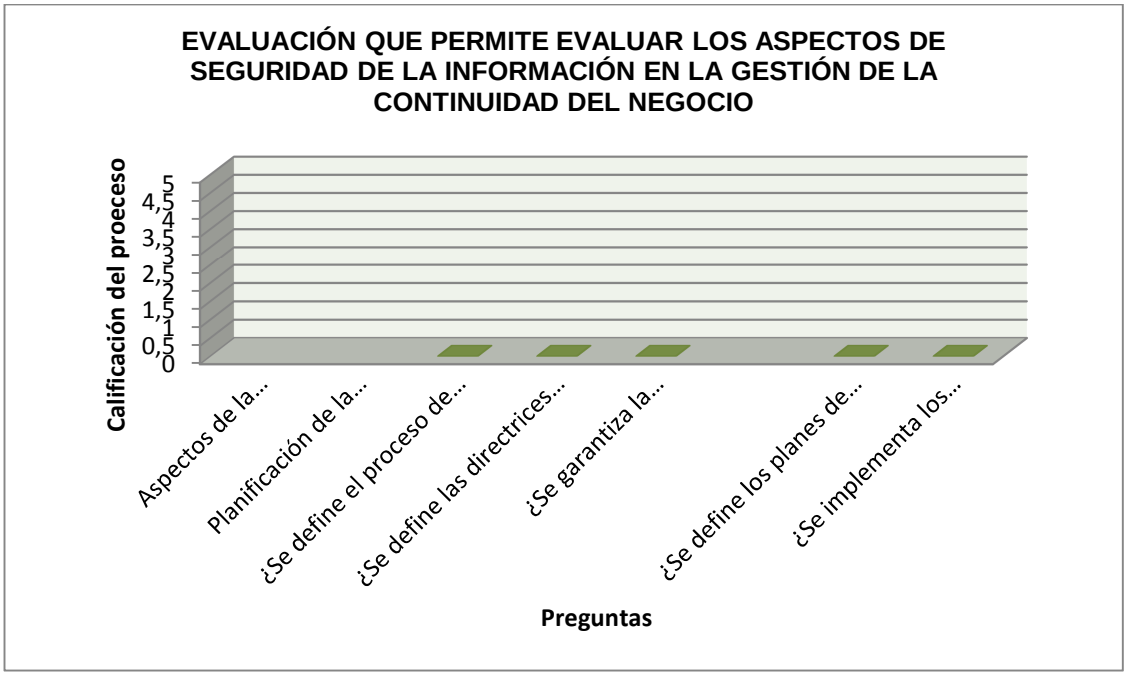
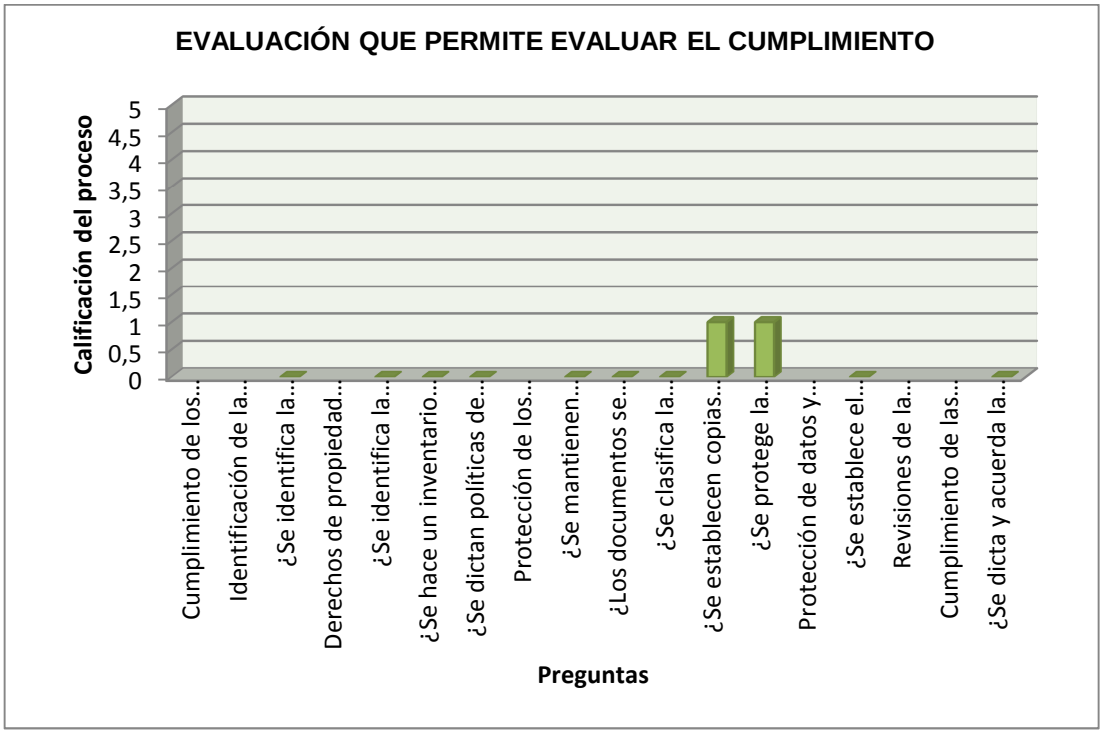


Ilustración 21 Cumplimiento Guille Sport



10.2.2. Análisis de resultados Color Shop

En la investigación realizada, se puede visualizar y evidenciar casi en un 100% la falta de conocimiento del personal en temas relacionados con la seguridad de la información, la infraestructura utilizada para la manipulación de la misma y el compromiso con sus empresas para mantener la integridad, disponibilidad y confidencialidad de esta.

De igual manera se nota la inexistencia de alguna política de seguridad de la información, procedimientos que permitan tener control adecuado de los procesos que tienen correlación con los datos y los elementos que con estos interactúan.

De este mismo modo casi el 100% de la población de estas empresas considera un costo alto e innecesario, la inversión en proyectos enmarcados en la seguridad de la información, por ende se estableció la siguiente tabla de vulnerabilidades, amenas y riesgos de la empresa.

Tabla 37 Descripción de las posibles vulnerabilidades, amenazas y riesgos Color Shop

Cód.	Vulnerabilidad	Amenazas Ligadas	Riesgos Potenciales
Hardware			
V1	Control a dispositivos de almacenamiento externos	Virus informáticos, malware.	Mal funcionamiento de los sistemas, destrucción de sistemas operativos, aplicativos e información.
V2	Manipulación de los equipos sin control alguno	Ataques insiders	Alteración de archivos, registros, robo o destrucción de información, robo o destrucción de equipos de cómputo, fuga de información.
V3	Falta de equipos UPS's para contingencias	Cortes de energía o sobrecargas en los equipos.	Perdida de información, daños en los equipos, perdida de tiempos en los procesos y actividades del negocio.

Software			
V4	Software con problemas de desarrollo	Ataques de Inyección SQL, información inconsistente	Modificación de información, robo de datos de los usuarios del sistema, bases de datos a merced del atacante.
V5	Sistemas sin restricciones de acceso	instalación de programas keylogger	Sustracción de información de la empresa o datos personales.
V6	Falta de control a las actualizaciones del proveedor	Utilización de exploit, propagación de código malicioso	Robo alteración y destrucción de datos, mal funcionamiento de los equipos y servicios.
Seguridad física			
V7	Instalaciones físicas con medidas de seguridad deficientes.	Intrusión de delincuencia común, saboteo al interior	Robo de equipos de cómputo, telecomunicaciones, papelería, archivos, elementos de almacenamiento de información, daño a la información y a los equipos que la contienen.
V8	Instalaciones con deficiencias en planes de contingencia ante desastres naturales o provocados.	Ataques deliberados a los equipos e instalaciones, desastres naturales.	Inundaciones, incendios, terremotos, tormentas, destrucción parcial o total de equipos y datos.
V9	Control de acceso físico a las oficinas no existente	Manipulación de información si control de acceso, ataques intencionados a los equipos, desastres provocados.	Robo, destrucción, modificación o borrado de información, destrucción física de equipos, incendios.
V10	Instalaciones físicas con control ambiental inapropiado	Destrucción de los equipos, degradación o inutilización de los mismos.	Perdida de información, equipos o partes asociadas a su gestión.

Seguridad lógica			
V11	Control en el recambio y destrucción de medios de almacenamiento	Entrega de medios obsoletos o dañados a terceros sin la adecuada destrucción o proceso de borrado de información.	Sustracción de información sensible de la compañía a través de personas externas.
V12	Control de acceso deficiente o faltante	Suplantación de contenido	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios.
Redes de comunicaciones			
V13	Vulnerabilidades de los navegadores utilizados	Inyección de código SSI, ataques con código XSS	Alteración en el funcionamiento del código, programas y sitios, apropiación de información sin autorización.
V14	Uso de aplicaciones poco confiables para compartir archivos o para asistencia remota	Inyección SQL	Robo de información de bases de datos.
Personal			
V15	Falta de una política de seguridad clara	Ataques no intencionados, ingeniería social, phishing.	Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal.
V16	Personal inconforme en la compañía	Ataques insiders	Alteración de archivos, registros, robo o destrucción de información, robo o destrucción de equipos de cómputo, fuga de información.
V17	Usuarios con pocos conocimientos en informática	Ataques con ingeniería social	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios.

V18	Falta de conciencia en los funcionarios para el uso de las tecnologías	Abuso de permisos, divulgación de contraseñas, instalación de software y complementos no autorizados.	Sustracción de información sensible de la compañía y los usuarios, daño en aplicativos, bases de datos y repositorios.
V19	Soportes técnicos con deficiencias en capacitación y experiencia	Dejar pasar instalaciones críticas en los equipos, como: Antivirus, Parches de seguridad o configuraciones seguras que causarían propagación de código malicioso o ingeniería social.	Sustracción de datos personales y su posterior uso en actividades delictivas, mal funcionamiento de los equipos, robo de información, o destrucción premeditada de la misma.

10.2.2.1. Evaluación de la auditoría para Color Shop

A continuación se presentan los resultados de la visita a la empresa Color Shop aplicando el instrumento de auditoría frente a la calificación de los procesos:

Ilustración 22 Política de seguridad de la información Color Shop

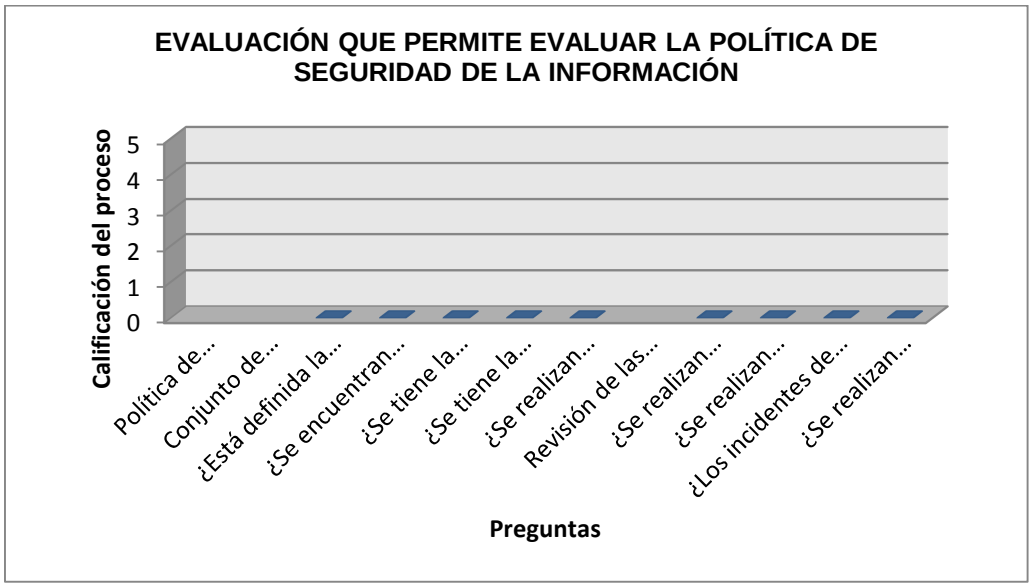


Ilustración 23 Aspectos organizativos de la seguridad de la información Color Shop

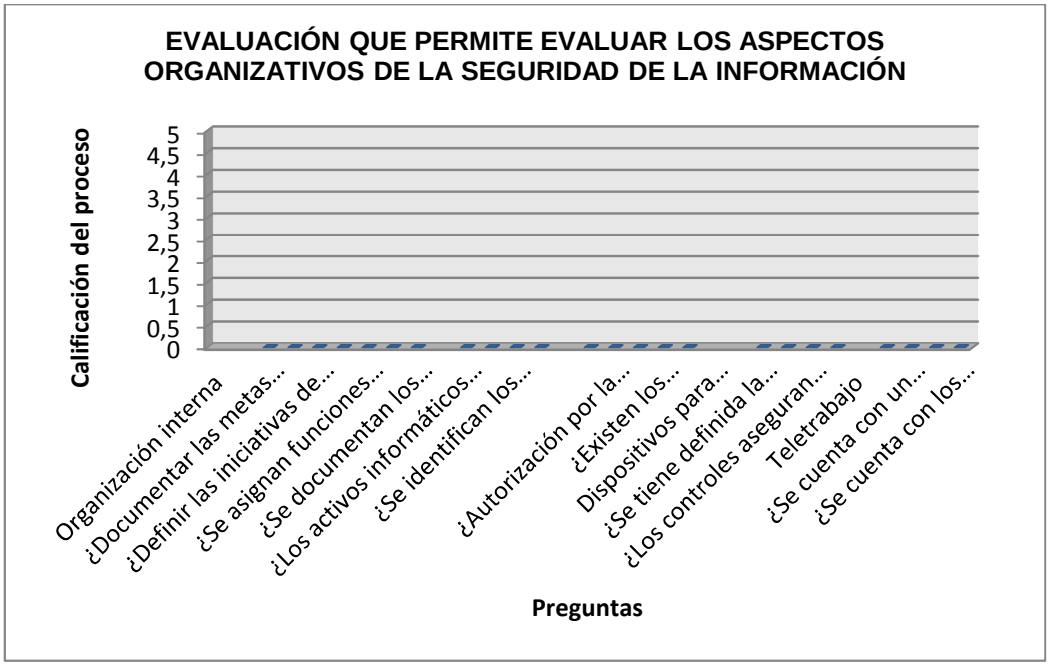


Ilustración 24 Seguridad ligada a los recursos humanos Color Shop

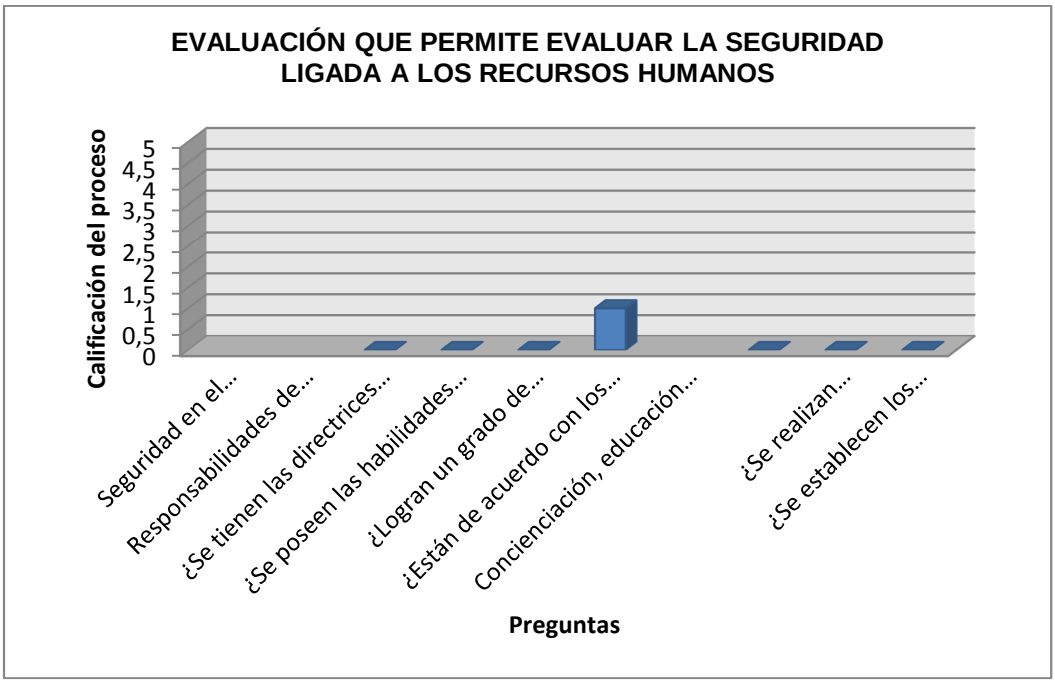


Ilustración 25 Gestión de activos Color Shop

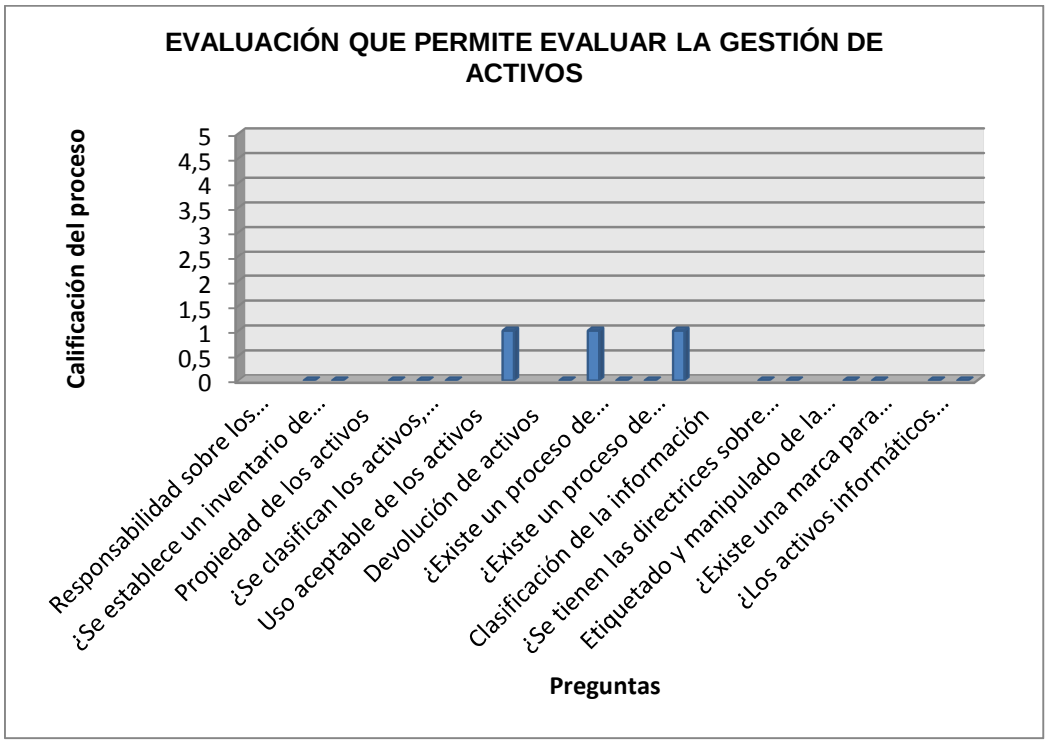


Ilustración 26 Control de acceso Color Shop

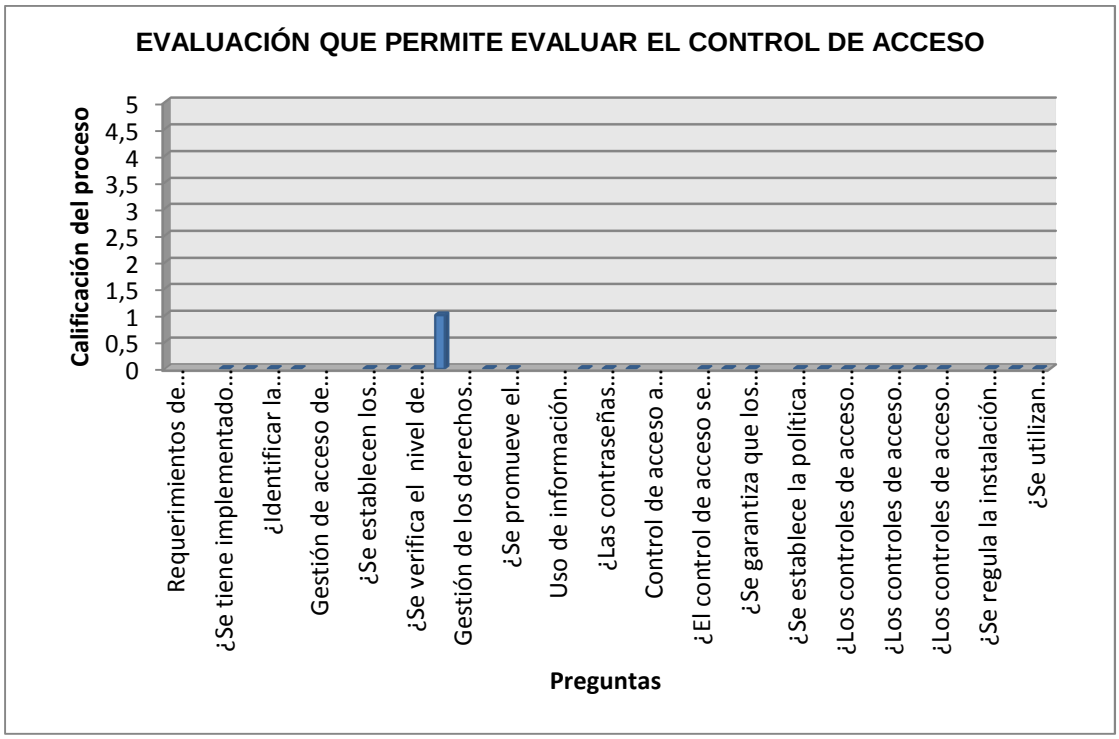


Ilustración 27 Cifrado Color Shop

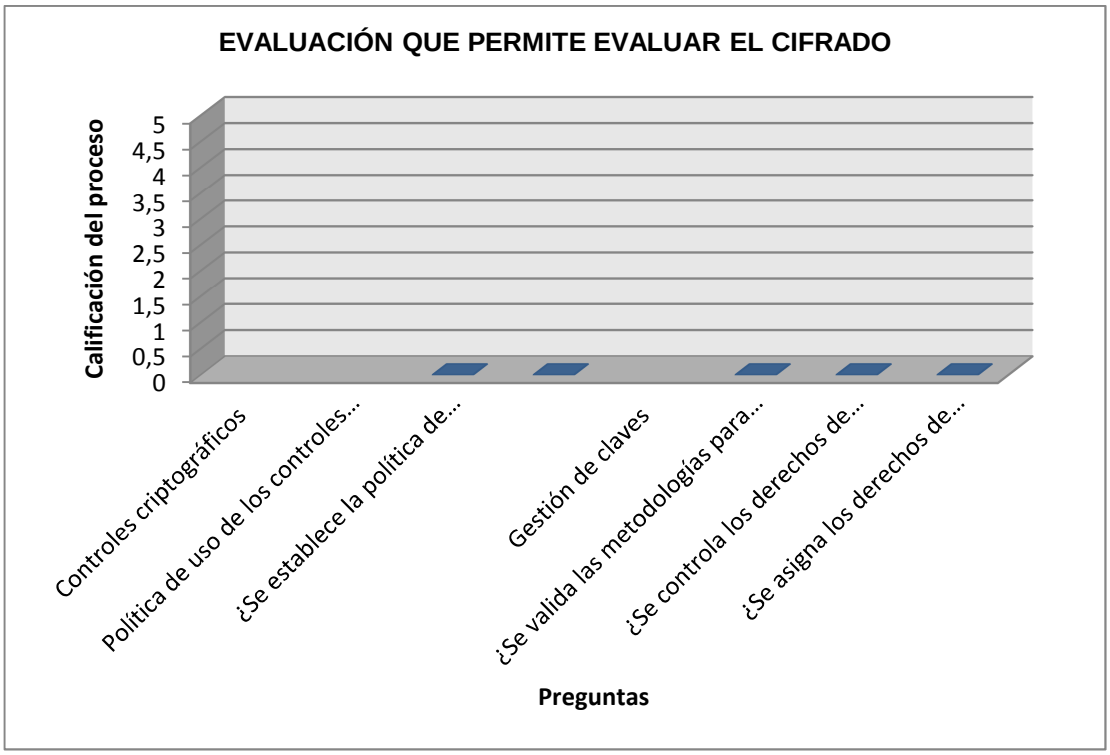


Ilustración 28 Seguridad física y del entorno Color Shop

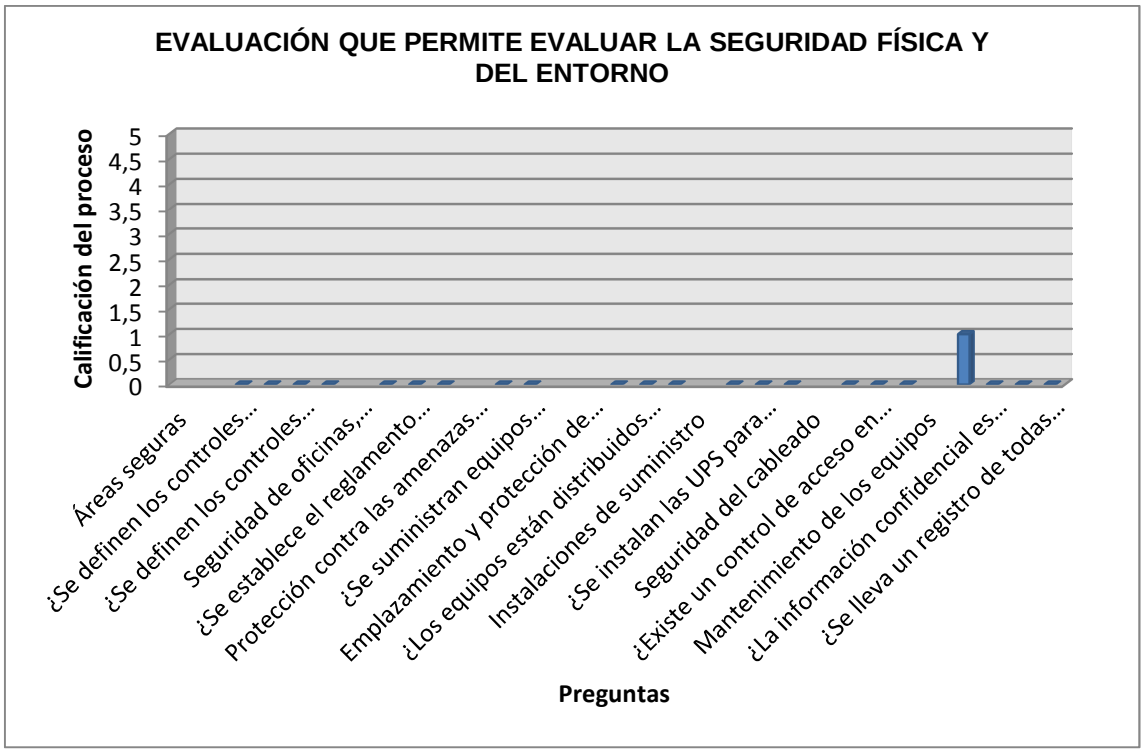


Ilustración 29 Seguridad en la operativa Color Shop

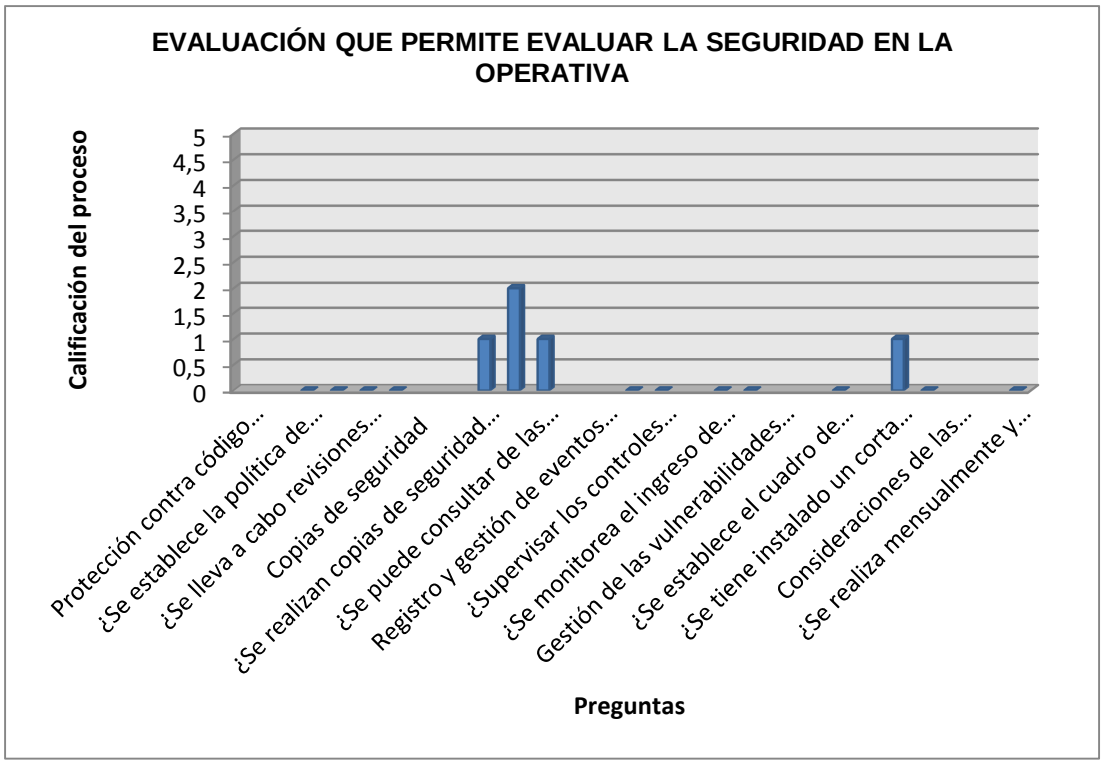


Ilustración 30 Seguridad en las telecomunicaciones Color Shop

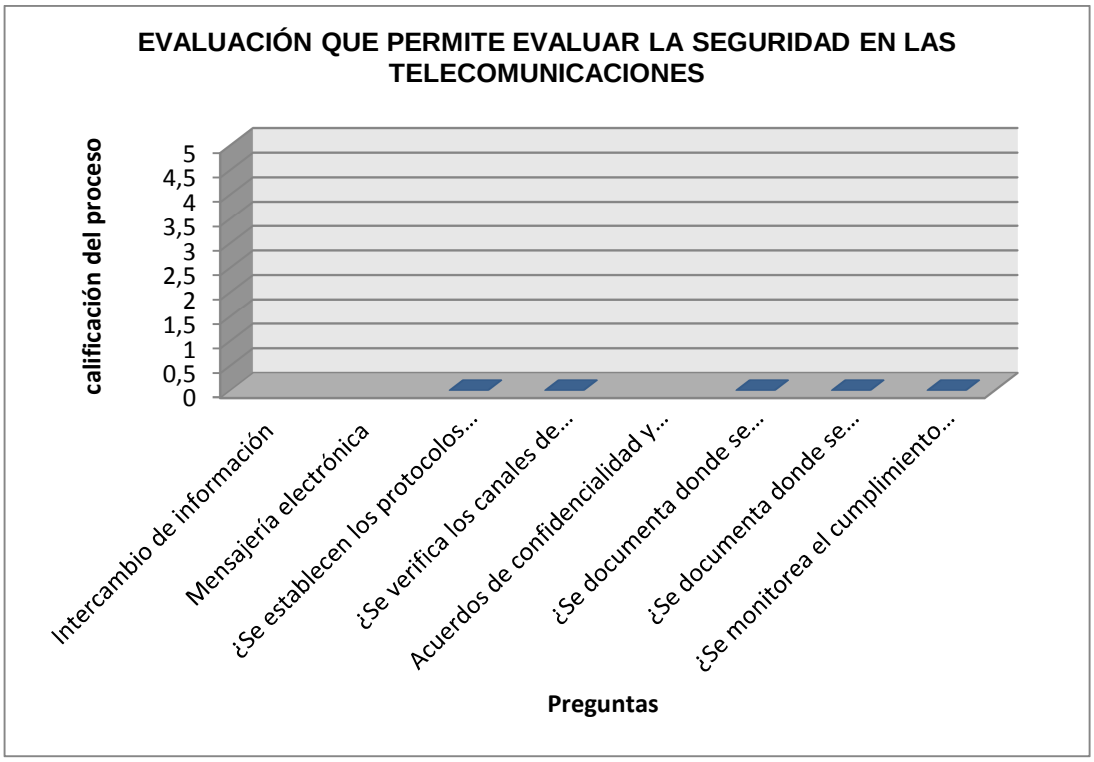


Ilustración 31 Gestión de incidentes en la seguridad de la información Color Shop

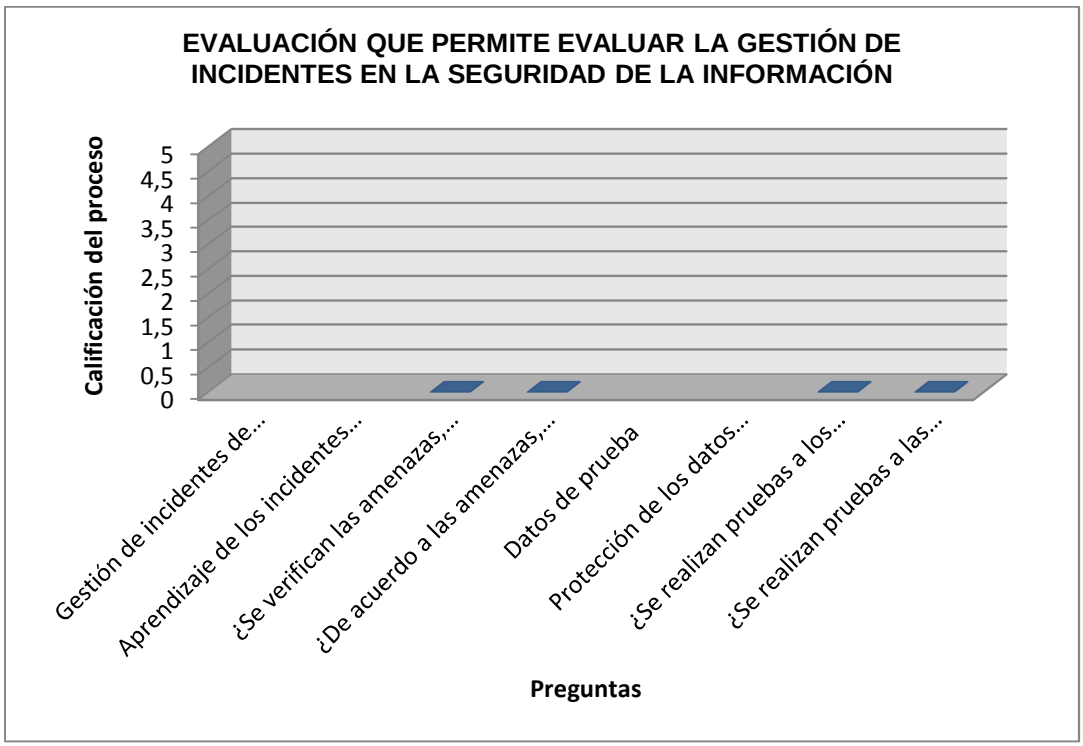


Ilustración 32 Adquisición, desarrollo y mantenimiento de los sistemas de información Color Shop

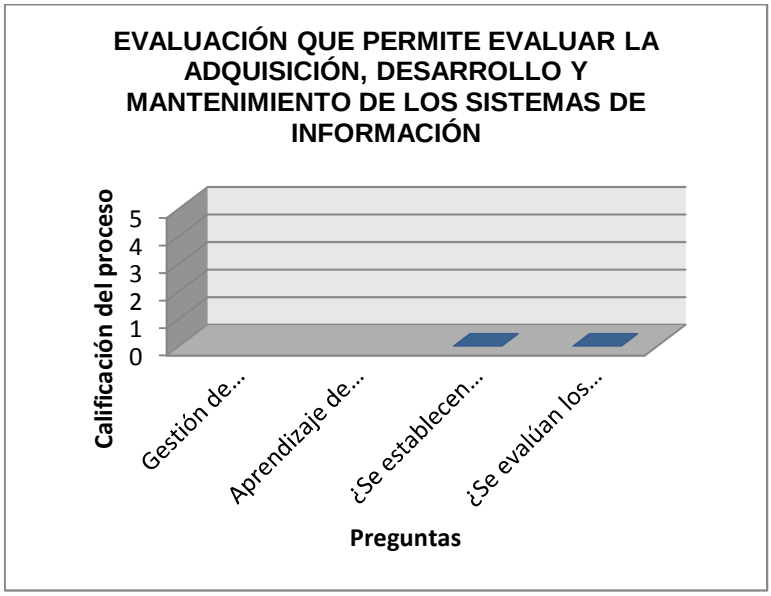


Ilustración 33 Aspectos de seguridad de la información en la gestión de la continuidad del negocio Color Shop

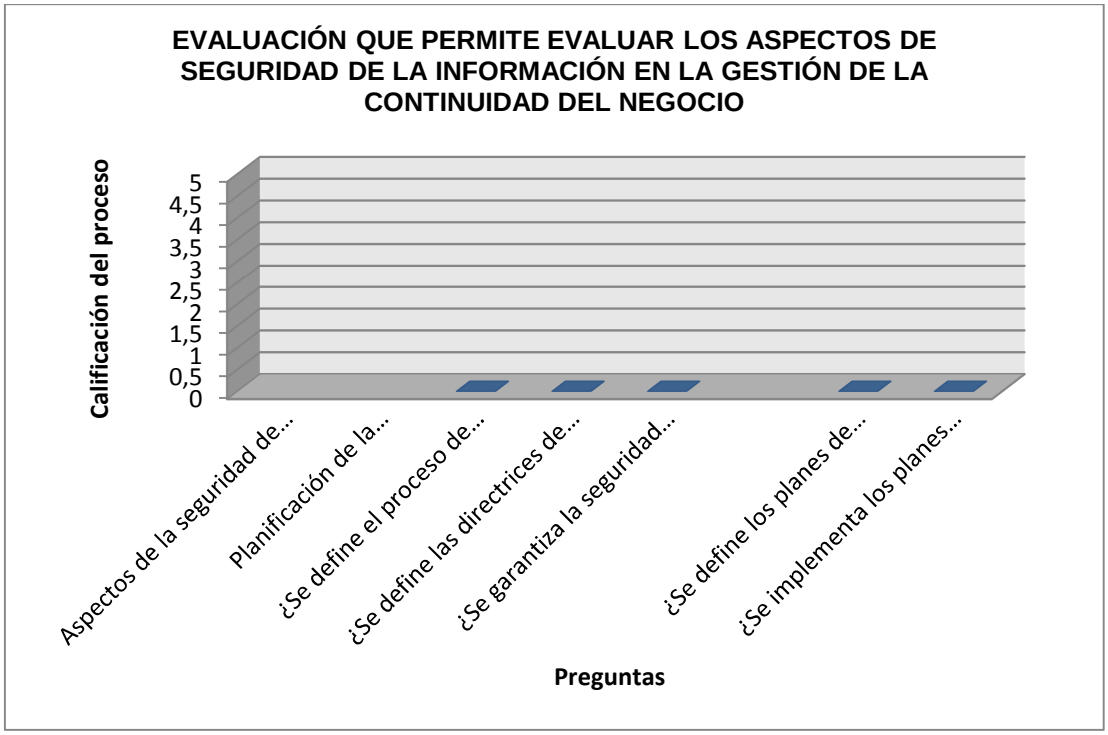
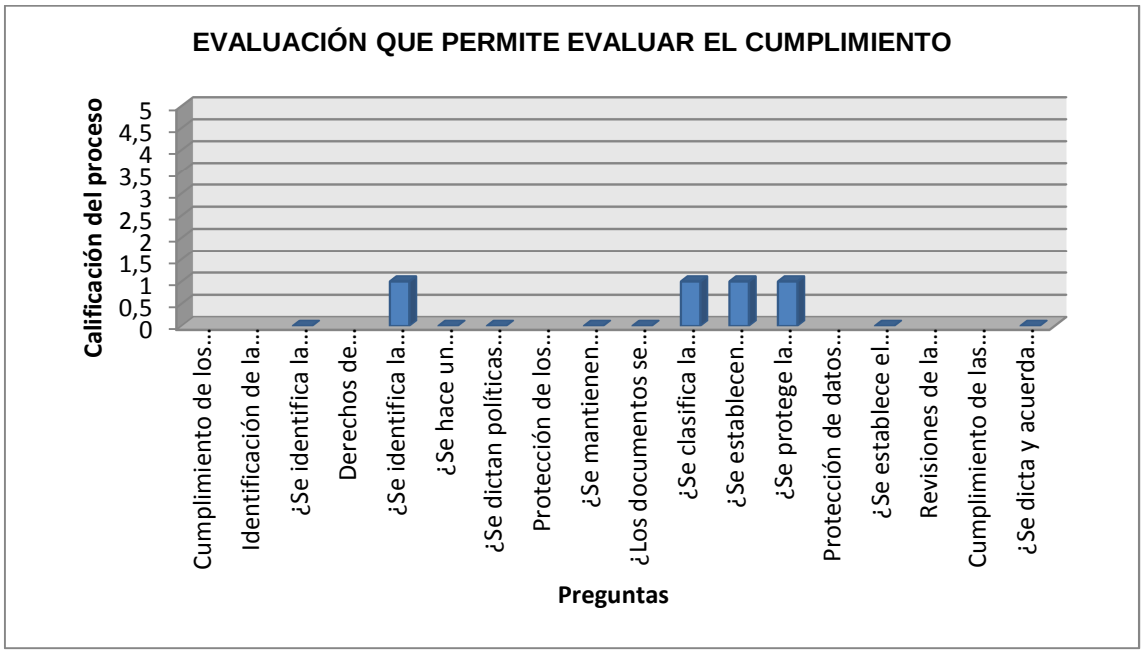


Ilustración 34 Cumplimiento Color Shop



10.3. Investigación de la información recolectada

Para determinar la valoración del riesgo e identificar la información recolectada, se equipara la probabilidad de ocurrencia y de impacto, conforme a las tablas de probabilidad de ocurrencia y valoración de impacto, de acuerdo a la información recolectada en la fase preliminar, el análisis del proceso de observación, instrumento de auditoría y fotografías de las Pymes:

Tabla 38 Probabilidad de ocurrencia[58]

Fuente: Tomada del libro I Magerit versión 3 p. 28

Probabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Tabla 39 Valoración de impacto

Fuente: Tomada del libro I Magerit versión 3 p. 28

Impacto	Valoración del impacto
Catastrófico	100%
Moderado	65%
Leve	30%

[58] UNIDISTRITAL. Gestión de riesgos. . [en línea]. [25 de febrero del 2015]. Disponible en: http://www.udistrital.edu.co:8080/documents/276352/356568/Cap5GestionRiesgo.pdf

Tabla 40 Probabilidad de Ocurrencia Guille Sport

	Variables	Número de veces que ocurre	Riesgos potenciales o peor escenario
	Hardware		
R1	Control a dispositivos de almacenamiento externos	1 vez cada 2 meses	Mal funcionamiento de los sistemas, destrucción de sistemas operativos, aplicativos e información.
R2	Manipulación de los equipos sin control alguno	1 vez al día	Alteración de archivos, registros, robo o destrucción de información, robo o destrucción de equipos de cómputo, fuga de información.
R3	Falta de equipos UPS's para contingencias	1 vez al año	Perdida de información, daños en los equipos, perdida de tiempos en los procesos y actividades del negocio.
	Software		
R4	Software no licenciado	1 vez al año	Mal funcionamiento de los sistemas, destrucción de sistemas operativos, aplicativos e información.
R5	Software con problemas de desarrollo	1 vez cada 2 meses	Modificación de información, robo de datos de los usuarios del sistema, bases de datos a merced del atacante.
R6	Sistemas sin restricciones de acceso	1 vez cada semana	Sustracción de información de la empresa o datos personales.
R7	Algunos equipos no tiene el sistema operativo actualizado	1 vez cada 6 meses	Intrusión no autorizada en los equipos, modificación, borrado o robo de información, ataques de DOS, consecución de privilegios.
R8	Falta de control a las actualizaciones del proveedor	1 vez cada 6 meses	Robo alteración y destrucción de datos, mal funcionamiento de los equipos y servicios.

	Seguridad física		
R9	Instalaciones físicas sin medidas de seguridad	1 vez al año	Robo de equipos de cómputo, telecomunicaciones, papelería, archivos, elementos de almacenamiento de información, daño a la información y a los equipos que la contienen.
R10	Instalaciones con deficiencias en planes de contingencia ante desastres naturales o provocados.	1 vez cada 6 meses	Inundaciones, incendios, terremotos, tormentas, destrucción parcial o total de equipos y datos.
R11	Control de acceso físico a las oficinas no existente	1 vez al día	Robo, destrucción, modificación o borrado de información, destrucción física de equipos, incendios.
R12	Instalaciones físicas con control ambiental inapropiado	1 vez cada semana	Perdida de información, equipos o partes asociadas a su gestión.
	Seguridad lógica		
R13	Control en el recambio y destrucción de medios de almacenamiento	1 vez cada 6 meses	Sustracción de información sensible de la compañía a través de personas externas.
R14	Control de acceso deficiente o faltante	1 vez cada semana	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios.
	Redes de comunicaciones		
R15	Vulnerabilidades de los navegadores utilizados	1 vez al año	Alteración en el funcionamiento del código, programas y sitios, apropiación de información sin autorización.
R16	Uso de aplicaciones poco confiables para compartir archivos o para asistencia remota	1 vez cada 2 meses	Robo de información de bases de datos.
	Personal		

R17	Falta de una política de seguridad clara	1 vez al día	Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal.
R18	Personal inconforme en la compañía	1 vez cada 6 meses	Alteración de archivos, registros, robo o destrucción de información, robo o destrucción de equipos de cómputo, fuga de información.
R19	Usuarios con pocos conocimientos en informática	1 vez cada semana	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios.
R20	Falta de conciencia en los funcionarios para el uso de las tecnologías	1 vez cada 2 meses	Sustracción de información sensible de la compañía y los usuarios, daño en aplicativos, bases de datos y repositorios.
R21	Soportes técnicos con deficiencias en capacitación y experiencia	1 vez cada 2 meses	Sustracción de datos personales y su posterior uso en actividades delictivas, mal funcionamiento de los equipos, robo de información, o destrucción premeditada de la misma.

Tabla 41 Valoración del riesgo Guille Sport[59]

Fuente: Tomado de UNAD. Valoración de amenazas

Riesgos / Valoración		Probabilidad					Impacto		
		Muy Alto (MA)	**Alto (A)**	**Medio (M)**	**Bajo (B)**	**Muy bajo (MB)**	**Leve**	**Moderado**	**Catastrófico**
	Hardware								
R1	Control a dispositivos de almacenamiento externos			50					100%
R2	Manipulación de los equipos sin control	100						65%	

[59] Fuente: Tomado de UNAD. Valoración de amenazas, op. cit, p.1.

	alguno								
R3	Falta de equipos UPS's para contingencias					5		65%	
	Software								
R4	Software no licenciado					5			100%
R5	Software con problemas de desarrollo			50					100%
R6	Sistemas sin restricciones de acceso		70						100%
R7	Algunos equipos no tiene el sistema operativo actualizado				10		30%		
R8	Falta de control a las actualizaciones del proveedor				10		30%		
	Seguridad física								
R9	Instalaciones físicas sin medidas de seguridad					5			100%
R10	Instalaciones con deficiencias en planes de contingencia ante desastres naturales o provocados.				10			65%	
R11	Control de acceso físico a las oficinas no existente	100					30%		
R12	Instalaciones físicas con control ambiental inapropiado		70					65%	
	Seguridad lógica								
R13	Control en el recambio y destrucción de medios de almacenamiento				10			65%	
R14	Control de acceso deficiente o faltante		70				30%		
	Redes de comunicaciones								
R15	Vulnerabilidades de los navegadores utilizados					5		65%	
R16	Uso de aplicaciones poco confiables			50			30%		

	para compartir archivos o para asistencia remota								
	Personal								
R17	Falta de una política de seguridad clara	100							100%
R18	Personal inconforme en la compañía				10			65%	
R19	Usuarios con pocos conocimientos en informática		70				30%		
R20	Falta de conciencia en los funcionarios para el uso de las tecnologías			50				65%	
R21	Soportes técnicos con deficiencias en capacitación y experiencia			50					100%

Tabla 42 Matriz clasificación de riesgo Guille Sport[60]

Fuente: Tomado de UNAD. Módulo riesgos y control informático

	Leve	**Moderado**	**Catastrófico**
Alta	R11, R14, R19	R2, R12	R6, R17
Media	R16	R20	R1, R5, R21
Baja	R7, R8	R3, R10, R13, R15, R18	R4, R9

[60] Fuente: Tomado de UNAD. Módulo riesgos y control informático. [en línea]. [25 de febrero del 2015]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/Modulo_Riesgos_y_Control_Informatico_V5_2012_DEFINITIVO_.pdf

10.3.1. Nivel Aceptable o que se debe monitorear de Guille Sport

R3	Falta de equipos UPS's para contingencias
R7	Algunos equipos no tiene el sistema operativo actualizado
R13	Control en el recambio y destrucción de medios de almacenamiento
R8	Falta de control a las actualizaciones del proveedor
R10	Instalaciones con deficiencias en planes de contingencia ante desastres naturales o provocados.
R18	Personal inconforme en la compañía
R16	Uso de aplicaciones poco confiables para compartir archivos o para asistencia remota
R15	Vulnerabilidades de los navegadores utilizados

10.3.2. Nivel de Investigación o que se requiere la posibilidad de un tratamientode Guille Sport

R14	Control de acceso deficiente o faltante
R11	Control de acceso físico a las oficinas no existente
R20	Falta de conciencia en los funcionarios para el uso de las tecnologías
R9	Instalaciones físicas sin medidas de seguridad
R4	Software no licenciado
R19	Usuarios con pocos conocimientos en informática

10.3.3. Nivel de Controles inmediatos o de mitigación de Guille Sport

R1	Control a dispositivos de almacenamiento externos
R17	Falta de una política de seguridad clara
R12	Instalaciones físicas con control ambiental inapropiado
R2	Manipulación de los equipos sin control alguno
R6	Sistemas sin restricciones de acceso
R5	Software con problemas de desarrollo
R21	Soportes técnicos con deficiencias en capacitación y experiencia

Tabla 43 Probabilidad de Ocurrencia Color Shop

	Variables	Número de veces que ocurre	Riesgos potenciales o peor escenario
		Hardware	
R1	Control a dispositivos de almacenamiento externos	1 vez cada 6 meses	Mal funcionamiento de los sistemas, destrucción de sistemas operativos, aplicativos e información.
R2	Manipulación de los equipos sin control alguno	1 vez al día	Alteración de archivos, registros, robo o destrucción de información, robo o destrucción de equipos de cómputo, fuga de información.
R3	Falta de equipos UPS's para contingencias	1 vez cada 6 meses	Perdida de información, daños en los equipos, perdida de tiempos en los procesos y actividades del negocio.
		Software	
R4	Software con problemas de desarrollo	1 vez cada semana	Modificación de información, robo de datos de los usuarios del sistema, bases de datos a merced del atacante.
R5	Sistemas sin restricciones de acceso	1 vez cada 2 meses	Sustracción de información de la empresa o datos personales.
R6	Falta de control a las actualizaciones del proveedor	1 vez al año	Robo alteración y destrucción de datos, mal funcionamiento de los equipos y servicios.
		Seguridad física	
R7	Instalaciones físicas con medidas de seguridad deficientes.	1 vez cada semana	Robo de equipos de cómputo, telecomunicaciones, papelería, archivos, elementos de almacenamiento de información, daño a la información y a los equipos que la contienen.
R8	Instalaciones con deficiencias en planes de contingencia ante desastres naturales o	1 vez cada semana	Inundaciones, incendios, terremotos, tormentas, destrucción parcial o total de equipos y datos.

	provocados.		
R9	Control de acceso físico a las oficinas no existente	1 vez cada 2 meses	Robo, destrucción, modificación o borrado de información, destrucción física de equipos, incendios.
R10	Instalaciones físicas con control ambiental inapropiado	1 vez al año	Perdida de información, equipos o partes asociadas a su gestión.
Seguridad lógica			
R11	Control en el recambio y destrucción de medios de almacenamiento	1 vez al año	Sustracción de información sensible de la compañía a través de personas externas.
R12	Control de acceso deficiente o faltante	1 vez al día	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios.
Redes de comunicaciones			
R13	Vulnerabilidades de los navegadores utilizados	1 vez cada 6 meses	Alteración en el funcionamiento del código, programas y sitios, apropiación de información sin autorización.
R14	Uso de aplicaciones poco confiables para compartir archivos o para asistencia remota	1 vez cada semana	Robo de información de bases de datos.
Personal			
R15	Falta de una política de seguridad clara	1 vez cada semana	Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal.
R16	Personal inconforme en la compañía	1 vez al año	Alteración de archivos, registros, robo o destrucción de información, robo o destrucción de equipos de cómputo, fuga de información.
R17	Usuarios con pocos conocimientos en informática	1 vez cada 2 meses	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios.
R18	Falta de conciencia en	1 vez al día	Sustracción de información sensible de la compañía y los usuarios,

	los funcionarios para el uso de las tecnologías		daño en aplicativos, bases de datos y repositorios.
R19	Soportes técnicos con deficiencias en capacitación y experiencia	1 vez al día	Sustracción de datos personales y su posterior uso en actividades delictivas, mal funcionamiento de los equipos, robo de información, o destrucción premeditada de la misma.

Tabla 44 Valoración del riesgo Color Shop[61]

Fuente: Tomado de UNAD. Valoración de amenazas

Riesgos / Valoración		Probabilidad					Impacto		
		Muy Alto (MA)	Alto (A)	Medio (M)	Bajo (B)	Muy bajo (MB)	Leve	Moderado	Catastrófico
HARDWARE									
R1	Control a dispositivos de almacenamiento externos				10		30%		
R2	Manipulación de los equipos sin control alguno	100							100%
R3	Falta de equipos UPS's para contingencias				10			65%	
SOFTWARE									
R4	Software con problemas de desarrollo		70					65%	
R5	Sistemas sin restricciones de acceso			50					100%
R6	Falta de control a las actualizaciones del proveedor					5	30%		
SEGURIDAD FÍSICA									
R7	Instalaciones físicas con medidas de seguridad deficientes.		70					65%	
R8	Instalaciones con deficiencias en planes de contingencia ante desastres naturales o		70						100%

[61] Fuente: Tomado de UNAD. Valoración de amenazas, op. cit, p.1.

	provocados.								
R9	Control de acceso físico a las oficinas no existente			50			30%		
R10	Instalaciones físicas con control ambiental inapropiado					5		65%	
SEGURIDAD LÓGICA									
R11	Control en el recambio y destrucción de medios de almacenamiento					5		65%	
R12	Control de acceso deficiente o faltante	100							100%
REDES DE COMUNICACIONES									
R13	Vulnerabilidades de los navegadores utilizados				**10**				100%
R14	Uso de aplicaciones poco confiables para compartir archivos o para asistencia remota		**70**				30%		
PERSONAL									
R15	Falta de una política de seguridad clara		70						100%
R16	Personal inconforme en la compañía					5	30%		
R17	Usuarios con pocos conocimientos en informática			50				65%	
R18	Falta de conciencia en los funcionarios para el uso de las tecnologías	100						65%	
R19	Soportes técnicos con deficiencias en capacitación y experiencia	100					30%		

Tabla 45. Matriz clasificación de riesgo Color Shop[62]

Fuente: Tomado de UNAD. Módulo riesgos y control informático

	Leve	Moderado	Catastrófico
Alta	R14, R19	R4, R7, R18	R2, R8, R12, R15
Media	R9	R17	R5
Baja	R1, R6, R16	R3, R10, R11	R13

10.3.4. Nivel Aceptable o que se debe monitorear de Color Shop

R1	**Control a dispositivos de almacenamiento externos**
R10	Instalaciones físicas con control ambiental inapropiado
R11	Control en el recambio y destrucción de medios de almacenamiento
R16	Personal inconforme en la compañía
R3	Falta de equipos UPS's para contingencias
R6	Falta de control a las actualizaciones del proveedor
R9	Control de acceso físico a las oficinas no existente

10.3.5. Nivel de Investigación o que se requiere la posibilidad de un tratamiento de Color Shop

R13	**Vulnerabilidades de los navegadores utilizados**
R14	Uso de aplicaciones poco confiables para compartir archivos o para asistencia remota
R17	Usuarios con pocos conocimientos en informática
R19	Soportes técnicos con deficiencias en capacitación y experiencia

10.3.6. Nivel de Controles inmediatos o de mitigación de Color Shop

R2	**Manipulación de los equipos sin control alguno**
R12	Control de acceso deficiente o faltante
R15	Falta de una política de seguridad clara
R18	Falta de conciencia en los funcionarios para el uso de las tecnologías
R4	Software con problemas de desarrollo
R5	Sistemas sin restricciones de acceso
R7	Instalaciones físicas con medidas de seguridad deficientes.
R8	Instalaciones con deficiencias en planes de contingencia ante desastres naturales o provocados.

[62] Fuente: Tomado de UNAD. Módulo riesgos y control informático, op. cit, p.1.

Tabla 46 Cuestionario de control Anexo 1

	FORMATO CUESTIONARIO DE CONTROL ANEXO 1	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A5: EVALUAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN				
A5.1.	**Política de Seguridad de la Información**			
	Conjunto de políticas para la seguridad de la información			
1	¿Está definida la política de seguridad para la empresa?			
2	¿Se encuentran definidos los objetivos generales y el alcance de seguridad informática, como mecanismo para compartir información?			
3	¿Se tiene la estructura necesaria para establecer los objetivos de control, evaluando los riesgos?			
4	¿Se tiene la estructura necesaria para establecer la gestión de los riesgos?			
5	¿Se realizan capacitaciones constantes sobre las vulnerabilidades, riesgos y amenazas que tiene una organización?			
	Revisión de las políticas para la seguridad de la información.			
1	¿Se realizan acciones preventivas y correctivas?			
2	¿Se realizan revisiones periódicas de la política de seguridad?			
3	¿Los incidentes de seguridad se reporta?			
4	¿Se realizan revisiones periódicas de la política de seguridad?			
OBSERVACIONES:				

Tabla 47 Cuestionario de control Anexo 2

	FORMATO CUESTIONARIO DE CONTROL ANEXO 2	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A6: EVALUAR LOS ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN				
A6.1.	**Organización interna**			
	Asignación de responsabilidades para la seguridad de la información			
1	¿Documentar las metas de seguridad, verificando que satisface los requisitos de la empresa?			
2	¿Revisar y probar la política de seguridad de la información?			
3	¿Definir las iniciativas de seguridad?			
4	¿Proporciona los recursos requeridos para la seguridad de la información?			
5	¿Se asignan funciones conforme a las necesidades de la información?			
6	¿Se asignan las responsabilidades a cada proceso de seguridad?			
7	¿Se documentan los procesos de asignación y seguridad?			
	Segregación de tareas			
1	¿Los activos informáticos se encuentran definidos claramente?			
2	¿Se garantizan las actividades de seguridad, siguiendo la política de seguridad?			
3	¿Se identifican los cambios, cuando existen amenazas?			
4	¿Se evalúan y coordinan los controles de seguridad?			
	Seguridad de la información en la gestión de proyectos			
1	¿La dirección se compromete con la seguridad de la información?			

2	¿Autorización por la dirección para la inversión de recursos, tiempos y formaciones?			
3	¿Existen los procedimientos documentados para contactar a las autoridades competentes?			
4	¿Existen los procedimientos documentados para contactar a las entidades públicas?			
5	¿Existen los procedimientos documentados para contactar a las empresas proveedoras de telecomunicaciones?			
A6.2.	**Dispositivos para movilidad y teletrabajo**			
	Política de uso de dispositivos para movilidad			
1	¿Se tiene definida la política de seguridad para dispositivos móviles?			
2	¿Los controles aseguran la protección de los canales de comunicación?			
3	¿Los controles aseguran la protección contra código malicioso?			
4	¿Los controles aseguran la disponibilidad, integridad y confidencialidad de la información?			
	Teletrabajo			
1	¿Se tiene la estructura clara para la presentación de informes?			
2	¿Se cuenta con unos procesos específicos para la gestión de cambio?			
3	¿La política de acceso, cuenta con los módulos permitidos para la identificación de usuario?			
4	¿Se cuenta con los privilegios de acceso?			
OBSERVACIONES:				

Tabla 48 Cuestionario de control Anexo 3

	FORMATO CUESTIONARIO DE CONTROL ANEXO 3	**Código: SGSI-P-02-F-02**
		Versión: **01**
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A7: EVALUAR LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS				
A7.2.	**Seguridad en el desempeño de las funciones del empleo**			
	Responsabilidades de gestión			
1	¿Se tienen las directrices sobre las funciones de seguridad en el sistema de información?			
2	¿Se poseen las habilidades y calificaciones apropiadas?			
3	¿Logran un grado de concientización sobre la seguridad dentro de la organización?			
4	¿Están de acuerdo con los términos y las condiciones laborales?			
	Concienciación, educación y capacitación en seguridad de la información			
1	¿Se utiliza una formación en el uso correcto de los servicios de procesamiento de información?			
2	¿Se realizan capacitaciones sobre las amenazas, riesgos y vulnerabilidades?			
3	¿Se establecen los procesos de formación y concientización, diseñado para presentar las políticas de seguridad de la organización?			
OBSERVACIONES:				

Tabla 49 Cuestionario de control Anexo 4

	FORMATO CUESTIONARIO DE CONTROL ANEXO 4	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A8: EVALUAR LA GESTIÓN DE ACTIVOS				
A8.1.	**Responsabilidad sobre los activos**			
	Inventario de activos			
1	¿Se establece un inventario de activos informáticos por categoría?			
2	¿Se incluyen los requisitos para mantener seguro los activos informáticos?			
	Propiedad de los activos			
1	¿Los activos informáticos mantienen un código de ingreso a la organización, cada vez que se adquiere uno nuevo?			
2	¿Se clasifican los activos, conforme a sus características?			
3	¿Los activos se clasifican por niveles?			
	Uso aceptable de los activos			
1	¿Se informa a los empleados el uso de los activos?			
	Devolución de activos			
1	¿Existe un proceso de terminación para incluir la devolución del software?			
2	¿Existe un proceso de terminación para incluir la devolución de los documentos?			
3	¿Existe un proceso de terminación para incluir la devolución de los equipos móviles?			
4	¿Existe un proceso de terminación para incluir la devolución de los equipos de cómputo?			
5	¿Existe un procedimiento que garantice la transferencia de información al finalizar su contratación?			

A8.2.	**Clasificación de la información**			
	Directrices de clasificación			
1	¿Se tienen las directrices sobre cómo se clasifican los activos informáticos?			
2	¿Existe la clasificación de seguridad por niveles?			
	Etiquetado y manipulado de la información			
1	¿Se capacita sobre cómo se debe enviar, y manipular las bases de información confidencial?			
2	¿Existe una marca para identificar las fuentes de información?			
	Manipulación de activos			
1	¿Los activos informáticos poseen una documentación adecuada?			
2	¿Existen manuales de configuración de los activos informáticos?			
OBSERVACIONES:				

Tabla 50 Cuestionario de control Anexo 5

	FORMATO CUESTIONARIO DE CONTROL ANEXO 5	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A9: EVALUACIÓN QUE PERMITE EVALUAR EL CONTROL DE ACCESO				
A9.1.	**Requerimientos de negocio para el control de acceso**			
	Política de control de acceso			
1	¿Se tiene implementado la política de control de acceso conforme a la política de seguridad?			
2	¿Se atiende la legislación vigente, conforme a las			

	normas actuales?			
3	¿Identificar la información relacionada con las aplicaciones?			
4	¿Identificar los riesgos asociados a la información?			
A9.2.	**Gestión de acceso de usuario**			
	Gestión de altas/bajas en el registro de usuarios			
1	¿Se establecen los repositorios donde se registran los usuarios que ingresan al sistema operativo?			
2	¿Se establecen los contadores para identificar cuantas sesiones están abiertas por usuario?			
3	¿Se verifica el nivel de acceso otorgado a cada usuario periódicamente?			
4	¿Se verifica que el usuario tenga autorización del dueño del sistema para el uso de la información?			
	Gestión de los derechos de acceso con privilegios especiales			
1	¿Se establece para cada tipo de activo los privilegios otorgados de acuerdo a la evaluación de riesgos asociada?			
2	¿Se promueve el desarrollo de rutinas del sistema para evitar la necesidad de otorgar privilegios innecesarios?			
A9.3.	**Responsabilidades de usuario**			
	Uso de información confidencial para la autenticación			
1	¿Está definida la política de seguridad para usuarios de los equipos?			
2	¿Las contraseñas predeterminadas por el proveedor se cambian inmediatamente después de la instalación de los sistemas o del software?			
3	¿Las contraseñas temporales se suministran de forma segura a los usuarios?			
A9.4.	**Control de acceso a sistemas operativo y aplicaciones**			
	Restricción del acceso a la información			
1	¿El control de acceso se realiza de acuerdo a la política del control de accesos?			
2	¿Se controla los derechos de acceso de otras aplicaciones?			
3	¿Se garantiza que los datos de salida de los sistemas de aplicación que manejan información sensible solo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados?			

	Procedimientos seguros de inicio de sesión			
1	¿Se establece la política de autenticación a los equipos, con contraseñas personales y perfiles definidos?			
2	¿Se valida la información de registro con la base de datos para el acceso?			
3	¿Los controles de acceso se aplican al personal de soporte técnico?			
4	¿Los controles de acceso se aplican a los operadores?			
5	¿Los controles de acceso se aplican a los administradores de red?			
6	¿Los controles de acceso se aplican a los programadores de sistemas?			
7	¿Los controles de acceso se aplican a los administradores de bases de datos?			
	Uso de herramientas de administración de sistemas			
1	¿Se regula la instalación de software en los equipos personales?			
2	¿Se lleva un registro de todo uso de las utilidades del sistema?			
3	¿Se utilizan procedimientos de identificación, autenticación y autorización para las utilidades del sistema?			
OBSERVACIONES:				

Tabla 51 Cuestionario de control Anexo 6

	FORMATO CUESTIONARIO DE CONTROL ANEXO 6	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	**PARÁMETRO**	**SI**	**NO**	**N/A**

A10: EVALUACIÓN QUE PERMITE EVALUAR EL CIFRADO				
A10.1.	**Controles criptográficos**			
	Política de uso de los controles criptográficos			
1	¿Se establece la política de cifrado para las claves públicas y privadas en el manejo de información confidencial?			
2	¿Se verifica periódicamente la política de cifrado conforme a la norma actual?			
	Gestión de claves			
1	¿Se valida las metodologías para cifrar las claves y uso en los mensajes emitidos?			
2	¿Se controla los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?			
3	¿Se asigna los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?			
OBSERVACIONES:				

Tabla 52 Cuestionario de control Anexo 7

	FORMATO CUESTIONARIO DE CONTROL ANEXO 7	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A11: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD FÍSICA Y DEL ENTORNO				
A11.1.	**Áreas seguras**			
	Controles físicos de entrada			
1	¿Se definen los controles físicos para cada activo?			

2	¿Se definen los controles técnicos para cada activo?			
3	¿Se definen los controles organizacionales para cada activo?			
4	¿Se dicta la política de control de accesos conforme al SGSI?			
	Seguridad de oficinas, despachos y recursos			
1	¿Se dicta la política de uso de las oficinas acorde a la política de gestión de acceso y del SGSI?			
2	¿Se establece el reglamento sobre las actividades y procesos informáticos?			
3	¿Se establece las normas sobre las actividades y procesos informáticos?			
	Protección contra las amenazas externas y ambientales			
1	¿Definir un plan de respuesta para cada tipo de efecto que pudiera causar amenaza externa?			
2	¿Se suministran equipos apropiados contra las amenazas ambientales y son ubicados adecuadamente?			
A11.2.	**Seguridad de los equipos**			
	Emplazamiento y protección de equipos			
1	¿Monitorear el uso de equipos personales a través de la política de uso de equipos personales?			
2	¿Los equipos están distribuidos de tal forma que no pueda acceder cualquier usuario?			
3	¿Los elementos que requieren protección especial están aislados?			
	Instalaciones de suministro			
1	¿Se establece el plan de continuidad para este tipo de riesgos?			
2	¿Se instalan las UPS para suministrar energía a los equipos de cómputo?			
3	¿Las UPS y plantas de energía son revisadas con frecuencia?			
	Seguridad del cableado			
1	¿El cableado se encuentre canalizado por conductos específicos del suelo técnico instalado en las oficinas?			
2	¿Existe un control de acceso en los cuartos de cableado que soportan los sistemas críticos?			
3	¿Tienen rótulos de equipos y de cables claramente identificables para minimizar los			

	errores en el manejo?			
	Mantenimiento de los equipos			
1	¿Se realiza el mantenimiento acorde a los procesos de gestión de activos?			
2	¿La información confidencial es retirada periódicamente de los equipos de cómputo?			
3	¿El personal de mantenimiento es suficientemente confiable?			
4	¿Se lleva un registro de todas las fallas reales y sospechosas?			
OBSERVACIONES:				

Tabla 53 Cuestionario de control Anexo 8

	FORMATO CUESTIONARIO DE CONTROL ANEXO 8	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A12: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LA OPERATIVA				
A12.1.	**Protección contra código malicioso**			
	Controles contra el código malicioso			
1	¿Se establece la política de seguridad de equipos personales en la que se previene el uso de programas no autorizados por la empresa?			
2	¿Se regula el uso de software antivirus y su actualización?			
3	¿Se lleva a cabo revisiones mensuales sobre el contenido del software y los datos que soportan los procesos críticos del negocio?			
4	¿Se investiga la aparición de archivos o códigos no autorizados por el desarrollador del software?			

A12.2.	**Copias de seguridad**			
	Copias de seguridad de la información			
1	¿Se realizan copias de seguridad de manera periódica sobre la información registrada en las oficinas – Backup?			
2	¿Las copias de seguridad se almacenan en un sitio seguro?			
3	¿Se puede consultar de las copias de seguridad los archivos y la información está completa?			
A12.4.	**Registro de actividad y supervisión**			
	Registro y gestión de eventos de actividad			
1	¿Se monitorea los cambios de configuración del sistema?			
2	¿Supervisar los controles definidos al uso de equipos personales?			
	Registros de actividad del administrador y operador del sistema			
1	¿Se monitorea el ingreso de usuarios a las diferentes aplicaciones?			
2	¿Se registran las alertas o fallas del sistema, como mensajes de consola?			
A12.6.	**Gestión de las vulnerabilidades técnicas**			
	Gestión de las vulnerabilidades técnicas			
1	¿Se establece el cuadro de control que evidencie los riesgos asociados a la organización?			
	Restricciones en la instalación de sistema operativo (S.O.)			
1	¿Se tiene instalado un corta fuego en el sistema operativo?			
2	¿Se asignan privilegios a los usuarios conforme a su perfil o cargo?			
A12.7.	**Consideraciones de las auditorías de los sistemas de información**			
	Controles de auditoría de los sistemas de información			
1	¿Se realiza mensualmente y trimestralmente una auditoría interna por los procesos de seguridad que se han implementado en la organización?			
OBSERVACIONES:				

Tabla 54 Cuestionario de control Anexo 9

	FORMATO CUESTIONARIO DE CONTROL ANEXO 9	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A13: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LAS TELECOMUNICACIONES				
A13.2.	**Intercambio de información**			
	Mensajería electrónica			
1	¿Se establecen los protocolos para enviar la información por los canales de comunicación?			
2	¿Se verifica los canales de comunicación mensualmente identificando los canales de transmisión por el internet?			
	Acuerdos de confidencialidad y secreto			
1	¿Se documenta donde se establecen los acuerdos de confidencialidad?			
2	¿Se documenta donde se establecen las políticas de confidencialidad?			
3	¿Se monitorea el cumplimiento de los acuerdos?			
OBSERVACIONES:				

Tabla 55 Cuestionario de control Anexo 10

	FORMATO CUESTIONARIO DE CONTROL ANEXO 10	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A16: EVALUACIÓN QUE PERMITE EVALUAR LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN				
A16.1.	**Gestión de incidentes de seguridad de la información y mejoras**			
	Aprendizaje de los incidentes de seguridad de la información			
1	¿Se verifican las amenazas, riesgos y vulnerabilidades asociados a la empresa?			
2	¿De acuerdo a las amenazas, riesgos y vulnerabilidades se debe establecer una propuesta para disminuir el riesgo?			
A14.3.	**Datos de prueba**			
	Protección de los datos utilizados en pruebas			
1	¿Se realizan pruebas a los activos informáticos, estableciendo las mejores alternativas para mitigar los riesgos?			
2	¿Se realizan pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial?			
OBSERVACIONES:				

Tabla 56 Cuestionario de control Anexo 11

	FORMATO CUESTIONARIO DE CONTROL ANEXO 11	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A14: EVALUACIÓN QUE PERMITE EVALUAR LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN				
A16.1.	**Gestión de incidentes de seguridad de la información y mejoras**			
	Aprendizaje de los incidentes de seguridad de la información			
	¿Se establecen procesos de resolución de incidentes de seguridad de la información?			
	¿Se evalúan los incidentes de seguridad?			
OBSERVACIONES:				

Tabla 57 Cuestionario de control Anexo 12

	FORMATO CUESTIONARIO DE CONTROL ANEXO 12	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A17: EVALUACIÓN QUE PERMITE EVALUAR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
A17.1.	**Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**			
	Planificación de la continuidad de la seguridad de la información			
1	¿Se define el proceso de gestión de continuidad del negocio?			
2	¿Se define las directrices de continuidad del negocio de conformidad con la política de seguridad de la información?			
3	¿Se garantiza la seguridad del personal, la protección de los servicios y procesos de información?			
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información			
1	¿Se define los planes de continuidad del negocio de acuerdo al orden de prioridades?			
2	¿Se implementa los planes de continuidad del negocio de acuerdo al orden de prioridades?			
OBSERVACIONES:				

Tabla 58 Cuestionario de control Anexo 13

	FORMATO CUESTIONARIO DE CONTROL ANEXO 13	**Código: SGSI-P-02-F-02**
		Versión: 01
		Fecha elaboración: 02/03/2015
		Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A18: EVALUACIÓN QUE PERMITE EVALUAR EL CUMPLIMIENTO				
A18.1.	**Cumplimiento de los requisitos legales y contractuales**			
	Identificación de la legislación aplicable			
1	¿Se identifica la legislación aplicable para los procesos que intervienen en el manejo de la información?			
	Derechos de propiedad intelectual (DPI)			
1	¿Se identifica la legislación aplicable y los términos contractuales en las licencias utilizadas?			
2	¿Se hace un inventario de software para garantizar la idoneidad de su uso?			
3	¿Se dictan políticas de cumplimiento?			
	Protección de los registros de la organización			
1	¿Se mantienen disponibles los documentos del Sistema de gestión de la seguridad informática - SGSI?			
2	¿Los documentos se mantienen editables para los usuarios autorizados?			
3	¿Se clasifica la información en función de su importancia?			
4	¿Se establecen copias de seguridad de la información relevante?			
5	¿Se protege la información física sensible?			
	Protección de datos y privacidad de la información personal			
1	¿Se establece el documento de seguridad de conformidad con la legislación de protección de			

	datos personales?			
A18.2.	**Revisiones de la seguridad de la información**			
	Cumplimiento de las políticas y normas de seguridad			
1	¿Se dicta y acuerda la política del sistema de gestión de la seguridad informática - SGSI?			
OBSERVACIONES:				

11. RESULTADOS DE LA AUDITORÍA

11.1. Resultados por Pyme

A partir del cuestionario de control y/o lista de chequeo en cada una de las empresas se identificó los siguientes resultados por empresa:

Ilustración 35 Política de seguridad de la información Guille Sport

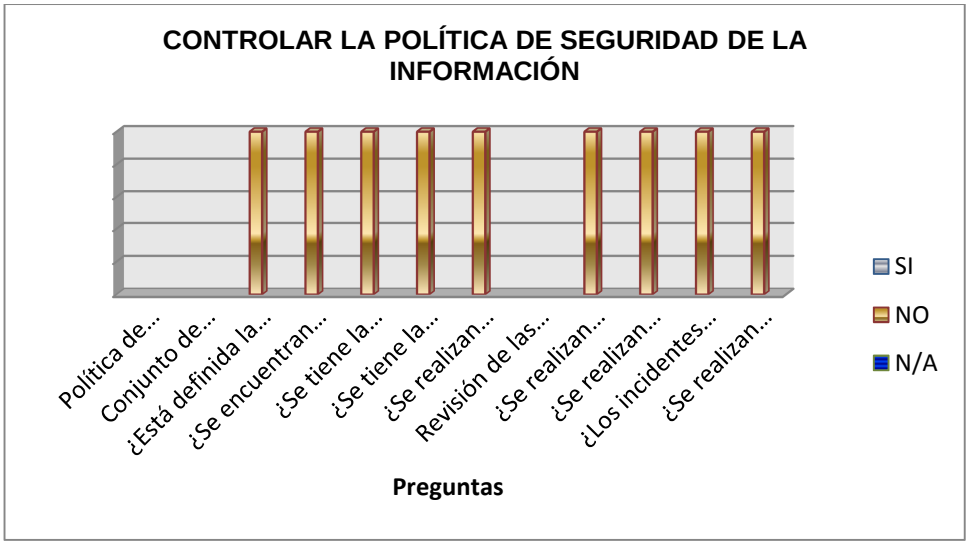


Ilustración 36 Aspectos organizativos de la seguridad de la información Guille Sport

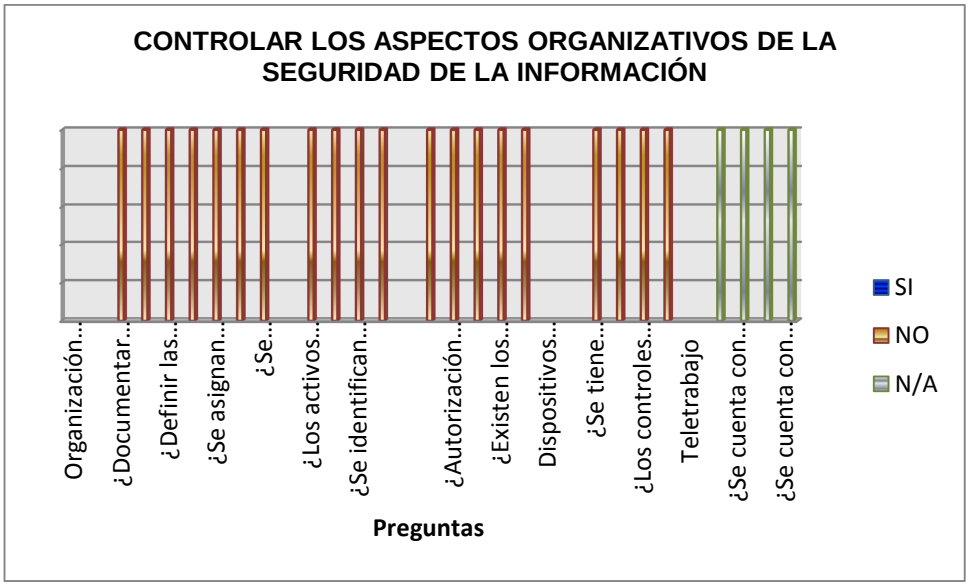


Ilustración 37 Seguridad ligada a los recursos humanos Guille Sport

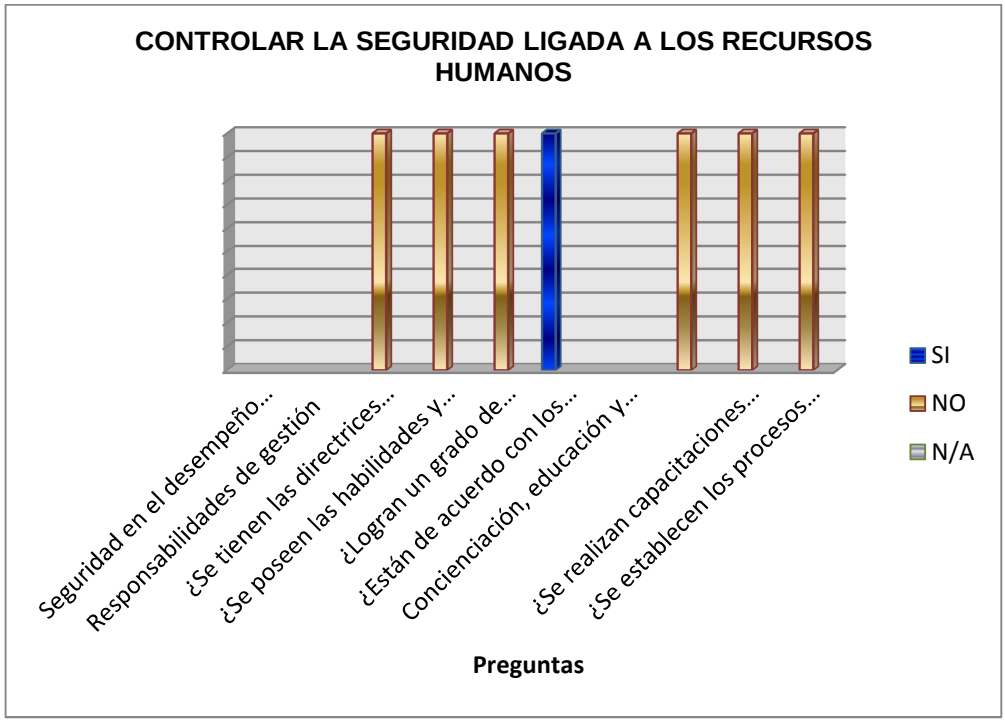


Ilustración 38 Gestión de activos Guille Sport

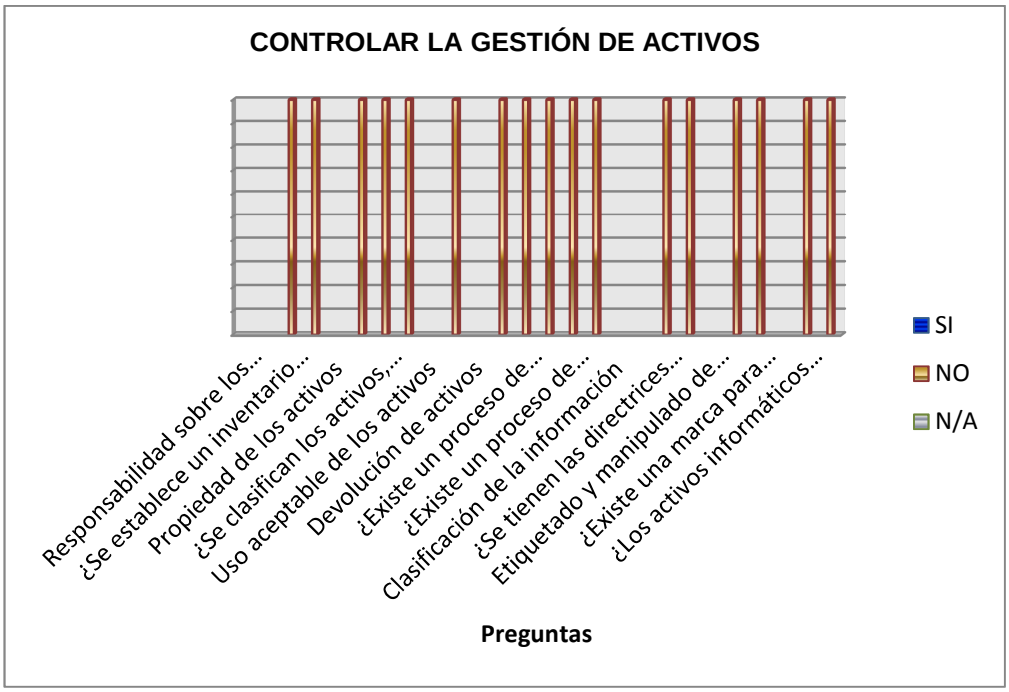


Ilustración 39 Control de accesos Guille Sport

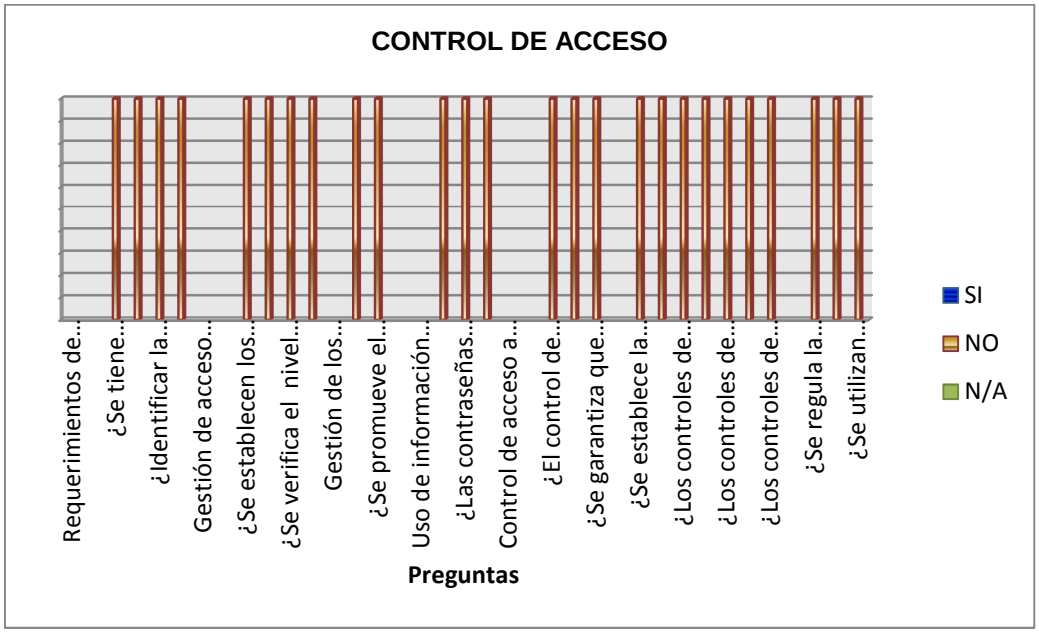


Ilustración 40 Cifrado Guille Sport

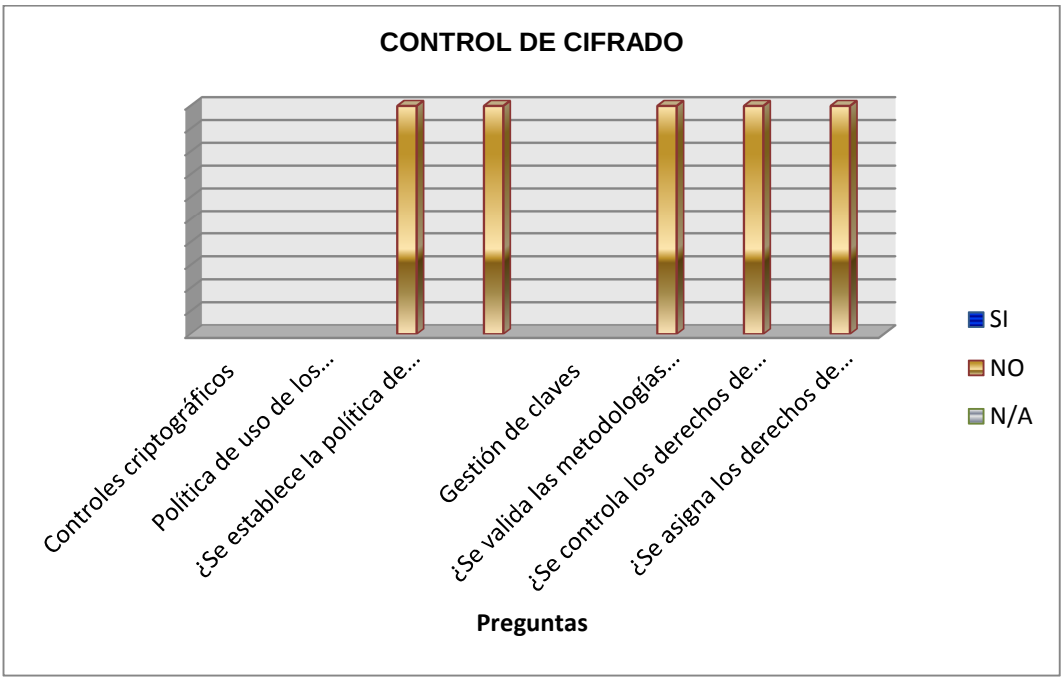


Ilustración 41 Seguridad física y del entorno Guille Sport

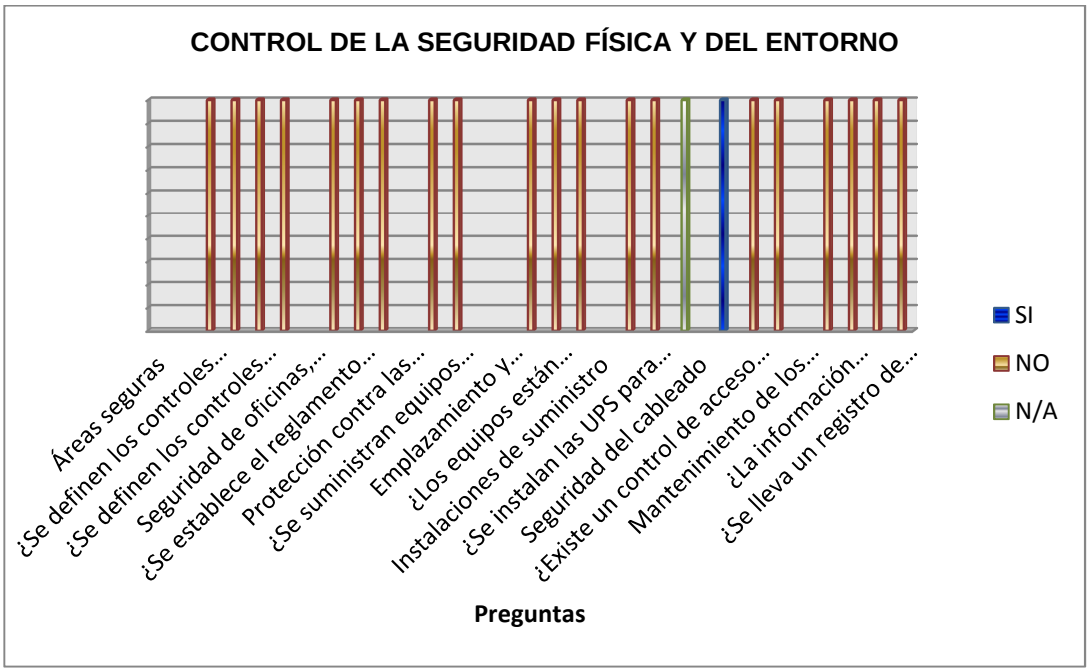


Ilustración 42 Seguridad en la operatividad Guille Sport

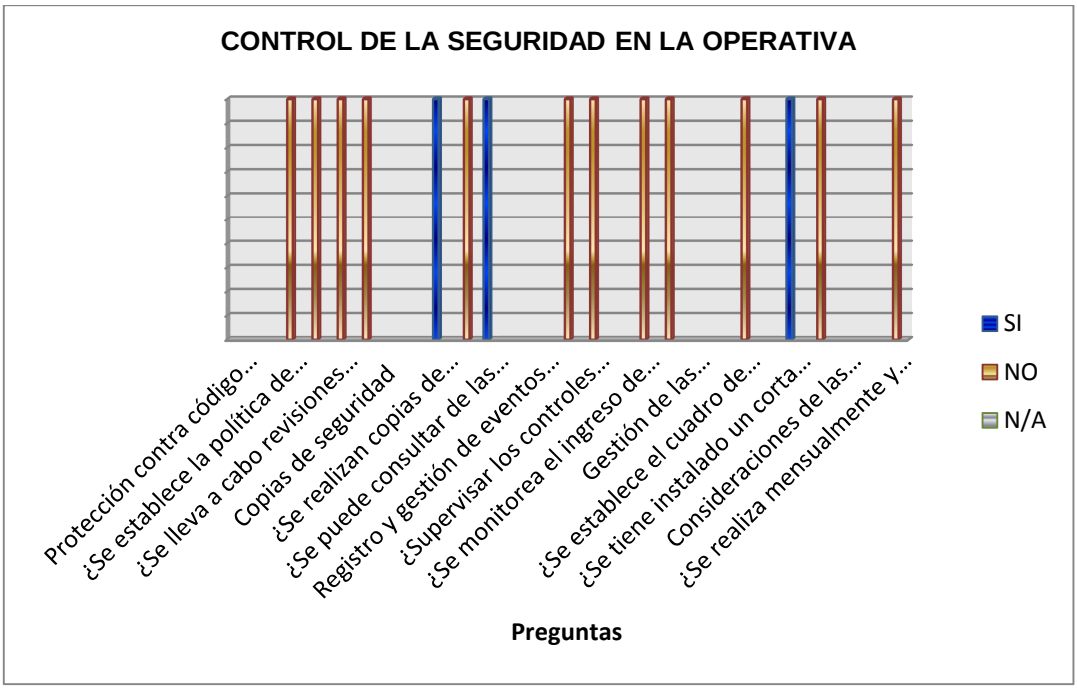


Ilustración 43 Seguridad en las telecomunicaciones Guille Sport

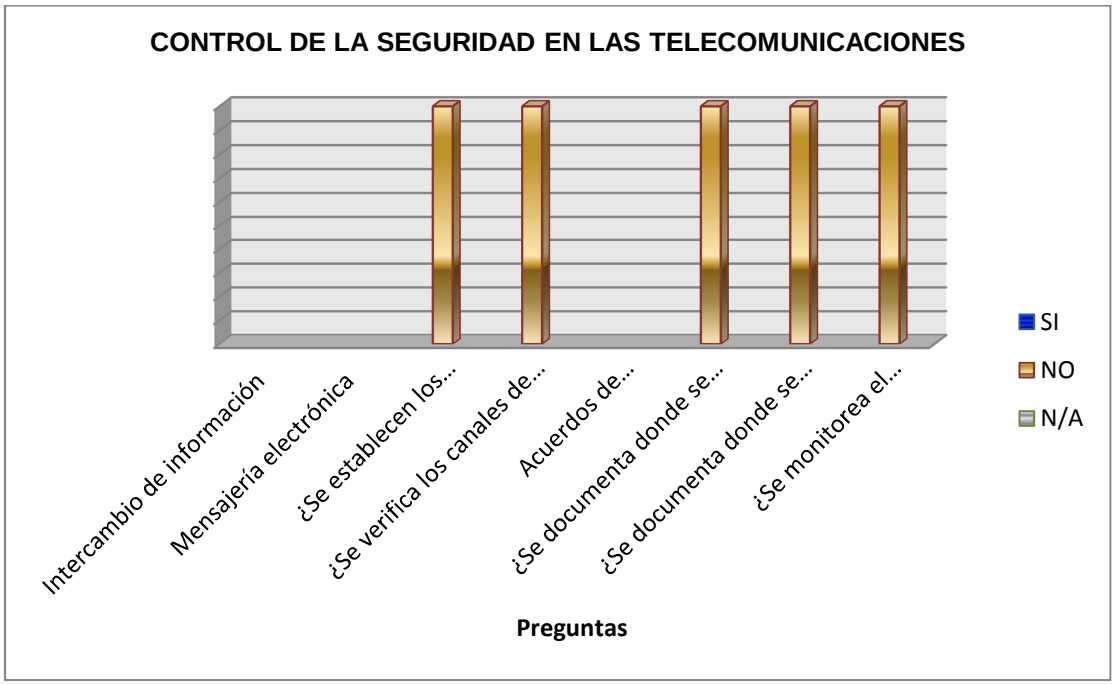


Ilustración 44 Gestión de incidentes en la seguridad de la información Guille Sport

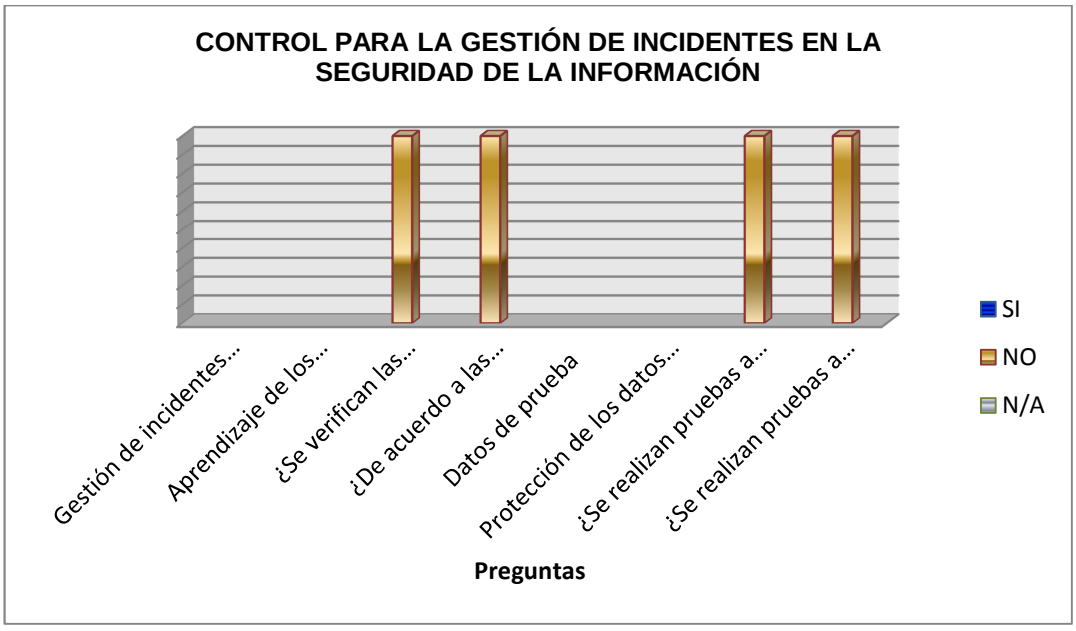


Ilustración 45 Adquisición, desarrollo y mantenimiento de los sistemas de información Guille Sport

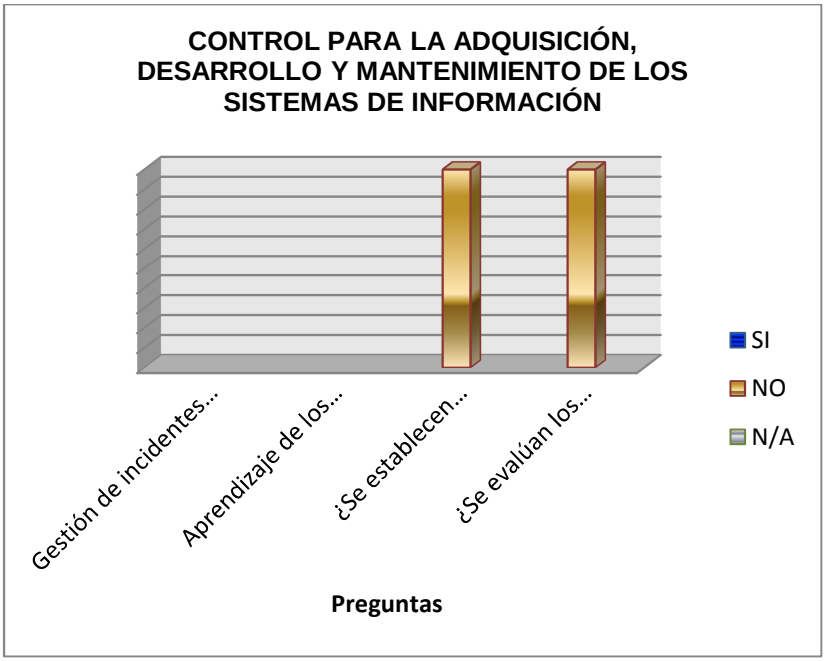


Ilustración 46 Aspectos de seguridad de la información en la gestión de la continuidad del negocio Guille Sport

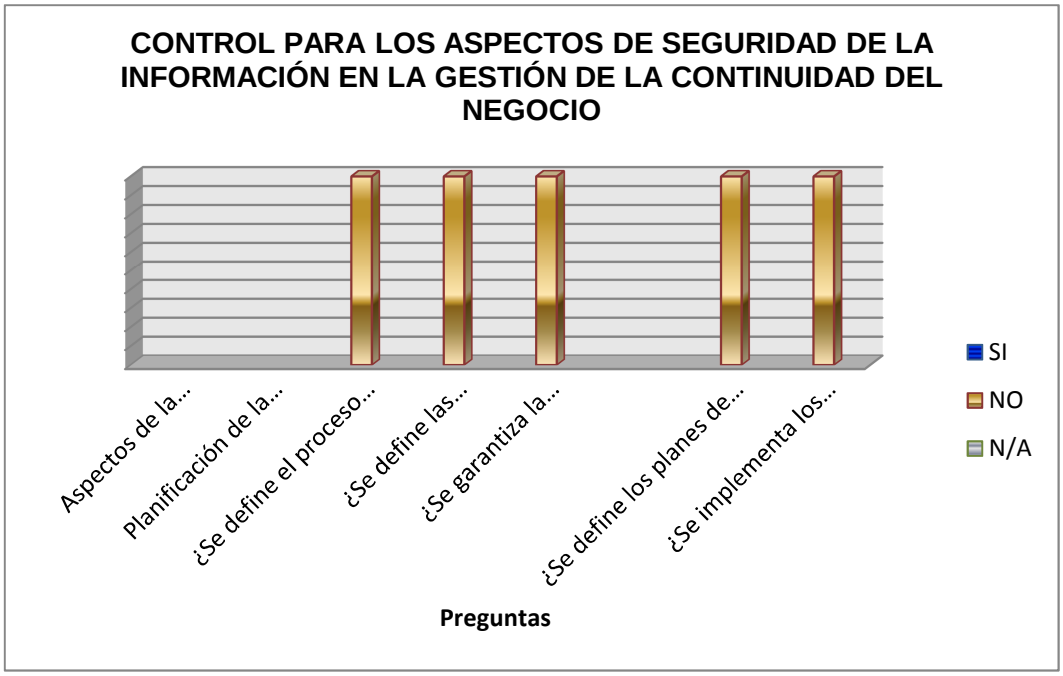
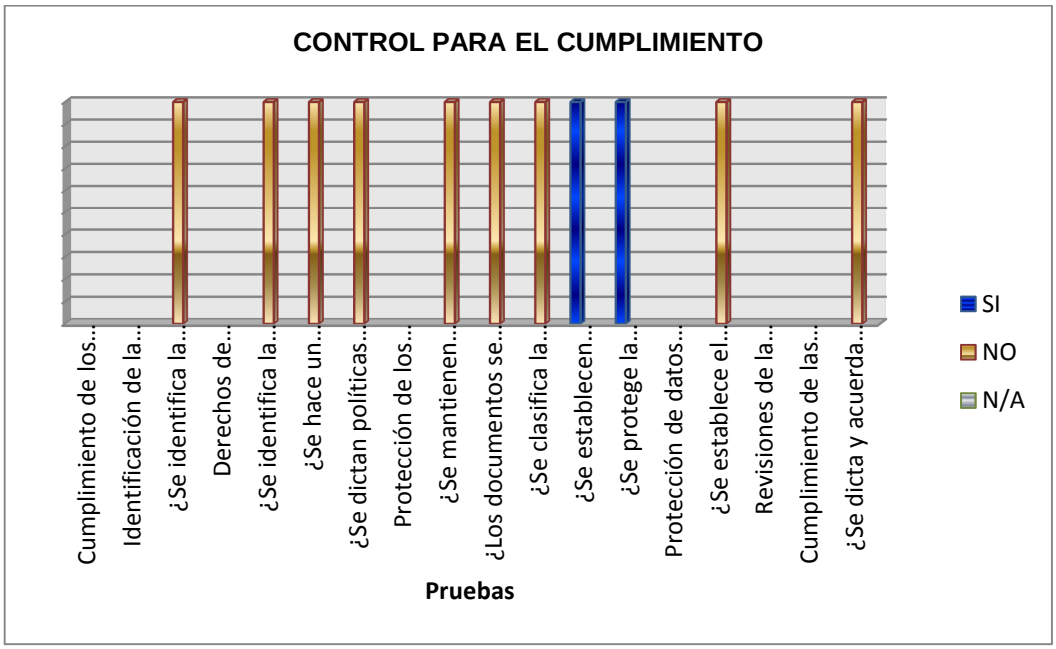


Ilustración 47 Cumplimiento Guille Sport



A través de las auditorias, visita preliminar y listas de chequeo se encontraron los siguientes hallazgos, con sus respectivas causas, recursos afectados y los controles por cada uno para determinar las posibles soluciones en prospectiva.

Tabla 59 Hallazgos Guille Sport

Ref.	Dominio/proceso	Hallazgo	Causas	Recursos afectados	Controles propuestos
5. POLÍTICA DE SEGURIDAD					
5.1. Política de Seguridad de la Información					
5.1.1	Conjunto de políticas para la seguridad de la información	No hay definida una política de seguridad de la información, ni objetivos ni alcance de seguridad, por ende no hay documentación ni procedimientos para ser revisados.	El desconocimiento de estándares y modelos de seguridad de la información, la visión de poca necesidad de proteger la información, la abnegación a la inversión en temas diferentes a la razón social.	La información, el buen nombre de la empresa, los equipos y procesos, y finalmente la compañía.	Establecer las políticas de seguridad de la información para la compañía
					Realizar revisiones periódicas de la política de seguridad
5.1.2	Revisión de las políticas para la seguridad de la información				Establecer objetivos, y alcance de la política de seguridad
					Hacerla de estricto cumplimiento para todos los colaboradores
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN					
6.1. Organización Interna					
6.1.1	Asignación de responsabilidades para la seguridad de la información	Se carece de procedimientos (documentos) para las actividades relacionadas con el manejo de la información. Nadie tiene	Exceso de confianza en el personal, desconocimiento de los riesgos y amenazas latentes al interior o exterior de la compañía. Organización por procesos y	La información, como activo más valioso, personal, equipos, procesos.	Documentar y definir los procesos de asignación y seguridad
					Asignar las responsabilidades a cada proceso de

		asignadas tareas que permitan controlar la manipulación de la información o hacerse responsable del buen uso de esta.	responsabilidades casi nulas, falta de compromiso de la dirección por la seguridad.		seguridad
6.1.2	Segregación de tareas				Definir los activos de información y asignar responsable
6.1.5	Seguridad de la información en la gestión de proyectos				Compromiso de la Dirección con la seguridad de la información
					Autorización por la dirección para la inversión de recursos, tiempos y formaciones
6.2. Dispositivos para movilidad y teletrabajo					
6.2.1.	Política de uso de dispositivos para movilidad	No hay existencia de política alguna para el control en la utilización de este tipo de dispositivos.	Falta de compromiso de la empresa para adoptar políticas relacionadas a la seguridad de la información	La información, las comunicaciones y los canales que esta emplea, los equipos.	Definir la política de seguridad para dispositivos móviles
6.2.2.	Teletrabajo				
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS					
7.2. Seguridad en el desempeño de las funciones del empleo (Durante la contratación)					
7.2.1	Responsabilidades de gestión	Personal poco capacitado en temas de seguridad, de manipulación de equipos de cómputo y de protección a los activos de información	Indiferencia por parte de la dirección para promover buenas prácticas en el manejo de equipos de cómputo y de la información, falta de capacitación y personal poco comprometido con la seguridad de la	La información, la credibilidad de la compañía, los equipos, los procesos.	Especificación de políticas de seguridad de información, involucrar al personal y hacer seguimiento
					Establecer las directrices sobre las funciones de seguridad informática.

7.2.2	Concienciación, educación y capacitación en seguridad de la información		información de la compañía, y poco consiente de hacer .un buen uso de los elementos informáticos.		Formación al personal en temas de seguridad de la información. Realizar capacitaciones sobre las amenazas, riesgos y vulnerabilidades Establecer los procesos de formación y concientización, diseñado para presentar las políticas de seguridad de la organización
8. GESTIÓN DE ACTIVOS					
8.1. Responsabilidad sobre los activos					
8.1.1	Inventario de Activos	Los activos no tiene responsables asignados y son accedidos y manipulados de manera incontrolada.	Falta de una definición clara de asignación de activos y responsables de su custodia y buen uso.	Equipos e información.	Mantener un inventario de activos definido. - Relación de riesgos con tipos de activos. - Mantener registro de personas y sus capacitaciones
8.1.2	Propiedad de los activos				Identificar el propietario de los activos y el responsable
8.1.3.	Uso aceptable de los activos				Informar a los empleados sobre el uso de los activos
8.1.4.	Devolución de activos				

8.2. Clasificación de la información					
8.2.1.	Directrices de clasificación	Los activos de información no pasan por unos procesos de documentación marcación asignación o clasificación, la información tampoco cuenta con procesos de organización o clasificación alguna.	Procesos inexistentes para clasificar, manipular o etiquetar la información	Información relevante.	Capacitar sobre cómo se debe enviar, y manipular las bases de información confidencial
8.2.2.	Etiquetado y manipulado de la información				Identificar y clasificar las fuentes de información
8.2.3.	Manipulación de activos				Documentar los activos de información.
9. CONTROL DE ACCESO					
9.1 Requerimientos de negocio para el control de acceso					
9.1.1	Política de control de acceso	El acceso a los equipos de cómputo se hace sin ningún tipo de control o restricción, no se define unos procesos para esto.	Falta de definición de controles de acceso a los equipos y recursos, no definir responsables para los activos y reglas de acceso a los mismos.	Equipos e información.	Definir la política de control de acceso para todos los usuarios de los equipos.
9.2. Gestión de acceso de usuario					
9.2.1	Gestión de altas/bajas en el registro de usuarios	Cualquier colaborador que desee ingresar a los equipos, lo hace sin restricciones, no se gestionan privilegios, debido a esto no hay implementada una gestión de altas y bajas de registros de usuarios.	No se tiene implementado un procedimiento para tal fin, no se define una política para gestión de accesos y privilegios a los usuarios.	Información relevante y/o sensible, equipos de cómputo, la continuidad del negocio.	Establecer privilegios de acceso a los usuarios según su rol y necesidad de acceder a la información.
					Verificar periódicamente que el nivel de acceso otorgado a cada usuario siga siendo el especificado en el documento.
					Verificar que el usuario

9.2.3	Gestión de los derechos de acceso con privilegios especiales				tenga autorización del dueño del sistema para el uso de la información.
9.3. Responsabilidades de usuario					
9.3.1	Uso de información confidencial para la autenticación	No se determina que información es confidencial, tampoco se le da un tratamiento a la misma para evitar fugas, o alteración de información.	No fijar procedimientos que indiquen la confidencialidad de la información.	La información, los equipos, el buen nombre de la compañía.	Definir políticas de seguridad para usuarios de los equipos. Establecer contratos con indicación de responsabilidad y confidencialidad sobre la información. Definir perfiles de usuario para el acceso a los equipos.
9.4. Control de acceso a sistemas operativo y aplicaciones					
9.4.1	Restricción del acceso a la información	No se evidencia procedimientos ni configuraciones para el inicio de sesión de usuarios a los equipos, los usuarios tienen acceso completo al sistema y a las aplicaciones instaladas.	Falta de definición de políticas que implementen reglas y configuraciones de inicio de sesión seguras, restricciones a personal no autorizado, o uso de herramientas del sistema sin autorización.	El sistema operativo y las aplicaciones, la información, los equipos de cómputo.	Implementar política de control de accesos Controlar los derechos de acceso de otras aplicaciones Establecer la política de autenticación a los equipos, con contraseñas personales y perfiles definidos. Regular la instalación de software en los equipos de cómputo personales, conforme a la política de seguridad de equipos
9.4.2	Procedimientos seguros de inicio de sesión				
9.5.4	Uso de herramientas de administración de sistemas				

					personales.
					Llevar un registro de todo uso de las utilidades del sistema
					Usar procedimientos de identificación, autenticación y autorización para las utilidades del sistema
10. CIFRADO					
10.1 Controles criptográficos					
10.1.1	Política de uso de los controles criptográficos	No se cifra o utiliza ningún tipo de procedimiento para cifrar datos o para gestionar claves de ningún tipo.	Interés bajo por parte de los propietarios por tener una política que permita mantener los activos de información lo más seguros posible.	La información, los equipos de cómputo-	Establecer la política de cifrado para las claves públicas y privadas en el manejo de información confidencial.
10.1.2	Gestión de claves				Controlar y asignar los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial.
11. SEGURIDAD FÍSICA Y DEL ENTORNO					
11.1. Áreas seguras					
11.1.2	Controles físicos de entrada	Hay libre acceso y tránsito por las oficinas donde se encuentran los equipos de cómputo, no se controla el acceso a estas, no se define una distribución de los activos o se adecuan	Exceso de confianza en el personal, falta de compromiso con la seguridad de los activos.	Equipos, información importante de la empresa, dispositivos externos.	Definición de controles físicos, técnicos y organizacionales para cada activo.
					Dictar la política de control de accesos conforme al SGSI.

11.1.3	Seguridad de oficinas, despachos y recursos	elementos necesarios para la protección de estos.			Definir la política de uso de las oficinas acorde a la política de gestión de acceso y del SGSI. Establecer el reglamento y las normas sobre las actividades y procesos informáticos.
11.1.4	Protección contra las amenazas externas y ambientales				Definición de un plan de respuesta para cada tipo de efecto que pudiera causar amenaza interna o externa. Suministrar equipos apropiados contra las amenazas ambientales y son ubicados adecuadamente.
11.2. Seguridad de los equipos					
11.2.1	Emplazamiento y protección de equipos	No se controla las temperaturas donde se encuentran los equipos de cómputo, el mantenimiento que se realiza es correctivo (solo cuando ocurre una incidencia que deja inoperativo el equipo), los equipos no cuentan con protección contra altas o bajas de tensión.	Desconocimiento de la importancia de mantener los equipos actualizados, con mantenimiento periódico, tener equipos de regulación de voltajes o UPS de contingencia, libres de temperaturas altas, o humedades en el ambiente.	Equipos de cómputo, dispositivos externos, información almacenada.	Regular y monitorear el uso de equipos personales a través de la política de uso de equipos personales. Distribuir los equipos donde sean accedidos solo por el personal autorizado. Aislar elementos que requieran protección especial
11.2.2	Instalaciones de				Establecer el plan de

	suministro				continuidad para este tipo de riesgos
11.2.3	Seguridad del cableado				Existe un control de acceso en los cuartos de cableado que soportan los sistemas críticos. Tienen rótulos de equipos y de cables claramente identificables para minimizar los errores en el manejo.
11.2.4	Mantenimiento de los equipos				Realizar mantenimiento acorde a los procesos de gestión de activos. Llevar un registro de todas las fallas reales y sospechosas.
12. SEGURIDAD EN LA OPERATIVA					
12.2. Protección contra código malicioso					
12.2.1	Controles contra el código malicioso	Los equipos carecen de sistemas de protección seguros contra código malicioso, están desactualizados de parches de seguridad y antivirus.	Falta de mantenimiento preventivo al sistema operativo y aplicaciones, licenciamiento del software inexistente.	Aplicaciones, Sistema Operativo, información, discos duros y dispositivos externos.	Establecer la política de seguridad de equipos personales en la que se previene el uso de programas no autorizados por la empresa. Regular el uso de software antivirus y su actualización. Llevar a cabo revisiones mensuales sobre el contenido del software y

					los datos que soportan los procesos críticos del negocio.
					Investigar la aparición de archivos o códigos no autorizados y aprobados por el desarrollador del software y/o aplicación.
12.3. Copias de seguridad					
12.3.1	Copias de seguridad de la información	Las copias de seguridad a la información importante, se realizan en dispositivos extraíbles, y se dejan conectados al equipo., donde cualquiera puede tomarlos	Falta de control de acceso a las oficinas y equipos de cómputo.	Dispositivos extraíbles, la información de la compañía.	Realizar copias de seguridad de manera periódica sobre la información registrada en las oficinas – Backup.
					Almacenar las copias de seguridad en lugares seguros y evitar que queden al alcance de personas no autorizadas.
12.4. Registro de actividad y supervisión					
12.4.1	Registro y gestión de eventos de actividad	La actividad en los activos de información no se monitorea, y no hay una administración clara de los sistemas.	No se definen procedimientos para esta actividad.	Información equipos, dispositivos extraíbles.	Supervisar los controles definidos al uso de equipos personales.
					Monitorear los cambios de configuración del sistema.
12.4.3	Registros de actividad del administrador y				Monitorear el ingreso de usuarios a las diferentes aplicaciones.

	operador del sistema				Registrar las alertas o fallas del sistema, como mensajes de consola.
12.6 Gestión de las vulnerabilidades técnicas					
12.6.1	Gestión de las vulnerabilidades técnicas	Restricciones inexistentes al sistema de los equipos, no se data ni se controlan las vulnerabilidades.	No hay política de seguridad establecida para estos procesos	El sistema, las aplicaciones, la información, los equipos	Establecer un cuadro de control o cuadro de mando que evidencie los riesgos asociados a la organización.
12.6.2	Restricciones en la instalación de sistema operativo (S.O.)				Instalación de corta fuegos y asignación de privilegios a cada usuario conforme a su perfil o cargo.
12.7 Consideraciones de las auditorías de los sistemas de información					
12.7.1	Controles de auditoría de los sistemas de información	No se audita ningún proceso relacionado con los activos de información.	No hay procedimientos de auditoría establecidos en la compañía.	Equipos, información.	Realizar mensualmente y trimestralmente una auditoría interna por los procesos de seguridad que se han implementado en la organización.
13. SEGURIDAD EN LAS TELECOMUNICACIONES					
13.2 Intercambio de información					
13.2.3	Mensajería electrónica	Los contratos no especifican mantener confidencialidad de la información de la empresa, no se realiza soporte a los procesos de transmisión de información	Políticas y procedimientos inexistentes en la compañía.	Información, buen nombre de la empresa.	Establecer los protocolos para enviar la información por los canales de comunicación.
					Verificar los canales de comunicación

		de manera electrónica.			mensualmente identificando los canales de transmisión por el internet.
13.2.4	Acuerdos de confidencialidad y secreto				Definir documento donde se establecen los acuerdos de confidencialidad.
					Definir documento donde se establecen las políticas de confidencialidad.
					Hacer seguimiento al cumplimiento de los acuerdos.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN					
14.1 Requisitos de seguridad de los sistemas de información					
14.1.1	Análisis y especificación de los requisitos de seguridad	No se plantea ningún requisito pertinente a la seguridad de la información, es un tema desconocido en la compañía.	Desconocimiento, falta de compromiso con la seguridad de la información.	Equipos, información relevante, el buen nombre de la compañía.	Mantener los sistemas actualizados, buscando identificar las amenazas, riesgos y vulnerabilidades asociados a los activos de información.
					Elaborar documento con especificaciones de los requisitos de seguridad para los sistemas de información.
14.3 Datos de prueba					

14.3.1	Protección de los datos utilizados en pruebas	No se ejecutan pruebas a los sistemas y a la información que interactúa con estos.	No existen procedimientos, protocolos o políticas para efectuar las actividades de pruebas.	Información relevante de la empresa	Definir un plan de pruebas a los activos informáticos, estableciendo las mejores alternativas para mitigar los riesgos.
					Definir un plan de pruebas a las pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN					
16.1. Gestión de incidentes de seguridad de la información y mejoras					
16.1.6	Aprendizaje de los incidentes de seguridad de la información	No se gestionan incidentes de seguridad de la información.	Desconocimiento sobre procesos, normas, estándares y buenas prácticas de la seguridad de la información.	Equipos de cómputo, dispositivos externos, información almacenada.	Establecer procesos de resolución de incidentes de seguridad de la información, bien sea de manera reactiva o proactiva.
					Implementar herramientas para evaluar los incidentes de seguridad.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
17.1. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio					
17.1.1	Planificación de la continuidad de la seguridad de la información	No se cuenta con planes de acción o de contingencia, ni documentación que permita mantener el	No se ve la seguridad de los activos de información, como una inversión o implementación necesaria en la compañía.	Toda la compañía y sus activos.	Definir el proceso de gestión de continuidad del negocio y las directrices de continuidad del negocio

		funcionamiento de la empresa ante la ocurrencia de riesgos o amenazas.			de conformidad con la política de seguridad de la información.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información				Definir e implantar los planes de continuidad del negocio de acuerdo al orden de prioridades, en los términos presentados en la instrucción de continuidad del negocio.
18. CUMPLIMIENTO					
18.1. Cumplimiento de los requisitos legales y contractuales					
18.1.1	Identificación de la legislación aplicable	No se cuenta con software licenciado, la información del personal es de fácil acceso en los equipos de cómputo, los registros no son bien custodiados.	Ahorro en adquisición de licencias, desconocimiento de la parte legal, exceso de confianza.	Registros físicos y lógicos, equipos, información personal, la compañía.	Identificar la legislación que aplica para los procesos que intervienen en el manejo de la información.
18.1.2	Derechos de propiedad intelectual (DPI)				Identificar la legislación aplicable y los términos contractuales en las licencias utilizadas
18.1.3	Protección de los registros de la organización				Hacer un inventario de software para garantizar la idoneidad de su uso. Dictar política de cumplimiento.
					Clasificar la información en función de su importancia.

					Establecer copias de seguridad de la información relevante, proteger en armarios o cajones bajo llave la información física sensible de pérdida.
18.1.4	Protección de datos y privacidad de la información personal				Establecer el documento de seguridad de conformidad con la legislación de protección de datos personales.
18.2. Revisiones de la seguridad de la información					
18.2.2	Cumplimiento de las políticas y normas de seguridad	No existe una política de seguridad de la información.	Desconocimiento, descuido, poco interesen la implementación de la política.	Todos los activos de la empresa.	Dictar y acordar la política del sistema de gestión de la seguridad informática – SGSI.

Ilustración 48 Política de seguridad de la información Color Shop

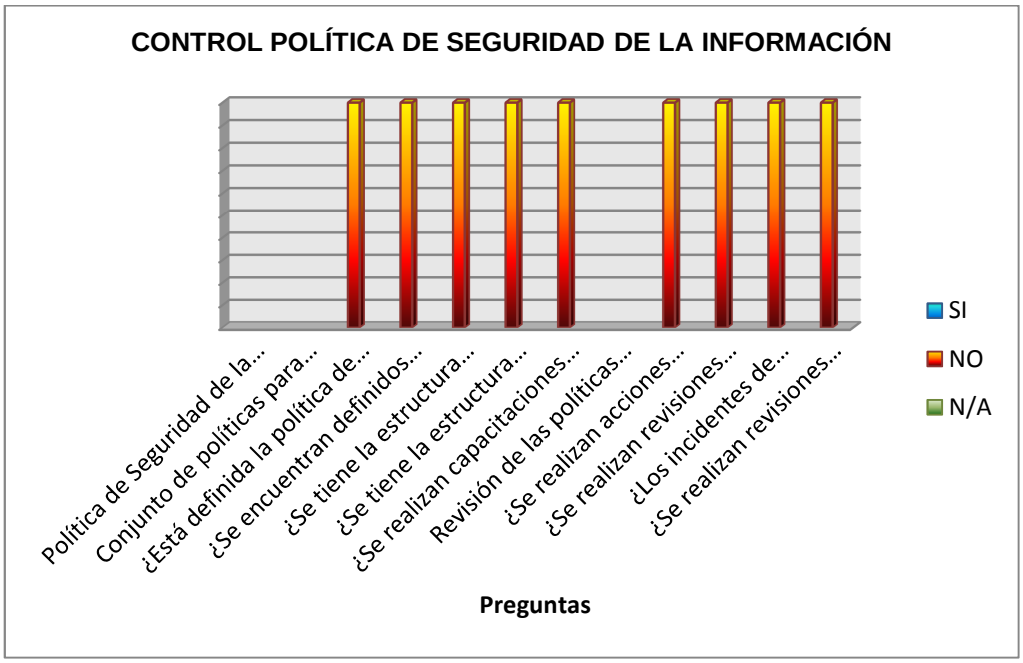


Ilustración 49 Aspectos organizativos de la seguridad de la información Color Shop

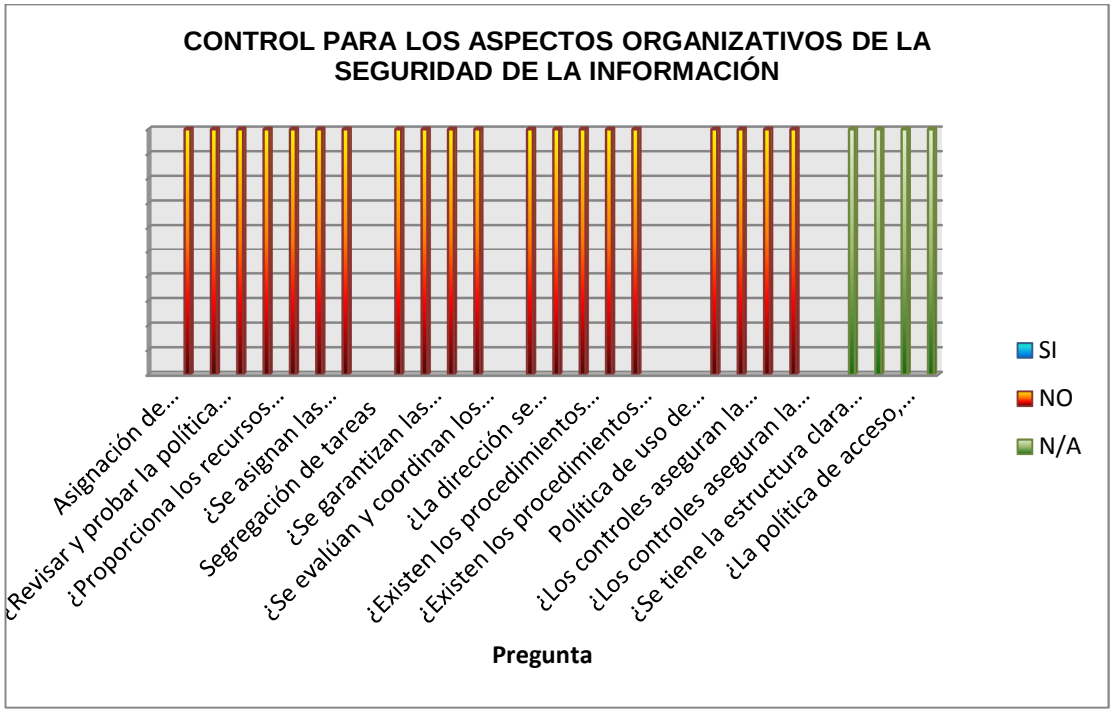


Ilustración 50 Seguridad ligada a los recursos humanos Color Shop

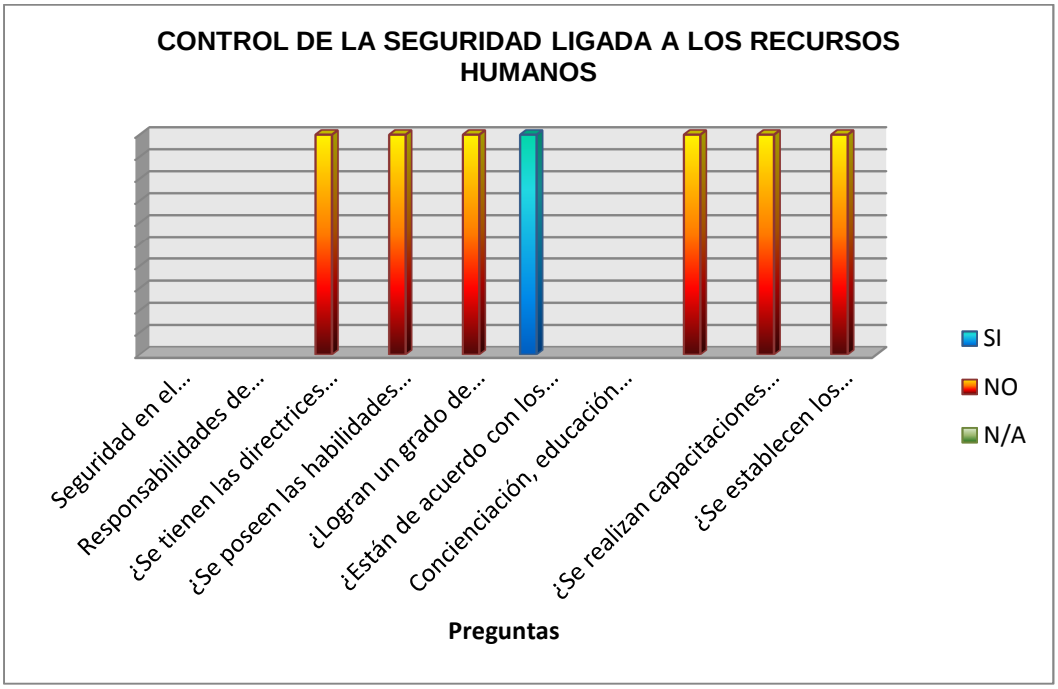


Ilustración 51 Gestión de activos Color Shop

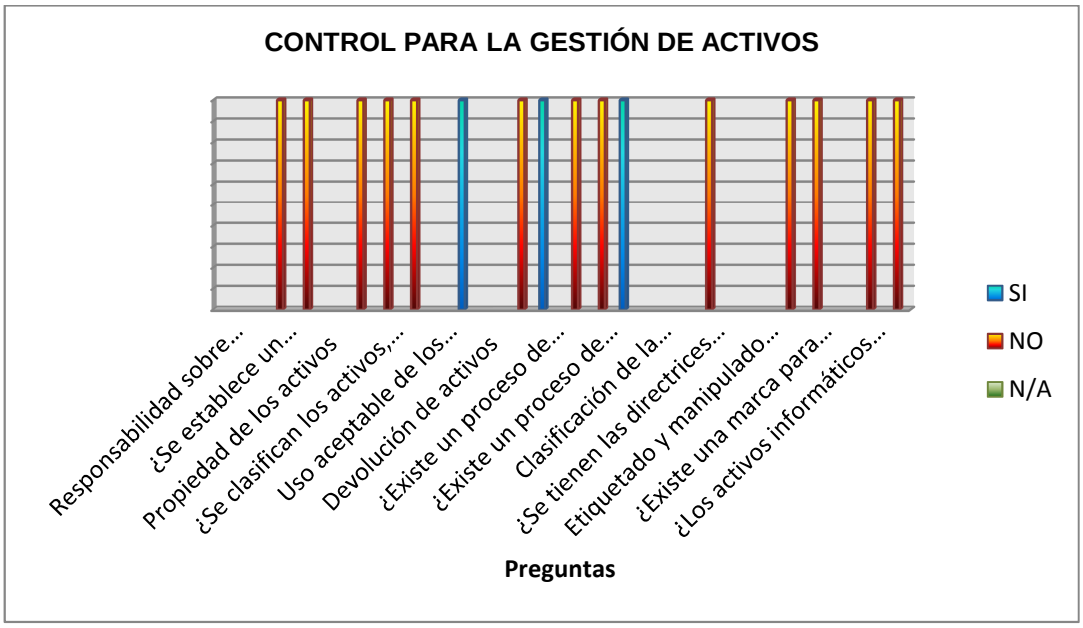


Ilustración 52 Control de acceso Color Shop

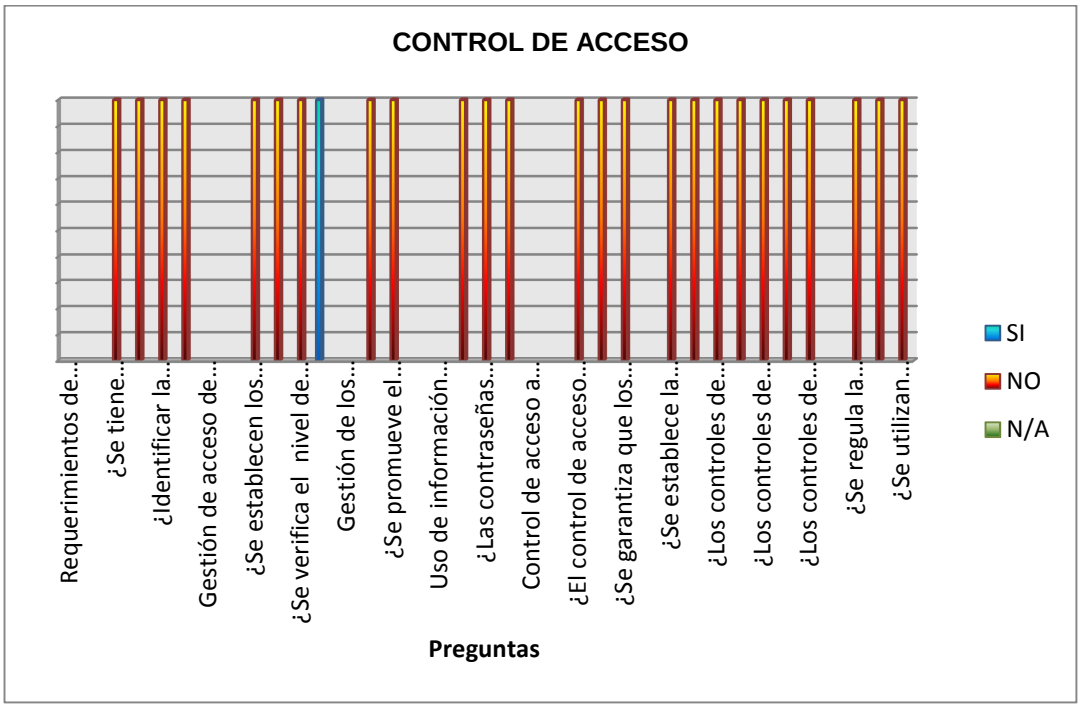


Ilustración 53 Cifrado Color Shop

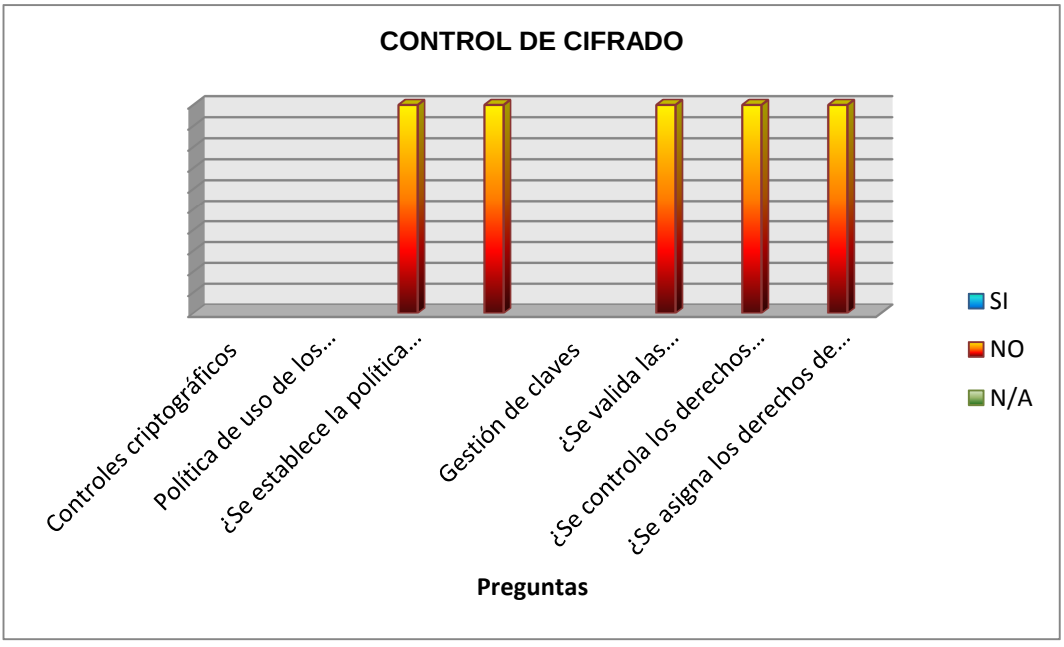


Ilustración 54 Seguridad física y del entorno Color Shop

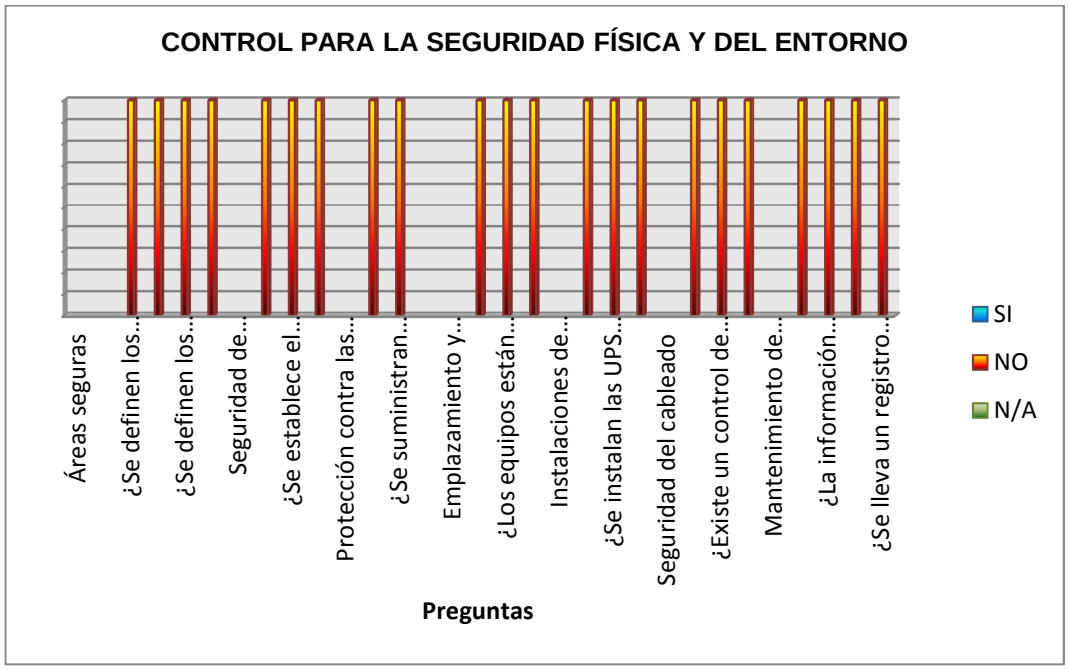


Ilustración 55 Seguridad en la operativa Color Shop

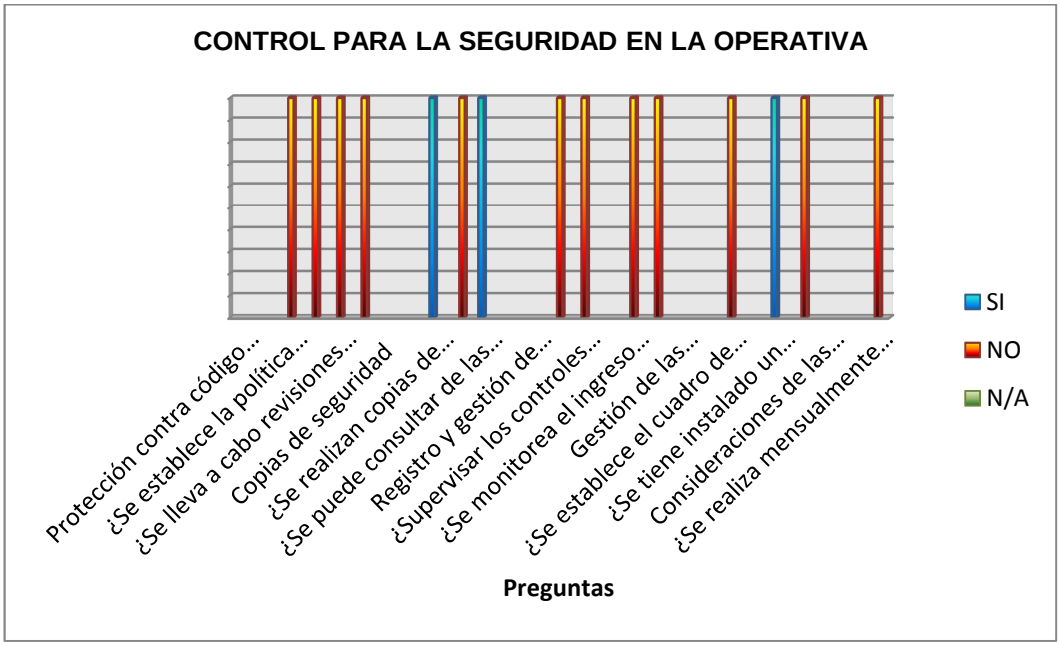


Ilustración 56 Seguridad en las telecomunicaciones Color Shop

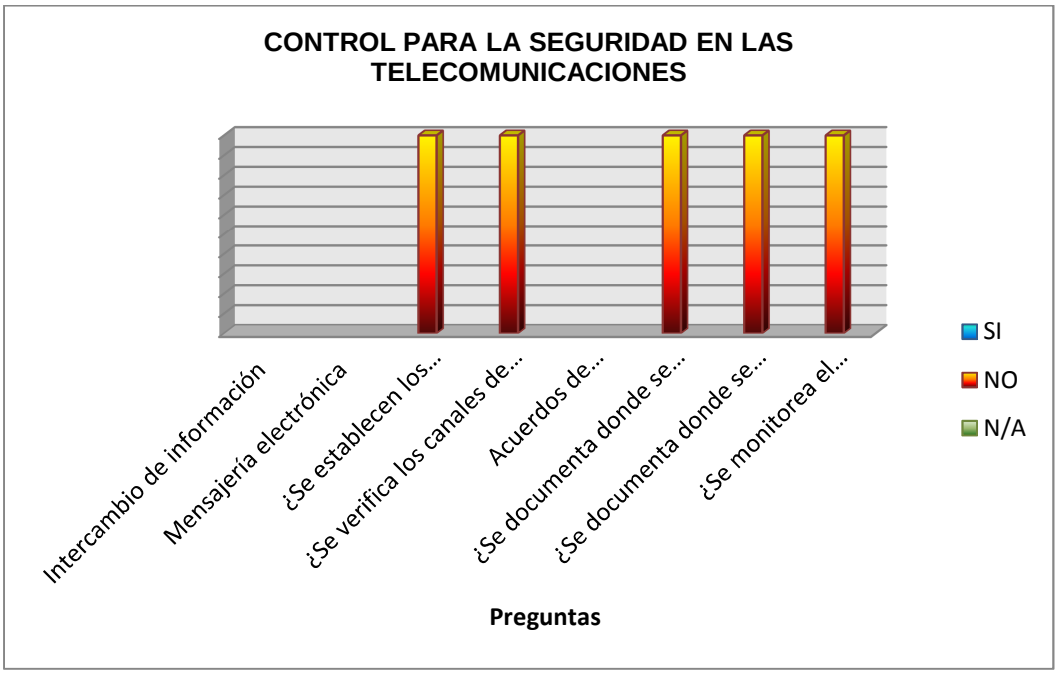


Ilustración 57 Gestión de incidentes en la seguridad de la información Color Shop

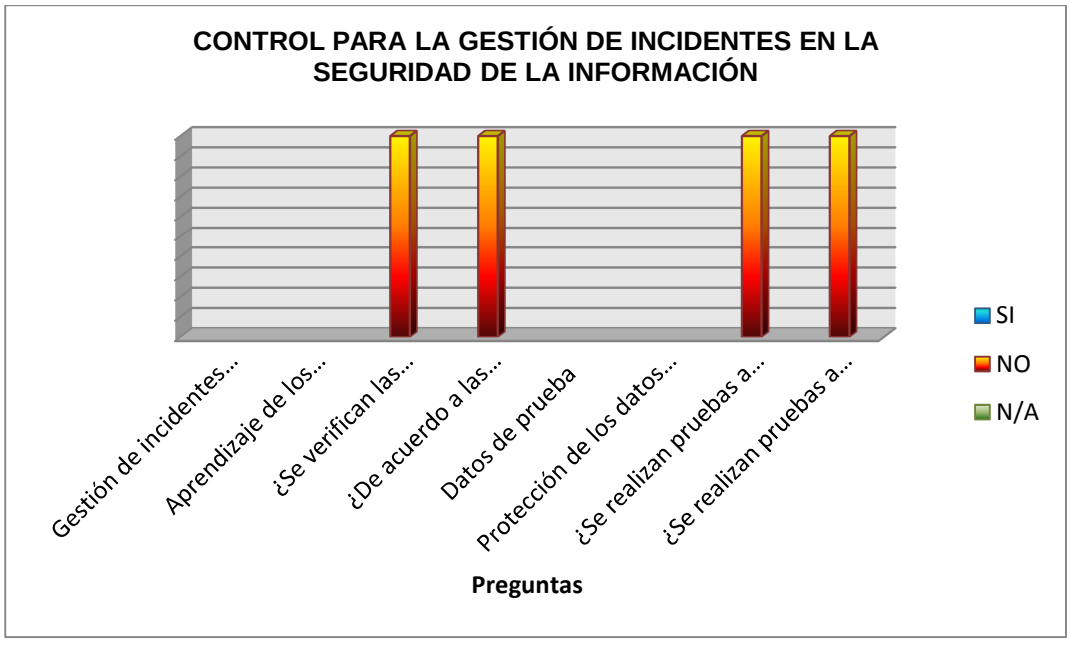


Ilustración 58 Adquisición, desarrollo y mantenimiento de los sistemas de información Color Shop

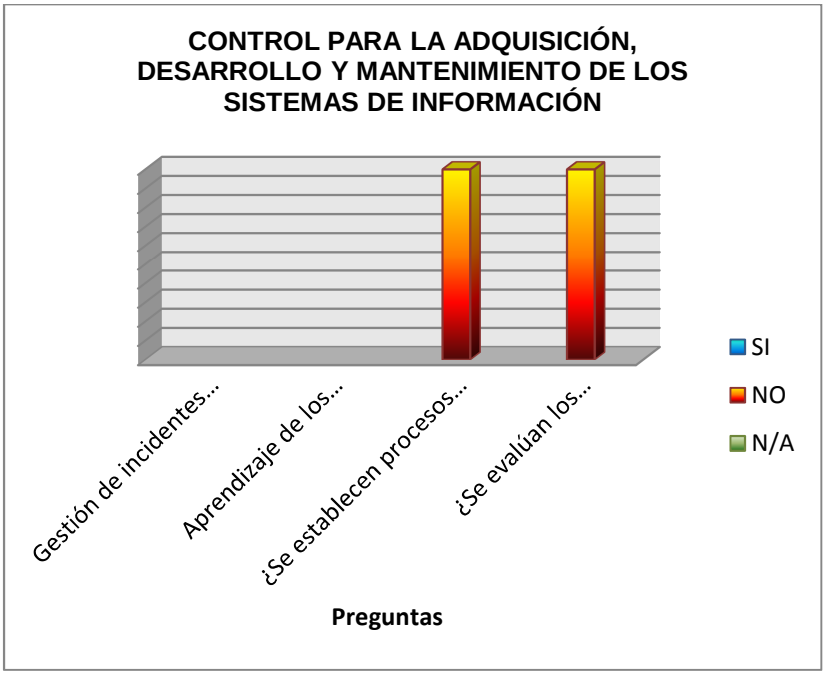


Ilustración 59 Aspectos de seguridad de la información en la gestión de la continuidad del negocio Color Shop

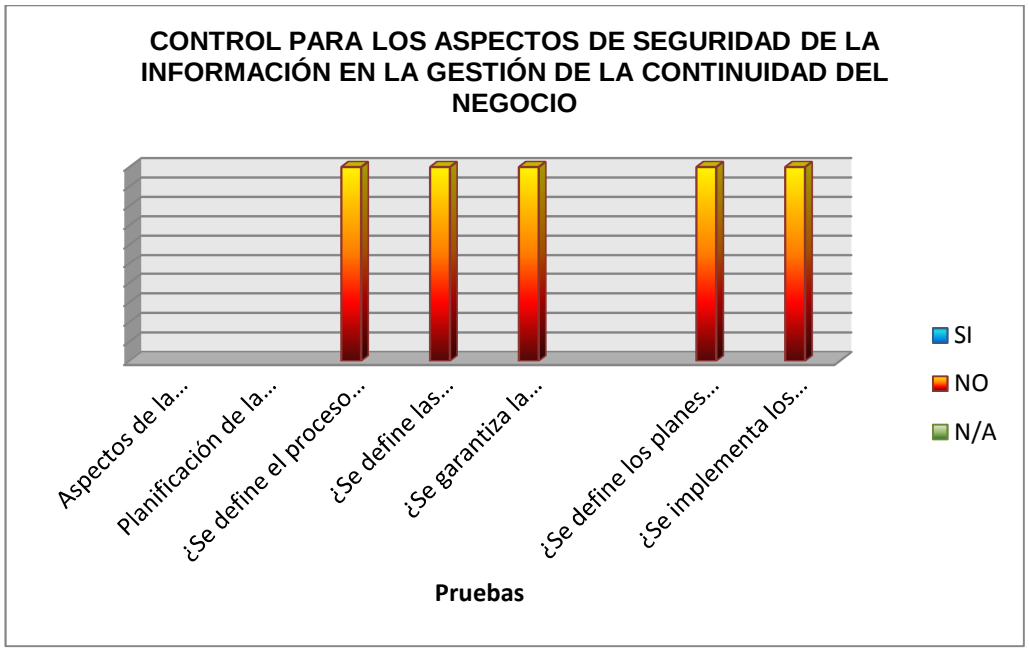
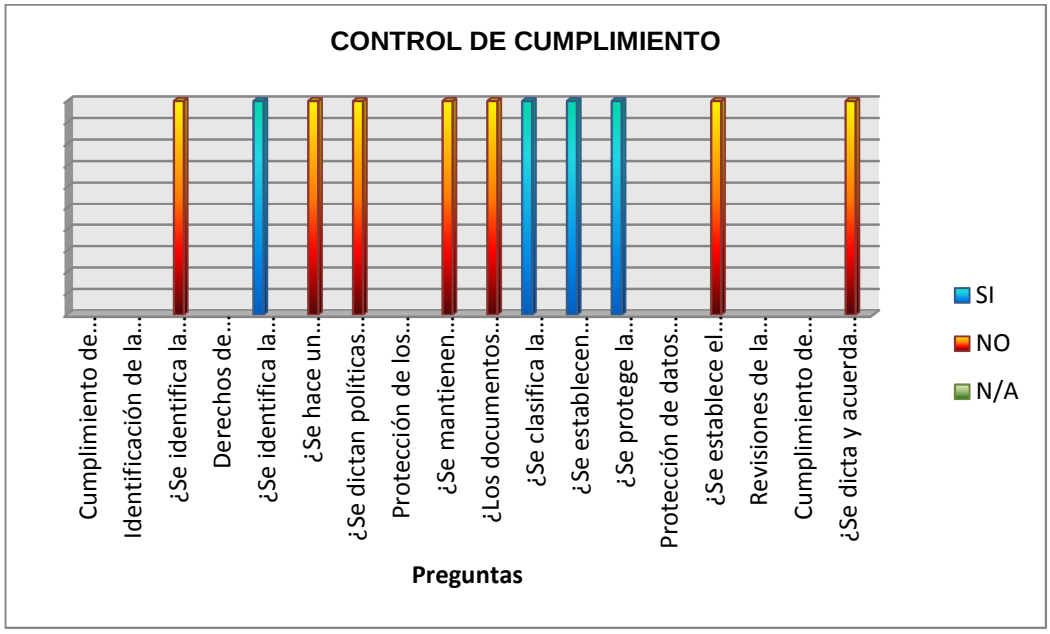


Ilustración 60 Cumplimiento Color Shop



A través de las auditorias, visita preliminar y listas de chequeo se encontraron los siguientes hallazgos, con sus respectivas causas, recursos afectados y los controles por cada uno para determinar las posibles soluciones en prospectiva.

Tabla 60 Hallazgos Color Shop

REF.	Dominio/proceso	Hallazgo	Causas	Recursos afectados	Controles propuestos
5. POLÍTICA DE SEGURIDAD					
5.1. Política de Seguridad de la Información					
5.1.1	Conjunto de políticas para la seguridad de la información	No se cuenta con una política de seguridad de la información, no se definen objetivos, ni alcance de un sistema de seguridad, no hay documentación relacionada a la seguridad de activos de información.	Desinterés por parte de la dirección en la adopción de modelos y estándares para proteger la información al ser temas desconocidos, visión incorrecta del costo-beneficio que representa la implementación de la política de seguridad	La información, el buen nombre de la empresa, los equipos y procesos, y finalmente la compañía.	Establecer las políticas de seguridad de la información para la compañía
					Realizar revisiones periódicas de la política de seguridad
5.1.2	Revisión de las políticas para la seguridad de la información				Establecer objetivos, y alcance de la política de seguridad
					Hacerla de estricto cumplimiento para todos los colaboradores
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN					
6.1. Organización Interna					
6.1.1	Asignación de responsabilidades para la seguridad de	Se carece de procedimientos (documentos) para las	Exceso de confianza en el personal, desconocimiento de los	La información, como activo más valioso, personal,	Documentar y definir los procesos de asignación y seguridad

	la información	actividades relacionadas con el manejo de la información. Nadie tiene asignadas tareas que permitan controlar la manipulación de la información o hacerse responsable del buen uso de esta.	riesgos y amenazas latentes al interior o exterior de la compañía. Organización por procesos y responsabilidades casi nulas, falta de compromiso de la dirección por la seguridad.	equipos, procesos.	Asignar las responsabilidades a cada proceso de seguridad
6.1.2	Segregación de tareas				Definir los activos de información y asignar responsable
6.1.5	Seguridad de la información en la gestión de proyectos				Compromiso de la Dirección con la seguridad de la información
					Autorización por la dirección para la inversión de recursos, tiempos y formaciones
6.2. Dispositivos para movilidad y teletrabajo					
6.2.1.	Política de uso de dispositivos para movilidad	No hay existencia de política alguna para el control en la utilización de este tipo de dispositivos.	Falta de compromiso de la empresa para adoptar políticas relacionadas a la seguridad de la información	La información, las comunicaciones y los canales que esta emplea, los equipos.	Definir la política de seguridad para dispositivos móviles
6.2.2.	Teletrabajo				
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS					
7.2. Seguridad en el desempeño de las funciones del empleo (Durante la contratación)					

7.2.1	Responsabilidades de gestión	Personal poco capacitado en temas de seguridad, de manipulación de equipos de cómputo y de protección a los activos de información	Poco interés por parte de la dirección en la implementación de espacios de capacitación. Falta de procedimientos para la asignación de responsabilidades en la gestión.	La información, la credibilidad de la compañía, los equipos, los procesos.	Especificación de políticas de seguridad de información, involucrar al personal y hacer seguimiento
					Establecer las directrices sobre las funciones de seguridad informática.
7.2.2	Concienciación, educación y capacitación en seguridad de la información				Formación al personal en temas de seguridad de la información.
					Realizar capacitaciones sobre las amenazas, riesgos y vulnerabilidades
					Establecer los procesos de formación y concientización, diseñado para presentar las políticas de seguridad de la organización
8. GESTIÓN DE ACTIVOS					
8.1. Responsabilidad sobre los activos					
8.1.1	Inventario de Activos	No hay unos procesos de inventario, asignación de responsables,	Falta de una definición clara de asignación de activos y responsables de su custodia y buen	Equipos e información.	Mantener un inventario de activos definido. - Relación de riesgos con tipos de activos. -

		propietarios y usos de los activos.	uso.		Mantener registro de personas y sus capacitaciones
8.1.2	Propiedad de los activos				Identificar el propietario de los activos y el responsable
8.1.3.	Uso aceptable de los activos				
8.1.4.	Devolución de activos				Informar a los empleados sobre el uso de los activos
8.2. Clasificación de la información					
8.2.1.	Directrices de clasificación	Los activos de información no pasan por unos procesos de documentación marcación asignación o clasificación, la información tampoco cuenta con procesos de organización o clasificación alguna.	Procesos inexistentes para clasificar, manipular o etiquetar la información	información relevante.	Capacitar sobre cómo se debe enviar, y manipular las bases de información confidencial
8.2.2.	Etiquetado y manipulado de la información				Identificar y clasificar las fuentes de información
8.2.3.	Manipulación de activos				Documentar los activos de información.
9. CONTROL DE ACCESO					
9.1 Requerimientos de negocio para el control de acceso					

9.1.1	Política de control de acceso	No existe restricción para el acceso a equipos o aplicaciones,	No hay definida una política que permita regular el acceso de acuerdo a roles y perfiles.	Equipos e información.	Definir la política de control de acceso para todos los usuarios de los equipos.
9.2. Gestión de acceso de usuario					
9.2.1	Gestión de altas/bajas en el registro de usuarios	El acceso a los equipos de cómputo se hace sin ningún tipo de control o restricción.	No hay definida una política para gestión de accesos y privilegios a los usuarios.	Información relevante y/o sensible, equipos de cómputo, la continuidad del negocio.	Establecer privilegios de acceso a los usuarios según su rol y necesidad de acceder a la información.
					Verificar periódicamente que el nivel de acceso otorgado a cada usuario siga siendo el especificado en el documento.
9.2.3	Gestión de los derechos de acceso con privilegios especiales				Verificar que el usuario tenga autorización del dueño del sistema para el uso de la información.
9.3. Responsabilidades de usuario					
9.3.1	Uso de información confidencial para la autenticación	La información es tratada toda con el mismo criterio, el personal la puede	No fijar procedimientos que indiquen la confidencialidad de la información,	La información, los equipos, el buen nombre de la compañía.	Definir políticas de seguridad para usuarios de los equipos.

		acceder cuando se utiliza el sistema, la contraseña de ingreso al equipo del propietario es conocida por varias personas.	especialmente la referente a la autenticación en los activos de información.		Establecer contratos con indicación de responsabilidad y confidencialidad sobre la información.
					Definir perfiles de usuario para el acceso a los equipos.
9.4. Control de acceso a sistemas operativo y aplicaciones					
9.4.1	Restricción del acceso a la información	No hay control alguno para el acceso a los equipos, no se tiene configuración de inicio de sesión en estos, se puede acceder a las herramientas administrativas del sistema sin ninguna restricción.	Falta de definición de políticas que implementen reglas y configuraciones de inicio de sesión seguras, restricciones a personal no autorizado, o uso de herramientas del sistema sin autorización.	El sistema operativo y las aplicaciones, la información, los equipos de cómputo.	Implementar política de control de accesos
					Controlar los derechos de acceso de otras aplicaciones
9.4.2	Procedimientos seguros de inicio de sesión				Establecer la política de autenticación a los equipos, con contraseñas personales y perfiles definidos.
9.5.4	Uso de herramientas de administración de sistemas				Regular la instalación de software en los equipos de cómputo personales, conforme a la política de seguridad de equipos personales.
					Llevar un registro de todo uso de las utilidades del sistema

					Usar procedimientos de identificación, autenticación y autorización para las utilidades del sistema
10. CIFRADO					
10.1 Controles criptográficos					
10.1.1	Política de uso de los controles criptográficos	No se cifra o utiliza ningún tipo de procedimiento para cifrar datos o para gestionar claves de ningún tipo.	Falta una política de seguridad para el proceso.	La información, los equipos de cómputo-	Establecer la política de cifrado para las claves públicas y privadas en el manejo de información confidencial.
10.1.2	Gestión de claves				Controlar y asignar los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial.
11. SEGURIDAD FÍSICA Y DEL ENTORNO					
11.1. Áreas seguras					
11.1.2	Controles físicos de entrada	Hay libre acceso y tránsito por las oficinas donde se encuentran los equipos de cómputo, no se controla el acceso a estas, no se define una distribución	Exceso de confianza en el personal, falta de compromiso con la seguridad de los activos.	Equipos, información importante de la empresa, dispositivos externos.	Definición de controles físicos, técnicos y organizacionales para cada activo.
					Dictar la política de control de accesos conforme al SGSI.

11.1.3	Seguridad de oficinas, despachos y recursos	de los activos o se adecuan elementos necesarios para la protección de estos.			Definir la política de uso de las oficinas acorde a la política de gestión de acceso y del SGSI.
					Establecer el reglamento y las normas sobre las actividades y procesos informáticos.
11.1.4	Protección contra las amenazas externas y ambientales				Definición de un plan de respuesta para cada tipo de efecto que pudiera causar amenaza interna o externa.
					Suministrar equipos apropiados contra las amenazas ambientales y son ubicados adecuadamente.
11.2. Seguridad de los equipos					
11.2.1	Emplazamiento y protección de equipos	No se identifica un sitio seguro para la protección de los equipos, el mantenimiento que se realiza es correctivo, las locaciones no cuentan con sistemas de	Falta de un plan de mantenimiento preventivo a los equipos, inexistencia de dispositivos de regulación de voltajes, temperaturas altas dentro de la compañía	Equipos de cómputo, dispositivos externos, información almacenada.	Regular y monitorear el uso de equipos personales a través de la política de uso de equipos personales.
					Distribuir los equipos donde sean accedidos solo por el personal

		enfriamiento adecuado para mantener la temperatura ideal que permita la protección de los equipos de cómputo.	sin sistemas de regulación para las mismas.		autorizado.
					Aislar elementos que requieran protección especial
11.2.2	Instalaciones de suministro				Establecer el plan de continuidad para este tipo de riesgos
11.2.3	Seguridad del cableado				Tienen rótulos de equipos y de cables claramente identificables para minimizar los errores en el manejo.
11.2.4	Mantenimiento de los equipos				Realizar mantenimiento acorde a los procesos de gestión de activos.
					Llevar un registro de todas las fallas reales y sospechosas.
12. SEGURIDAD EN LA OPERATIVA					
12.2. Protección contra código malicioso					
12.2.1	Controles contra el código malicioso	Los equipos cuentan con antivirus, pero se encuentran	Falta de actualización a los equipos y aplicaciones, con los	Aplicaciones, Sistema Operativo,	Establecer la política de seguridad de equipos personales en

		desactualizados, no hay herramientas diferentes como protección contra el código malicioso.	parches y controladores más recientes.	información, discos duros y dispositivos externos.	la que se previene el uso de programas no autorizados por la empresa. Regular el uso de software antivirus y su actualización.
					Llevar a cabo revisiones mensuales sobre el contenido del software y los datos que soportan los procesos críticos del negocio.
					Investigar la aparición de archivos o códigos no autorizados y aprobados por el desarrollador del software y/o aplicación.
12.3. Copias de seguridad					
12.3.1	Copias de seguridad de la información	Se hacen copias de seguridad, pero en dispositivos extraíbles, corriendo el riesgo de pérdida de estos en el transporte de un lugar a	No se ha determinado la mejor manera de mantener copias de seguridad, y en lugares seguros.	Dispositivos extraíbles, la información de la compañía.	Realizar copias de seguridad de manera periódica sobre la información registrada en las oficinas – Backup.

		otro.			Almacenar las copias de seguridad en lugares seguros y evitar que queden al alcance de personas no autorizadas.
12.4. Registro de actividad y supervisión					
12.4.1	Registro y gestión de eventos de actividad	No se administra el sistema en los equipos de cómputo, no se registra de ninguna manera eventos de actividad en los mismos.	No se definen procedimientos para esta actividad.	Información equipos, dispositivos extraíbles.	Supervisar los controles definidos al uso de equipos personales.
					Monitorear los cambios de configuración del sistema.
12.4.3	Registros de actividad del administrador y operador del sistema				Monitorear el ingreso de usuarios a las diferentes aplicaciones.
					Registrar las alertas o fallas del sistema, como mensajes de consola.
12.6 Gestión de las vulnerabilidades técnicas					
12.6.1	Gestión de las vulnerabilidades técnicas	No hay documentos donde se plasmen las vulnerabilidades técnicas, no hay	No existe una política de seguridad establecida para estos procesos	El sistema, las aplicaciones, la información, los equipos	Establecer un cuadro de control o cuadro de mando que evidencie los riesgos asociados

		restricciones para el acceso a los S.O.			a la organización.
12.6.2	Restricciones en la instalación de sistema operativo (S.O.)				Instalación de corta fuegos y asignación de privilegios a cada usuario conforme a su perfil o cargo.
12.7 Consideraciones de las auditorías de los sistemas de información					
12.7.1	Controles de auditoría de los sistemas de información	No se audita ningún proceso relacionado con los activos de información.	No hay procedimientos de auditoría establecidos en la compañía.	Equipos, información.	Realizar mensualmente y trimestralmente una auditoría interna por los procesos de seguridad que se han implementado en la organización.
13. SEGURIDAD EN LAS TELECOMUNICACIONES					
13.2 Intercambio de información					
13.2.3	Mensajería electrónica	No hay artículos o cláusulas de confidencialidad de la información en los contratos y en el manejo de la información y su transmisión por vía electrónica.	Políticas y procedimientos inexistentes en la compañía, falta de personal capacitado para la realización de procesos de mantenimiento y soporte en procesos de transmisión de información electrónica..	Información, buen nombre de la empresa.	Establecer los protocolos para enviar la información por los canales de comunicación.
					Verificar los canales de comunicación mensualmente identificando los canales de transmisión por el internet.

					Definir documento donde se establecen los acuerdos de confidencialidad.
13.2.4	Acuerdos de confidencialidad y secreto				Definir documento donde se establecen las políticas de confidencialidad.
					Hacer seguimiento al cumplimiento de los acuerdos.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN					
14.1 Requisitos de seguridad de los sistemas de información					
14.1.1	Análisis y especificación de los requisitos de seguridad	No se identifica ningún análisis o estudio de requisitos para implementar la seguridad de la información.	Desconocimiento, falta de compromiso con la seguridad de la información por parte del propietario de la compañía.	Equipos, información relevante, el buen nombre de la compañía.	Mantener los sistemas actualizados, buscando identificar las amenazas, riesgos y vulnerabilidades asociados a los activos de información.
					Elaborar documento con especificaciones de los requisitos de seguridad para los sistemas de información.
14.3 Datos de prueba					
14.3.1	Protección de los datos utilizados en	No se realizan pruebas a los sistemas y a la	No existen procedimientos,	Información relevante de la	Definir un plan de pruebas a los activos

	pruebas	información que interactúa con estos.	protocolos o políticas para efectuar las actividades de pruebas.	empresa	informáticos, estableciendo las mejores alternativas para mitigar los riesgos.
					Definir un plan de pruebas a las pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN					
16.1. Gestión de incidentes de seguridad de la información y mejoras					
16.1.6	Aprendizaje de los incidentes de seguridad de la información	No se gestionan incidentes de seguridad de la información.	Desconocimiento sobre procesos, normas, estándares y buenas prácticas de la seguridad de la información.	Equipos de cómputo, dispositivos externos, información almacenada.	Establecer procesos de resolución de incidentes de seguridad de la información, bien sea de manera reactiva o proactiva.
					Implementar herramientas para evaluar los incidentes de seguridad.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
17.1. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio					
17.1.1	Planificación de la continuidad de la	No hay definidos ni documentados planes a	Desconocimiento de los SGSI, y su aplicación	Toda la compañía y sus activos.	Definir el proceso de gestión de continuidad

	seguridad de la información	seguir como contingencia para que el negocio pueda continuar en momentos de riesgo o amenaza.	como elemento primordial para la seguridad de los activos de información.		del negocio y las directrices de continuidad del negocio de conformidad con la política de seguridad de la información.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información				Definir e implantar los planes de continuidad del negocio de acuerdo al orden de prioridades, en los términos presentados en la instrucción de continuidad del negocio.
18. CUMPLIMIENTO					
18.1. Cumplimiento de los requisitos legales y contractuales					
18.1.1	Identificación de la legislación aplicable	Se accede a los equipos de manera sencilla, y se obtiene igualmente de una manera fácil la información del personal almacenada en estos, aunque el S.O y el software de Ofimática, cuentan con licencia OEM, hay otras	Uso indebido de los equipos, acceso a descargas de aplicaciones sin control, falta de una política de control de accesos, ser permisivos en el uso de los equipos, falta de conciencia en mantener los equipos con los aplicativos bajo las	Registros físicos y lógicos, equipos, información personal, la compañía.	Identificar la legislación que aplica para los procesos que intervienen en el manejo de la información.
18.1.2	Derechos de propiedad intelectual (DPI)				Identificar la legislación aplicable y los términos contractuales en las licencias utilizadas

		aplicaciones sin licenciamiento.	indicaciones del marco legal.		Hacer un inventario de software para garantizar la idoneidad de su uso. Dictar política de cumplimiento.
18.1.3	Protección de los registros de la organización				Clasificar la información en función de su importancia.
					Establecer copias de seguridad de la información relevante, proteger en armarios o cajones bajo llave la información física sensible de pérdida.
18.1.4	Protección de datos y privacidad de la información personal				Establecer el documento de seguridad de conformidad con la legislación de protección de datos personales.
18.2. Revisiones de la seguridad de la información					
18.2.2	Cumplimiento de las políticas y normas de seguridad	No se cuenta con una política de seguridad de la información.	Desconocimiento, descuido, poco interés en la implementación procedimientos y políticas ligada a la seguridad de los activos	Todos los activos de la empresa.	Dictar y acordar la política del sistema de gestión de la seguridad informática – SGSI.

			de información.		

11.2. Resultados comparativos en la aplicación de la auditoría

Ilustración 61 Política de seguridad de la información

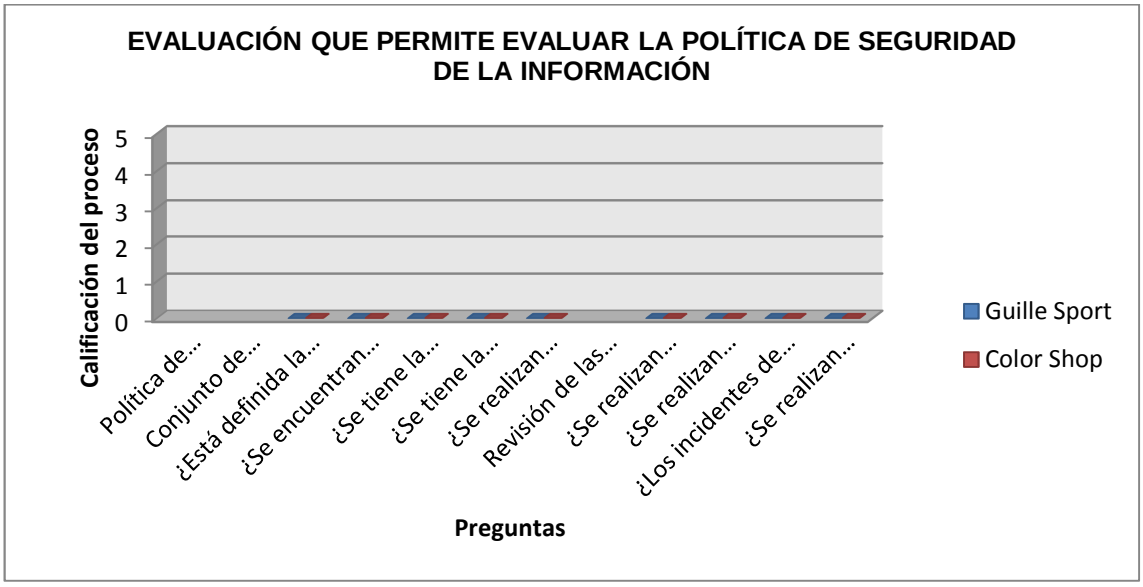


Ilustración 62 Aspectos organizativos de la seguridad de la información

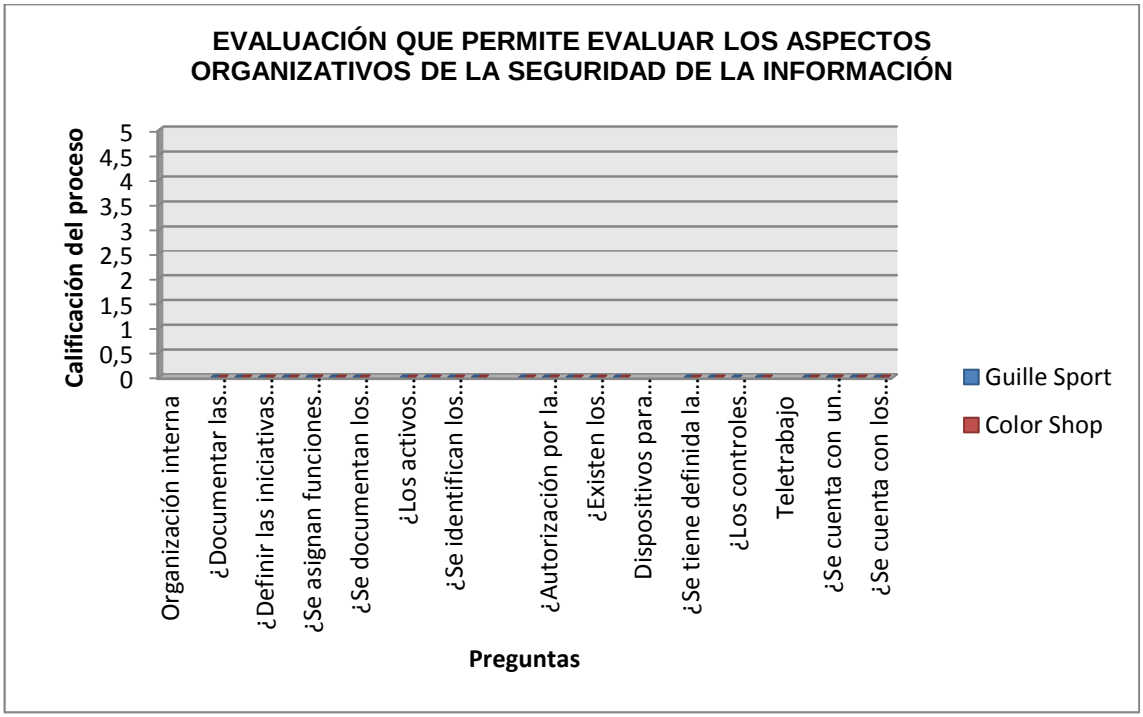


Ilustración 63 Seguridad ligada a los recursos humanos

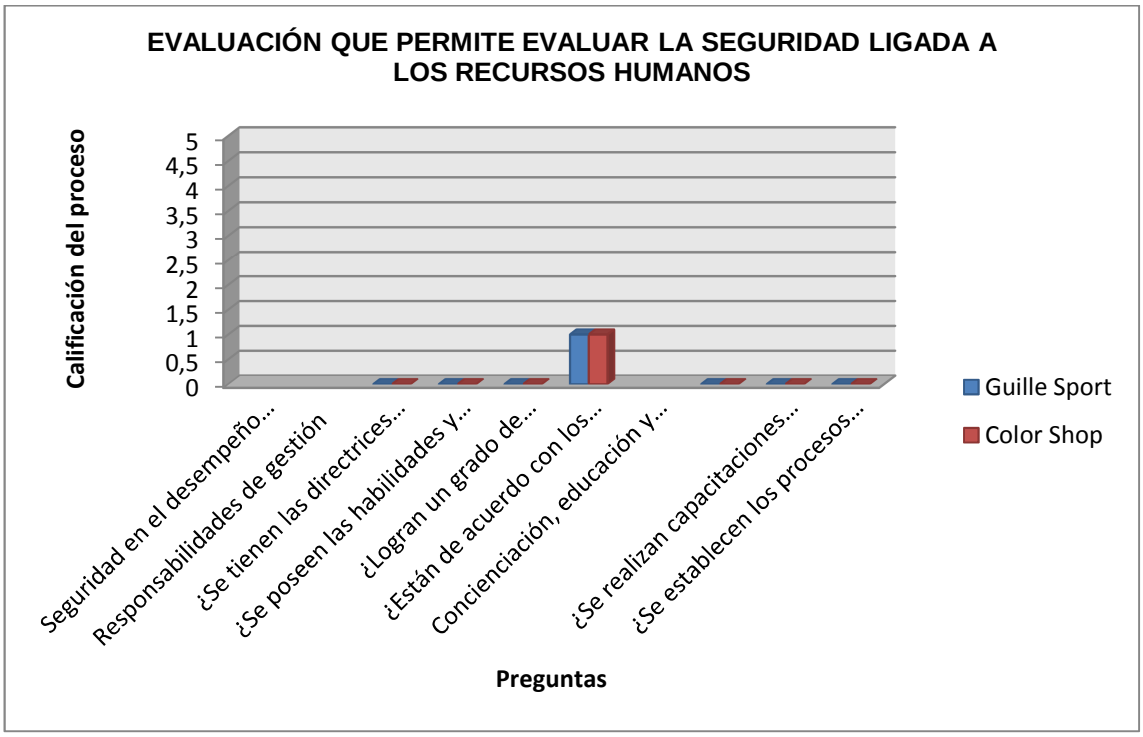


Ilustración 64 Gestión de activos

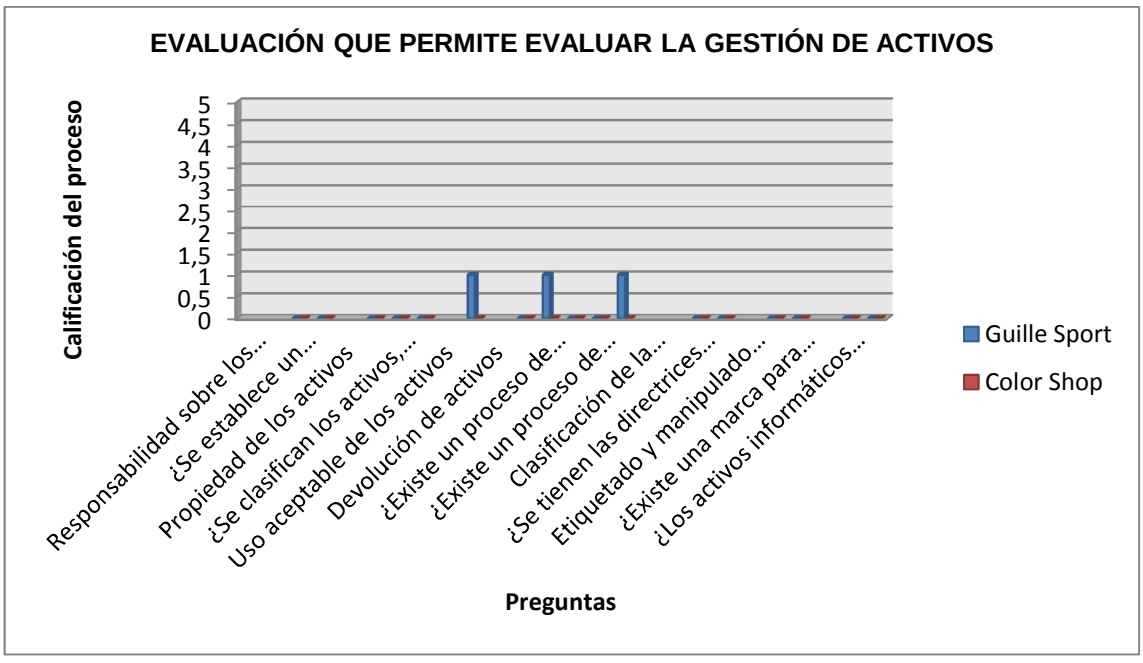


Ilustración 65 Control de acceso

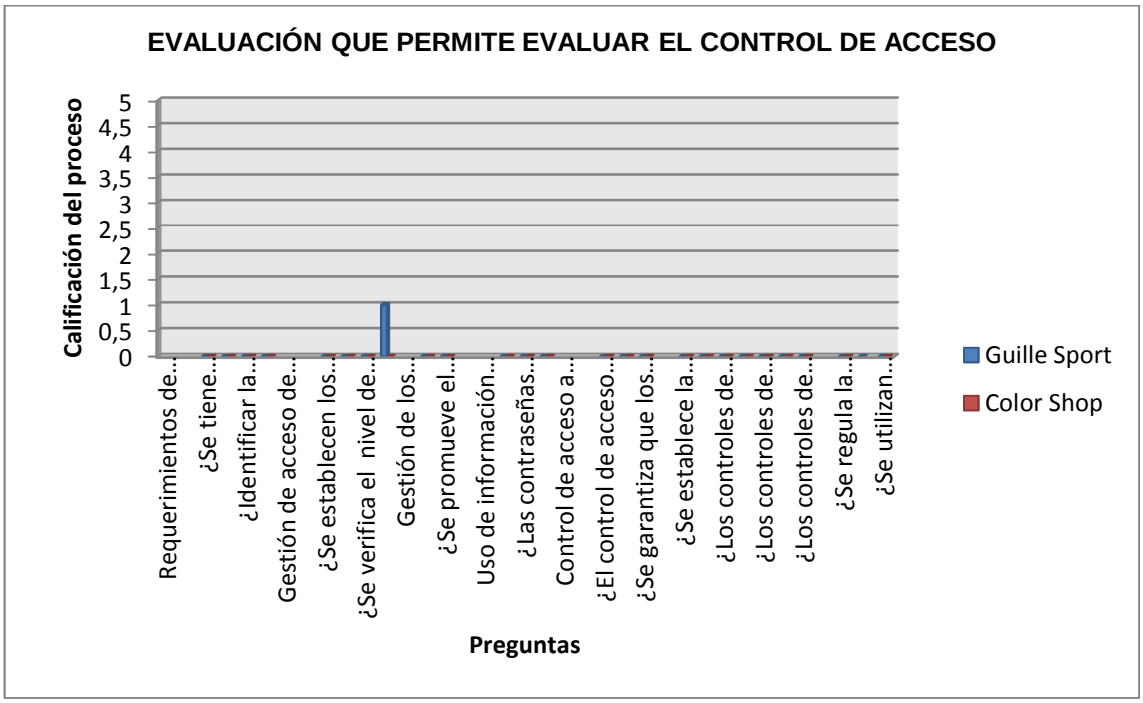


Ilustración 66 Cifrado

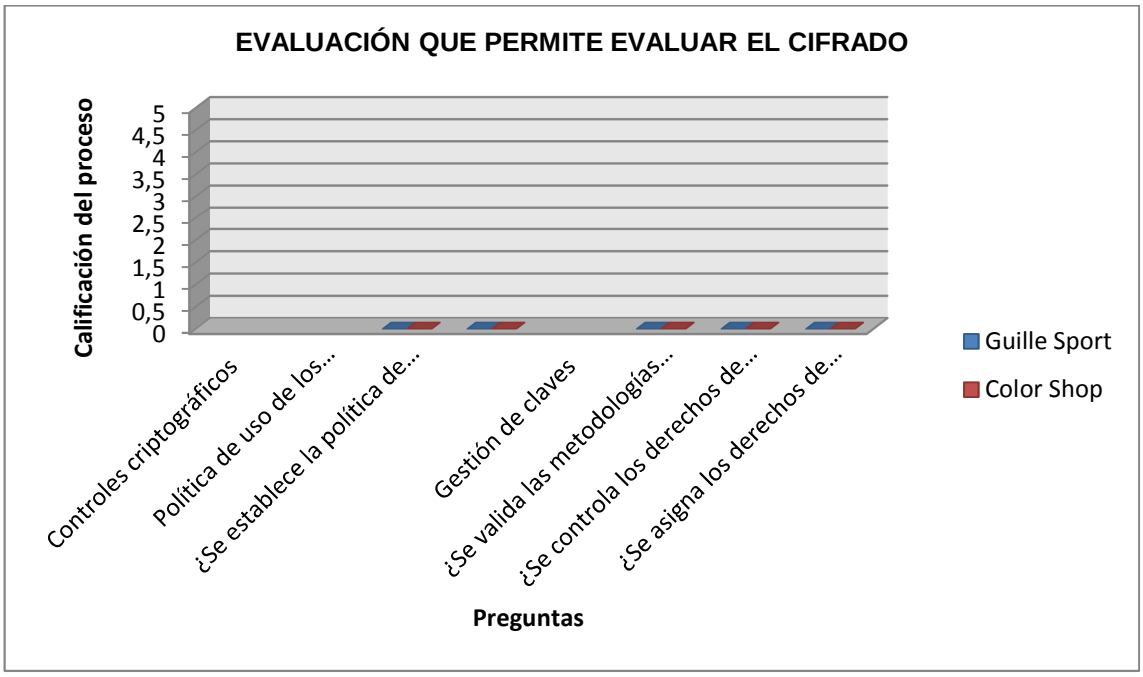


Ilustración 67 Seguridad física y del entorno

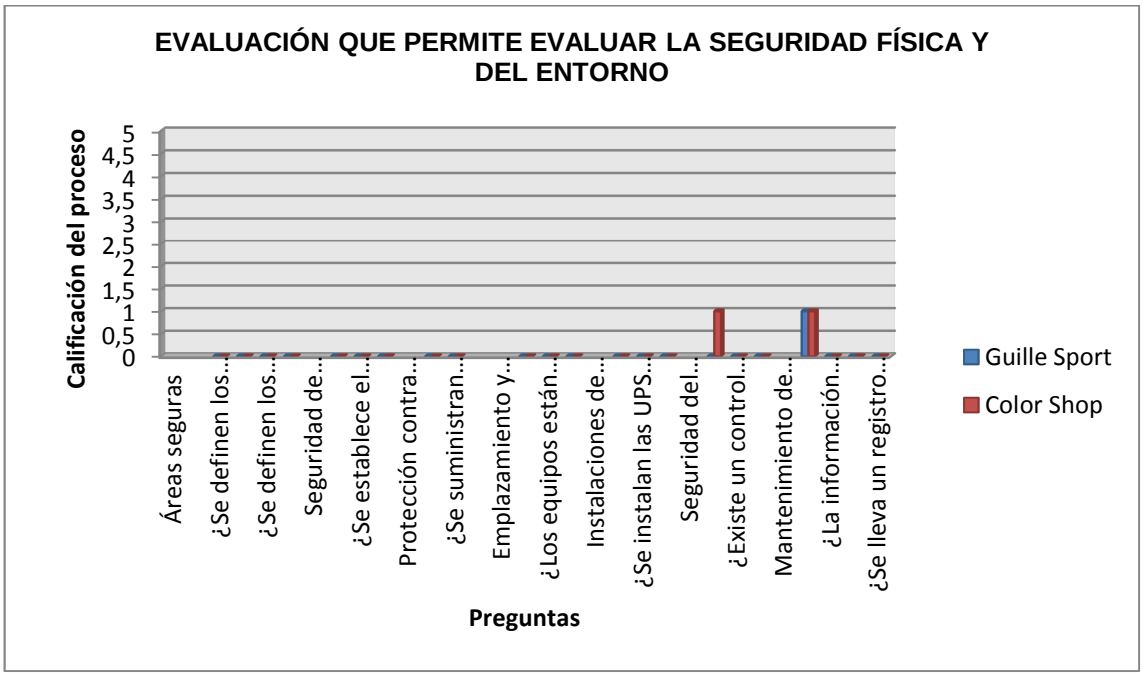


Ilustración 68 Seguridad en la operativa

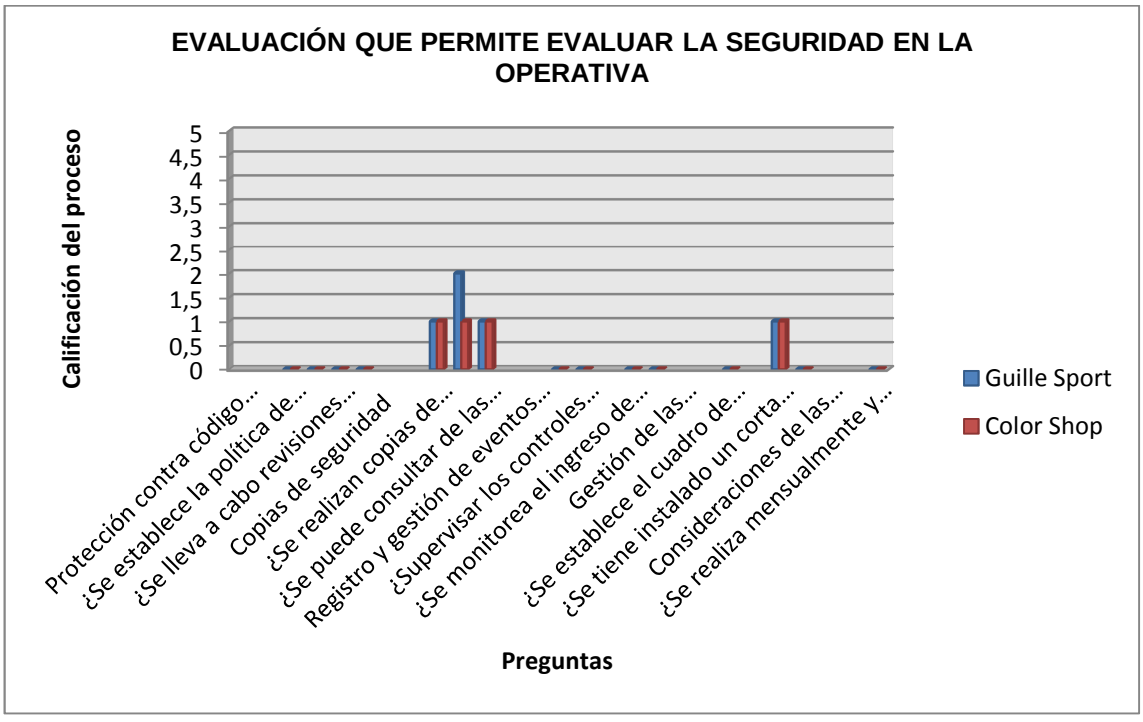


Ilustración 69 Seguridad en las telecomunicaciones

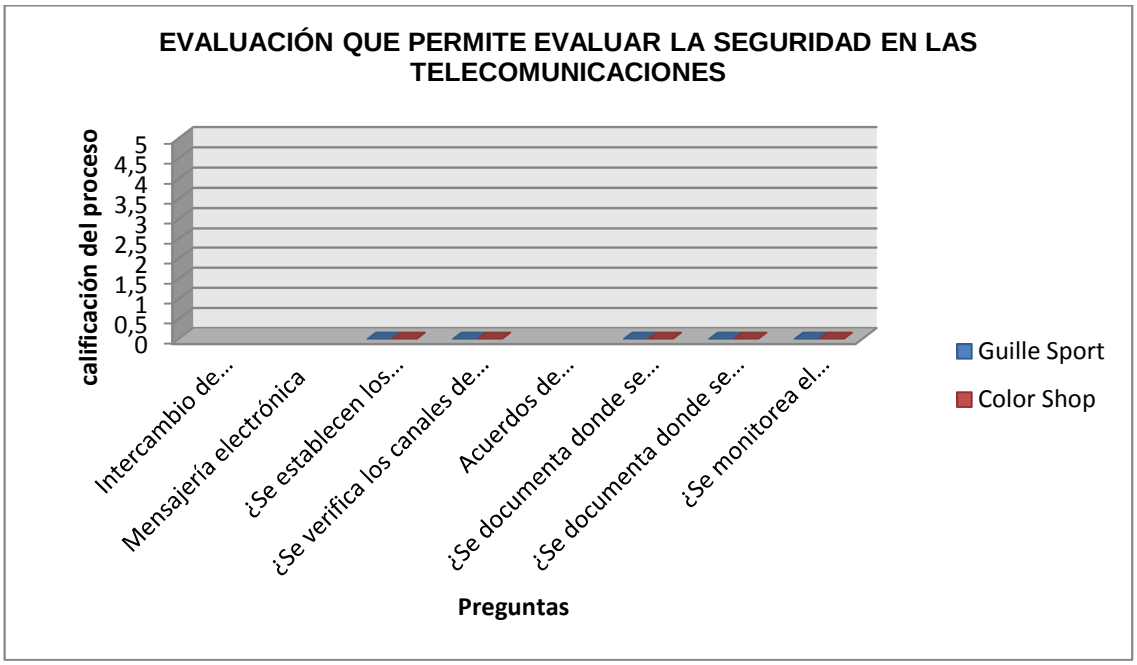


Ilustración 70 Gestión de incidentes en la seguridad de la información

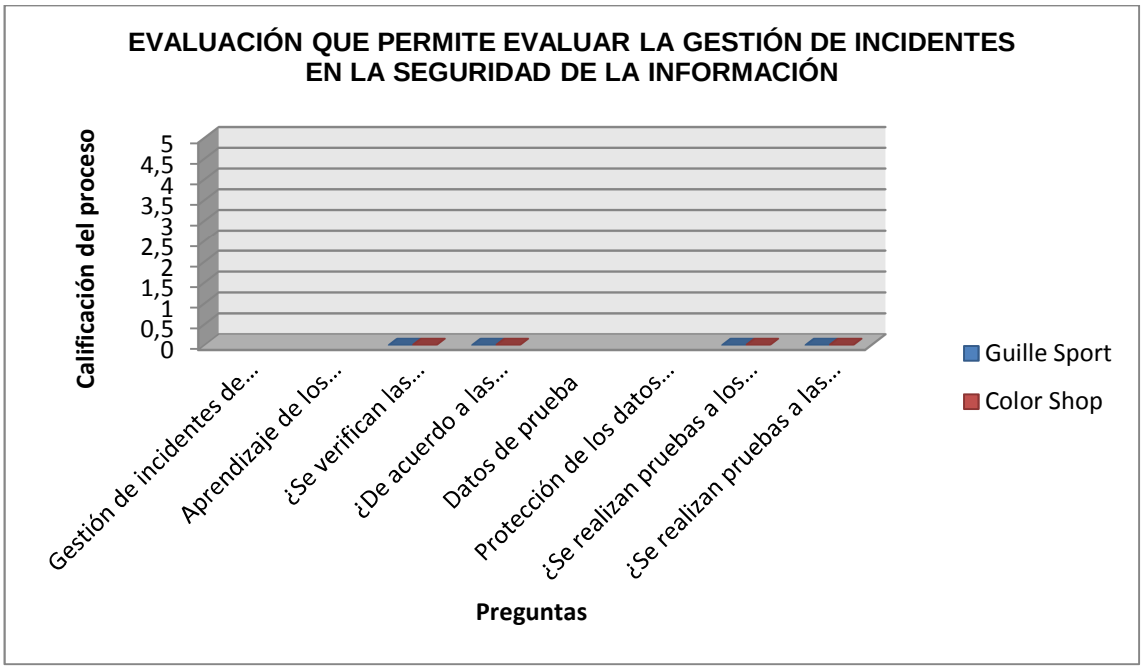


Ilustración 71 Adquisición, desarrollo y mantenimiento de los sistemas de información

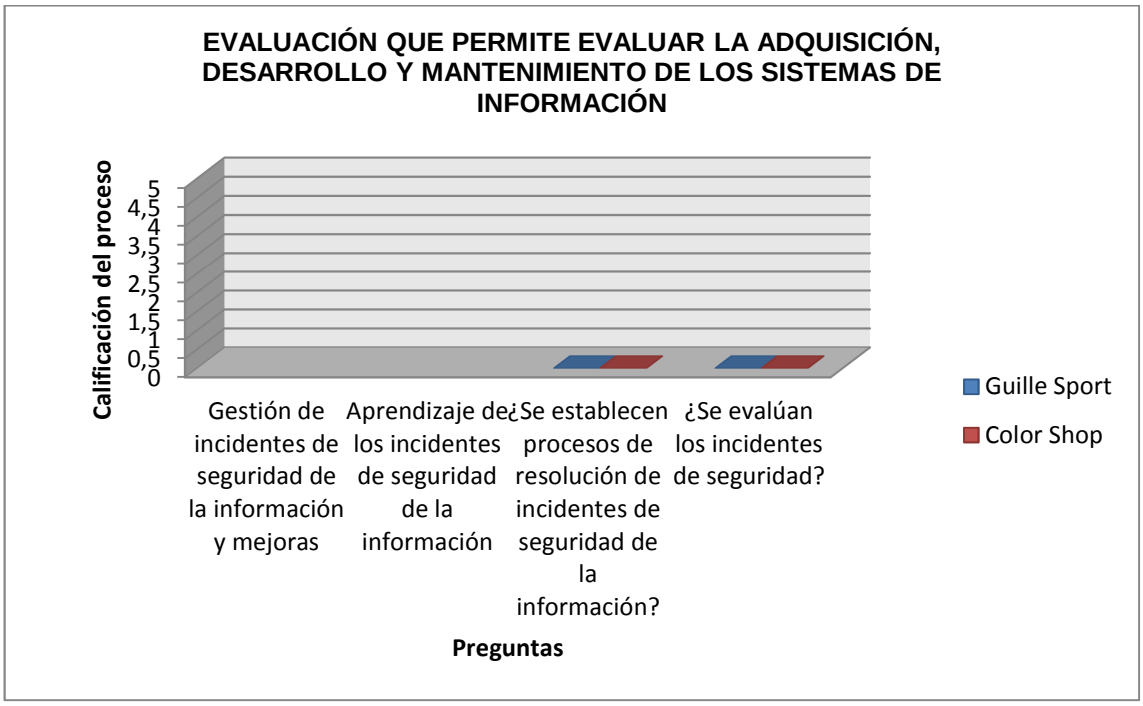


Ilustración 72 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

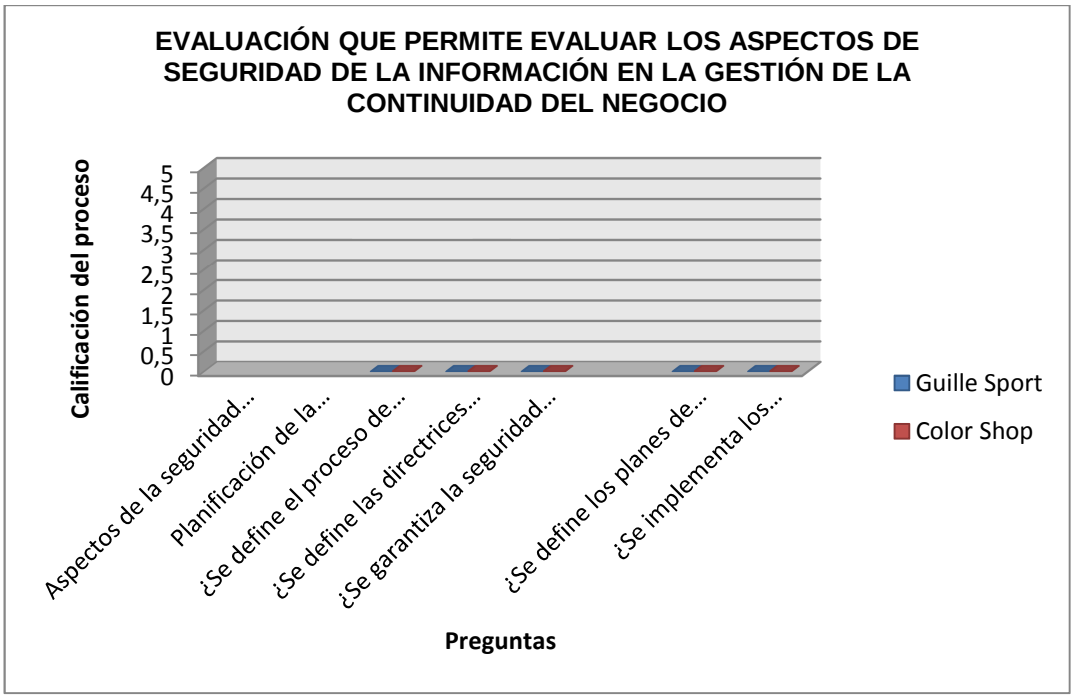


Ilustración 73 Cumplimiento

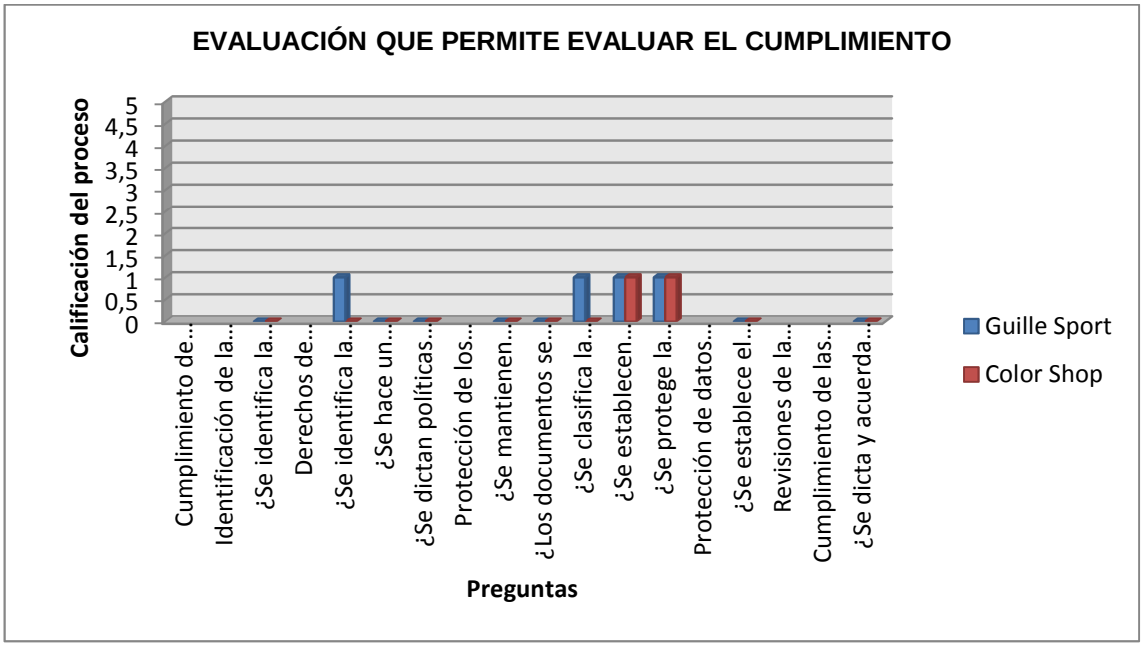


Tabla 61 Tabla comparativa entre las empresas

	Empresa 1 **Guille Sport**	**Empresa 2** **Color Shop**
Semejanzas	Control casi nulo para el acceso a los equipos, y por ende a la información que en estos se almacena. Gran cantidad de software inapropiado, improductivo y de dudosa procedencia. No tiene procedimientos escritos para procesos de manejos de información. Falta de control para el ingreso a las oficinas donde se almacena la información. Parte de la información, específicamente facturas y	Control casi nulo para el acceso a los equipos, y por ende a la información que en estos se almacena. Gran cantidad de software inapropiado, improductivo y de dudosa procedencia. No tiene procedimientos escritos para procesos de manejos de información. Falta de control para el ingreso a las oficinas donde se almacena la información. Parte de la información, específicamente facturas y contabilidad son manejadas de

	contabilidad son manejadas de forma física (papel). Trabaja casi con igual cantidad de personal y de equipos de cómputo.	forma física (papel). Trabaja casi con igual cantidad de personal y de equipos de cómputo.
Diferencias	Las instalaciones físicas mantienen una temperatura más apta para los equipos de cómputo. Cuenta con una persona para el mantenimiento de los equipos de cómputo (aunque empírica en el campo)	El Sistema Operativo y el software de Ofimática eslegal. Los dispositivos extraíbles para respaldo de información solo se conectan cuando se va a realizar este proceso, posteriormente se desconecta y es guardado por el gerente.

12. DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA – SGSI

12.1. Objetivo del SGSI

Establecer la política y los controles necesarios para proteger la información de las Pymes del sector textil en Medellín, Itagüí y Bogotá D.C., conforme a los hallazgos detectados a través de la auditoría.

12.2. Alcance del SGSI

Diseñar y proponer el sistema de gestión de la seguridad informática (SGSI) con sus respectivos controles, enmarcados en la política de seguridad para establecer las mejores prácticas en cuanto a cómo se debe gestionar los riesgos, vulnerabilidades y amenazas asociadas a las empresas textiles de las ciudades de Medellín, Itagüí y Bogotá D.C., conforme a los procedimientos propuestos.

12.3. Dominios evaluados y procesos seleccionados

Tabla 62 Dominios y procesos seleccionados[63]

Fuente: Tabla estructurada con los dominios y procesos seleccionados

REF.	CONTROL
5. POLÍTICA DE SEGURIDAD	
5.1. Política de Seguridad de la Información	
5.1.1	Conjunto de políticas para la seguridad de la información
5.1.2	Revisión de las políticas para la seguridad de la información
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1. Organización Interna	
6.1.1	Asignación de responsabilidades para la seguridad de la información
6.1.2	Segregación de tareas
6.1.5	Seguridad de la información en la gestión de proyectos
6.2. Dispositivos para movilidad y teletrabajo	
6.2.1.	Política de uso de dispositivos para movilidad
6.2.2.	Teletrabajo
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	
7.2. Seguridad en el desempeño de las funciones del empleo (Durante la	

[63] Fuente: Tabla estructurada con los dominios y procesos seleccionados

contratación)	
7.2.1	Responsabilidades de gestión
7.2.2	Concienciación, educación y capacitación en seguridad de la información
8. GESTIÓN DE ACTIVOS	
8.1. Responsabilidad sobre los activos	
8.1.1	Inventario de Activos
8.1.2	Propiedad de los activos
8.1.3.	Uso aceptable de los activos
8.1.4.	Devolución de activos
8.2. Clasificación de la información	
8.2.1.	Directrices de clasificación
8.2.2.	Etiquetado y manipulado de la información
8.2.3.	Manipulación de activos
9. CONTROL DE ACCESO	
9.1 Requerimientos de negocio para el control de acceso	
9.1.1	Política de control de acceso
9.2. Gestión de acceso de usuario	
9.2.1	Gestión de altas/bajas en el registro de usuarios
9.2.3	Gestión de los derechos de acceso con privilegios especiales
9.3. Responsabilidades de usuario	
9.3.1	Uso de información confidencial para la autenticación
9.4. Control de acceso a sistemas operativo y aplicaciones	
9.4.1	Restricción del acceso a la información
9.4.2	Procedimientos seguros de inicio de sesión
9.5.4	Uso de herramientas de administración de sistemas
10. CIFRADO	
10.1 Controles criptográficos	
10.1.1	Política de uso de los controles criptográficos
10.1.2	Gestión de claves
11. SEGURIDAD FÍSICA Y DEL ENTORNO	
11.1. Áreas seguras	
11.1.2	Controles físicos de entrada
11.1.3	Seguridad de oficinas, despachos y recursos
11.1.4	Protección contra las amenazas externas y ambientales
11.2. Seguridad de los equipos	
11.2.1	Emplazamiento y protección de equipos
11.2.2	Instalaciones de suministro
11.2.3	Seguridad del cableado
11.2.4	Mantenimiento de los equipos
12. SEGURIDAD EN LA OPERATIVA	
12.2. Protección contra código malicioso	
12.2.1	Controles contra el código malicioso
12.3. Copias de seguridad	
12.3.1	Copias de seguridad de la información

12.4. Registro de actividad y supervisión	
12.4.1	Registro y gestión de eventos de actividad
12.4.3	Registros de actividad del administrador y operador del sistema
12.6 Gestión de las vulnerabilidades técnicas	
12.6.1	Gestión de las vulnerabilidades técnicas
12.6.2	Restricciones en la instalación de sistema operativo (S.O.)
12.7 Consideraciones de las auditorías de los sistemas de información	
12.7.1	Controles de auditoría de los sistemas de información
13. SEGURIDAD EN LAS TELECOMUNICACIONES	
13.2 Intercambio de información	
13.2.3	Mensajería electrónica
13.2.4	Acuerdos de confidencialidad y secreto
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	
14.1 Requisitos de seguridad de los sistemas de información	
14.1.1	Análisis y especificación de los requisitos de seguridad
14.3 Datos de prueba	
14.3.1	Protección de los datos utilizados en pruebas
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	
16.1. Gestión de incidentes de seguridad de la información y mejoras	
16.1.6	Aprendizaje de los incidentes de seguridad de la información
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
17.1. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio	
17.1.1	Planificación de la continuidad de la seguridad de la información
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
18. CUMPLIMIENTO	
18.1. Cumplimiento de los requisitos legales y contractuales	
18.1.1	Identificación de la legislación aplicable
18.1.2	Derechos de propiedad intelectual (DPI)
18.1.3	Protección de los registros de la organización
18.1.4	Protección de datos y privacidad de la información personal
18.2. Revisiones de la seguridad de la información	
18.2.2	Cumplimiento de las políticas y normas de seguridad

12.4. Declaración de aplicabilidad

Aplicabilidad en dominios, objetivos de control y controles acorde a la norma ISO 27002:2013

Tabla 63 Declaración de aplicabilidad con los controles propuestos

DECLARACIÓN DE APLICABILIDAD		
REF.	**CONTROL**	**APLICACIÓN**
5. POLÍTICA DE SEGURIDAD		
5.1. Política de Seguridad de la Información		
5.1.1	Conjunto de políticas para la seguridad de la información	Documento de política de seguridad de la información
		Establecer las políticas de seguridad de la información para la compañía
5.1.2	Revisión de las políticas para la seguridad de la información	Realizar acciones preventivas y correctivas cada vez que se evidencie un hallazgo.
		Realizar revisiones periódicas de la política de seguridad
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN		
6.1. Organización Interna		
6.1.1	Asignación de responsabilidades para la seguridad de la información	Asignar las responsabilidades a cada proceso de seguridad
		Revisar la política de seguridad de la información.
		Documentar y definir los procesos de asignación y seguridad
		Asignar las responsabilidades a cada proceso de seguridad
6.1.2	Segregación de tareas	Los activos informáticos se encuentran definidos claramente
		Garantizar las actividades de seguridad, siguiendo la política de seguridad
6.1.5	Seguridad de la información en la gestión de proyectos	Compromiso de la Dirección con la seguridad de la información
		Autorización por la dirección para la inversión de recursos, tiempos y formaciones
		Procedimientos documentados para contactar a las autoridades competentes.
		Procedimientos documentados para contactar a las entidades públicas
6.2. Dispositivos para movilidad y teletrabajo		
6.2.1.	Política de uso de	Definir la política de seguridad para dispositivos

	dispositivos para movilidad	móviles
		Los controles aseguran la protección de los canales de comunicación
		Los controles aseguran la protección contra código malicioso
		Los controles aseguran la disponibilidad, integridad y confidencialidad de la información
6.2.2.	Teletrabajo	Estructurar clara para la presentación de informes
		Contar con un procesos específico para la gestión de cambio
		La política de acceso, cuenta con los módulos permitidos para la identificación de usuario
		Contar con los privilegios de acceso
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
7.2. Seguridad en el desempeño de las funciones del empleo (Durante la contratación)		
7.2.1	Responsabilidades de gestión	Especificación de políticas de seguridad de información, involucrar al personal y hacer seguimiento
		Establecer las directrices sobre las funciones de seguridad informática.
7.2.2	Concienciación, educación y capacitación en seguridad de la información	Formación al personal en temas de seguridad de la información.
		Realizar capacitaciones sobre las amenazas, riesgos y vulnerabilidades
		Establecer los procesos de formación y concientización, diseñado para presentar las políticas de seguridad de la organización
8. GESTIÓN DE ACTIVOS		
8.1. Responsabilidad sobre los activos		
8.1.1	Inventario de Activos	Mantener un inventario de activos definido. - Relación de riesgos con tipos de activos. - Mantener registro de personas y sus capacitaciones
8.1.2	Propiedad de los activos	Identificar el propietario de los activos y el responsable
		Los activos se clasifican por niveles
8.1.3.	Uso aceptable de los activos	Informar a los empleados sobre el uso de los activos
8.1.4.	Devolución de activos	Proceso de terminación para incluir la devolución del software.
		Proceso de terminación para incluir la devolución de los documentos
		Proceso de terminación para incluir la devolución de los equipos móviles.

		Proceso de terminación para incluir la devolución de los equipos de cómputo.
		Procedimiento que garantice la transferencia de información al finalizar su contratación.
8.2. Clasificación de la información		
8.2.1.	Directrices de clasificación	Existen las directrices sobre cómo se clasifican los activos informáticos
		Existe la clasificación de seguridad por niveles
8.2.2.	Etiquetado y manipulado de la información	Capacitar sobre cómo se debe enviar, y manipular las bases de información confidencial
		Existe una marca para identificar las fuentes de información
8.2.3.	Manipulación de activos	Los activos informáticos poseen una documentación adecuada
		Manuales de configuración de los activos informáticos
9. CONTROL DE ACCESO		
9.1 Requerimientos de negocio para el control de acceso		
9.1.1	Política de control de acceso	Desarrollar la política de control de accesos conforme con la política de seguridad y atendiendo la legislación aplicable.
		Identificar la información relacionada con las aplicaciones y los riesgos asociados a la información
9.2. Gestión de acceso de usuario		
9.2.1	Gestión de altas/bajas en el registro de usuarios	Establecer para cada activo, un repositorio donde quede registro de los usuarios para tener inventario de todos los accesos otorgados a cada activo.
		Verificar que el nivel de acceso otorgado a cada usuario periódicamente.
		Verificar que el usuario tenga autorización del dueño del sistema para el uso de la información.
9.2.3	Gestión de los derechos de acceso con privilegios especiales	Establecer para cada tipo de activo los privilegios otorgados de acuerdo a la evaluación de riesgos asociada.
		Promueve el desarrollo de rutinas del sistema para evitar la necesidad de otorgar privilegios innecesarios.
9.3. Responsabilidades de usuario		
9.3.1	Uso de información confidencial para la autenticación	Definir políticas de seguridad para usuarios de los equipos.
		Las contraseñas predeterminadas por el proveedor se cambian inmediatamente después de la instalación de los sistemas o del software
		Las contraseñas temporales se suministran de

		forma segura a los usuarios.
9.4. Control de acceso a sistemas operativo y aplicaciones		
9.4.1	Restricción del acceso a la información	El control de acceso se realiza de acuerdo a la política del control de accesos.
		Controlar los derechos de acceso de otras aplicaciones
		Garantiza que los datos de salida de los sistemas de aplicación que manejan información sensible solo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados.
9.4.2	Procedimientos seguros de inicio de sesión	Establecer la política de autenticación a los equipos, con contraseñas personales y perfiles definidos.
		Validar la información de registro con la base de datos para el acceso.
		El control se aplica a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de red, programadores de sistemas y administradores de bases de datos)
9.5.4	Uso de herramientas de administración de sistemas	Regular la instalación de software en los equipos de cómputo personales, conforme a la política de seguridad de equipos personales.
		Llevar un registro de todo uso de las utilidades del sistema
		Usar procedimientos de identificación, autenticación y autorización para las utilidades del sistema
10. CIFRADO		
10.1 Controles criptográficos		
10.1.1	Política de uso de los controles criptográficos	Establecer la política de cifrado para las claves públicas y privadas en el manejo de información confidencial.
		Verificar la política de cifrado conforme a la norma actual.
10.1.2	Gestión de claves	Validar las metodologías para cifrar las claves y uso en los mensajes emitidos.
		Controlar y asignar los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial.
11. SEGURIDAD FÍSICA Y DEL ENTORNO		
11.1. Áreas seguras		
11.1.2	Controles físicos de entrada	Definición de controles físicos, técnicos y organizacionales para cada activo.
		Dictar la política de control de accesos

		conforme al SGSI.
11.1.3	Seguridad de oficinas, despachos y recursos	Dictar la política de uso de las oficinas acorde a la política de gestión de acceso y del SGSI.
		Establecer el reglamento y las normas sobre las actividades y procesos informáticos.
11.1.4	Protección contra las amenazas externas y ambientales	Definición de un plan de respuesta para cada tipo de efecto que pudiera causar amenaza externa.
		Suministrar equipos apropiados contra las amenazas ambientales y son ubicados adecuadamente.
11.2. Seguridad de los equipos		
11.2.1	Emplazamiento y protección de equipos	Regular y monitorear el uso de equipos personales a través de la política de uso de equipos personales.
		Los equipos están distribuidos de tal forma que no pueda acceder cualquier usuario.
		Los elementos que requieren protección especial están aislados.
11.2.2	Instalaciones de suministro	Establecer el plan de continuidad para este tipo de riesgos
		Instalar las UPS y los suministros de energía necesarios, para dar soporte al cierre del ordenador o al funcionamiento continuo de equipos que soportan operaciones críticas para el negocio.
		Las UPS y plantas de energía son revisadas con frecuencia para asegurarse de que tiene la capacidad adecuada.
11.2.3	Seguridad del cableado	El cableado se encuentre canalizado por conductos específicos del suelo técnico instalado en las oficinas.
		Existe un control de acceso en los cuartos de cableado que soportan los sistemas críticos.
		Tienen rótulos de equipos y de cables claramente identificables para minimizar los errores en el manejo.
11.2.4	Mantenimiento de los equipos	Realizar mantenimiento acorde a los procesos de gestión de activos.
		La información confidencial es retirada periódicamente de los equipos de cómputo o el personal de mantenimiento es suficientemente confiable.
		Llevar un registro de todas las fallas reales y sospechosas.
12. SEGURIDAD EN LA OPERATIVA		
12.2. Protección contra código malicioso		

12.2.1	Controles contra el código malicioso	Establecer la política de seguridad de equipos personales en la que se previene el uso de programas no autorizados por la empresa. Regular el uso de software antivirus y su actualización.
		Llevar a cabo revisiones mensuales sobre el contenido del software y los datos que soportan los procesos críticos del negocio.
		Investigar la aparición de archivos o códigos no autorizados y aprobados por el desarrollador del software y/o aplicación.
12.3. Copias de seguridad		
12.3.1	Copias de seguridad de la información	Realizar copias de seguridad de manera periódica sobre la información registrada en las oficinas – Backup.
		Las copias de seguridad se almacenan en un sitio seguro.
		Después de realizar la copia de seguridad se puede consultar los archivos y la información está completa.
12.4. Registro de actividad y supervisión		
12.4.1	Registro y gestión de eventos de actividad	Supervisar los controles definidos al uso de equipos personales.
		Monitorear los cambios de configuración del sistema.
12.4.3	Registros de actividad del administrador y operador del sistema	Monitorear el ingreso de usuarios a las diferentes aplicaciones.
		Registrar las alertas o fallas del sistema, como mensajes de consola.
12.6 Gestión de las vulnerabilidades técnicas		
12.6.1	Gestión de las vulnerabilidades técnicas	Establecer un cuadro de control o cuadro de mando que evidencie los riesgos asociados a la organización.
12.6.2	Restricciones en la instalación de sistema operativo (S.O.)	Instalación de corta fuego y asignación de privilegios a cada usuario conforme a su perfil o cargo.
12.7 Consideraciones de las auditorías de los sistemas de información		
12.7.1	Controles de auditoría de los sistemas de información	Realizar mensualmente y trimestralmente una auditoría interna por los procesos de seguridad que se han implementado en la organización.
13. SEGURIDAD EN LAS TELECOMUNICACIONES		
13.2 Intercambio de información		
13.2.3	Mensajería electrónica	Establecer los protocolos para enviar la información por los canales de comunicación.
		Verificar los canales de comunicación mensualmente identificando los canales de

		transmisión por el internet.
13.2.4	Acuerdos de confidencialidad y secreto	Documento donde se establecen los acuerdos de confidencialidad.
		Documento donde se establecen las políticas de confidencialidad.
		Monitorear el cumplimiento de los acuerdos.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN		
14.1 Requisitos de seguridad de los sistemas de información		
14.1.1	Análisis y especificación de los requisitos de seguridad	Verificar las amenazas, riesgos y vulnerabilidades asociados a la empresa.
		Conforme a las amenazas, riesgos y vulnerabilidades se debe establecer una propuesta para disminuir el riesgo.
14.3 Datos de prueba		
14.3.1	Protección de los datos utilizados en pruebas	Realizar pruebas a los activos informáticos, estableciendo las mejores alternativas para mitigar los riesgos.
		Realizar pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN		
16.1. Gestión de incidentes de seguridad de la información y mejoras		
16.1.6	Aprendizaje de los incidentes de seguridad de la información	Establecer procesos de resolución de incidentes de seguridad de la información, bien sea de manera reactiva o proactiva.
		Evaluar los incidentes de seguridad.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
17.1. Aspectos de la seguridad de la información en la gestión de la continuidad del negocio		
17.1.1	Planificación de la continuidad de la seguridad de la información	Definir el proceso de gestión de continuidad del negocio y las directrices de continuidad del negocio de conformidad con la política de seguridad de la información.
		Garantizar la seguridad del personal, la protección de los servicios y procesos de información.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Definir e implantar los planes de continuidad del negocio de acuerdo al orden de prioridades, en los términos presentados en la instrucción de continuidad del negocio.
18. CUMPLIMIENTO		
18.1. Cumplimiento de los requisitos legales y contractuales		
18.1.1	Identificación de la legislación aplicable	Identificar la legislación que aplica para los procesos que intervienen en el manejo de la

		información.
18.1.2	Derechos de propiedad intelectual (DPI)	Identificar la legislación aplicable y los términos contractuales en las licencias utilizadas
		Hacer un inventario de software para garantizar la idoneidad de su uso. Dictar política de cumplimiento.
18.1.3	Protección de los registros de la organización	Mantener disponibles los documentos del sistema de gestión de la seguridad informática – SGSI.
		Los documentos solo son editables para los responsables de estos y/o usuarios autorizados.
		Clasificar la información en función de su importancia.
		Establecer copias de seguridad de la información relevante, proteger en armarios o cajones bajo llave la información física sensible de pérdida.
18.1.4	Protección de datos y privacidad de la información personal	Establece el documento de seguridad de conformidad con la legislación de protección de datos personales.
18.2. Revisiones de la seguridad de la información		
18.2.2	Cumplimiento de las políticas y normas de seguridad	Dictar y acordar la política del sistema de gestión de la seguridad informática – SGSI.

12.5. Política de seguridad de la información

DISPOSICION NRO 001

Por la cual se adoptan las políticas de seguridad de la información de las PYMES del sector textil en las ciudades de Itagüí, Medellín y Bogotá DC.

El gerente de la PYME en uso de sus facultades legales y estatutarias, y

CONSIDERANDO:

Que la Política de Seguridad de la información en la PYME. Establece la forma como la información generada en la empresa, o proveniente de sus clientes o terceras personas debe ser manejada en sus diversas formas.

Que mediante la disposición 01 de marzo 20 de 2015, la PYME. Adopta la norma ISO/IEC 27001, como mejor práctica para establecer el Sistema de Gestión de Seguridad de la Información.

Que mediante la Directiva Nro. 01 de marzo de 2015, la PYME. Fija los lineamientos para la gestión integral de los riesgos, entre los que se incluyen los riesgos de seguridad de la información de la compañía.

DISPONE:

1. Introducción

La Política de Seguridad de la Información de la PYME. Es una declaración de la conducta, ética y responsabilidades adoptada por la compañía y aceptada por sus colaboradores para proveer y procurar un ambiente seguro en el manejo de la información propia, de clientes y de terceras personas.

1.1. Objetivo General

El objetivo principal de la Política de Seguridad de la Información es que la PYME. Vele para que la información que maneja, bien sea propia, dejada en custodia o compartida con terceros:

1.1.1 Se encuentre protegida contra modificaciones no autorizadas, realizadas con o sin intención.

1.1.2 Sea accedida y utilizada únicamente por aquellas personas que tienen una necesidad justificada para la realización de sus funciones dentro de la organización y/o negocio.

1.1.3 Esté disponible cuando se requiera y sea utilizada para los fines que fue obtenida.

1.2. Objetivos Específicos

Los objetivos específicos que busca la Política de Seguridad de la información son:

- Determinar la información de los clientes y de la PYME. como el activo de información más importante a ser protegido.
- Definir la conducta a seguir en lo referente al acceso, uso, manejo y administración de la información.
- Fundamentar el desarrollo, implantación, mantenimiento y cumplimiento de la Política de Seguridad de la información.
- Comunicar a todo el personal y a los que vayan a hacer uso de la información de la PYME. de sus responsabilidades y cuidado de la misma.
- Establecer y comunicar internamente en la compañía y a las personas externas interesadas, la responsabilidad en el acceso, uso, manejo y administración de los activos de información, que soportan el conocimiento, procesos, y sistemas del negocio.

2. Alcance

La Política de Seguridad de la Información aplica a los colaboradores, clientes, proveedores, y demás entes externos de la PYME, que accedan a cualquier activo de información de la compañía, o que lo tienen bajo su responsabilidad no importando su ubicación.

3. Cumplimiento de la Política de Seguridad de la Información

Es de carácter obligatorio, el cumplimiento de las Políticas de Seguridad de la Información establecidas en esta disposición, junto con los estándares de seguridad y el sistema de gestión que las contempla. Todos los colaboradores de la compañía, clientes y usuarios deben entender su rol y asumir su responsabilidad respecto al acceso, uso, manejo y administración de la información al igual que de los activos que se relacionan con esta. Cualquier

incumplimiento a esta Política que ponga en riesgo la integridad, confidencialidad y disponibilidad de la información o que afecte el acceso, uso, manejo o administración de la misma se verá sometido a las acciones legales y/o disciplinarias que se consideren pertinentes.

4. Políticas de Seguridad de la información

Las Políticas de Seguridad de la Información que la PYME, adopta por medio de esta disposición y que serán desarrolladas a través de los estándares de seguridad y los sistemas de gestión que las despliegan son:

Política 1. Gestión de la Seguridad de la Información

- La PYME. Implementa y mantiene una Política de Seguridad de la Información.

Política 2. Administración y Protección de activos de información

- Cada activo de información se administra y protege acorde a su nivel de clasificación.

Política 3. Administración del Riesgo de Seguridad de la Información

- La PYME. Administra los riesgos asociados a los activos de información.

Política 4. Seguridad de la información en los procesos asociados

- La PYME. Establece y aplica las mejores prácticas de seguridad de la información en procesos asociados a las personas.

Política 5. Seguridad Física

- La PYME. Aplica las mejores prácticas en seguridad física.

Política 6. Administración de las plataformas de TIC

- La PYME. Administra sus plataformas de tecnologías de información y comunicaciones, adoptando las mejores prácticas internacionales en seguridad de la información.

Política 7. Control de acceso

- Todo acceso autorizado, requiere de una identificación y autenticación personal e intransferible.

Política 8. Gestión de incidentes de seguridad

- La PYME. Provee los mecanismos y recursos necesarios para atender y responder ante los incidentes de seguridad de la información.

Política 9. Cumplimiento y gestión de regulaciones

- La PYME. Gestiona la conformidad con los requisitos legales y normativos.

Política 10. Sobre la responsabilidad de Terceros

- Terceros que utilicen local o remotamente activos de información de la PYME, deben cumplir con la política de seguridad de la información.

Nombre completo

Gerente PYME.

Proyectó:	Visto bueno	Fecha
Aprobó:	Visto bueno	Fecha

12.6. Procedimientos propuestos para mitigar los riesgos

12.6.1. Procedimiento de control de documentos

Procedimiento Control de Documentos	Código:	P-SGSI-01-001
	Versión:	1
	Vigencia:	Marzo de 2015
	Página:	1 de 1

1. Objetivo
2. Alcance
3. Definiciones y abreviaturas
4. Procedimiento
5. Registro

1. OBJETIVO

Garantizar que la compañía cuente con los documentos necesarios, que contengan la información explicita para controlar procesos relacionados con los activos de información.

2. ALCANCE

El alcance de este procedimiento es la documentación que la dirección considere necesaria para abordar los temas de seguridad de la información acorde a las necesidades.

3. DEFINICIONES Y ABREVIATURAS

SGSI: Sistema de Gestión de Seguridad de la Información.

5. PROCEDIMIENTO

La dirección elaborará los documentos que se requieran para mantener un control adecuado sobre los procesos de la compañía en los cuales intervengan activos de información, en su defecto delegará a alguno de los empleados a tal

función, una vez se tenga cada documento, los pasos a seguir son los siguientes:

- El encargado del control de los documentos elabora una ficha o archivo digital con el listado de todos los documentos, su identificación y localización.
- Se hará una verificación periódica (la determina la dirección) de la actualización de cada documento.
- Se informará al director de la necesidad de actualizar uno o más documentos.
- Se actualizan los documentos informados, buscando que la información de estos sea confiable.
- Se hace la verificación de la actualización realizada al documento y se actualiza el archivo de listado de documentos.

6. REGISTRO

Los registros que se obtienen de poner en práctica este procedimiento, se generan cuando las personas encargadas elaboran un nuevo documento, o en su defecto realizan cambios o actualizaciones en uno o más de ellos, de lo cual queda el registro del documento activo con todas sus actualizaciones y demás información, y el registro del listado de documentos igualmente actualizado con la información pertinente.

12.6.2. Procedimiento de control de registros

Procedimiento Control de Registros	Código:	P-SGSI-01-002
	Versión:	1
	Vigencia:	Marzo de 2015
	Página:	1 de 1

1. Objetivo
2. Alcance
3. Definiciones y abreviaturas
4. Procedimiento
5. Registro

1. OBJETIVO

Verificar que las acciones realizadas en los activos de información tengan un registro documentado, y que los resultados se mantengan actualizados y agreguen valor para la toma de decisiones.

2. ALCANCE

El alcance de este procedimiento es registrar las actividades realizadas por las personas en los activos de información, buscando que cada acción lleve un seguimiento que permita determinar el uso de los activos y realizar los respectivos ajustes a las desviaciones en los procesos y políticas de SGSI.

3. DEFINICIONES Y ABREVIATURAS

SGSI: Sistema de Gestión de Seguridad de la Información.

5. PROCEDIMIENTO

La dirección indicará que procesos que involucren los activos de información, tendrán supervisión y control a la actividad realizada en estos, una vez se determine, se tendrá la documentación necesaria para llevar dichos registros, los resultados y las acciones realizadas en caso de hacer uso de estas, para esto se seguirán los siguientes pasos:

- El encargado del control de registros elabora una ficha o plantilla digital con el listado de todos los activos, su identificación y localización.
- Se hará una verificación periódica (la determina la dirección) de los registros generados en cada activo.
- Se informará al director de la actividad encontrada y de los registros que incumplen con la política de seguridad de la información adoptada por la compañía.
- Se registran las acciones realizadas y avaladas por la dirección.
- Se hace verificación al cumplimiento de las acciones propuestas y realizadas.

6. REGISTRO

Los registros que se obtienen de poner en práctica este procedimiento, se generan cuando las personas encargadas actualizan o realizan cambios en los documentos asociados, de estos queda el registro del documento activo con todas sus actualizaciones y demás información, y el registro del listado de documentos igualmente actualizado con la información pertinente a todos los cambios realizados.

12.6.3. Procedimiento de auditoría interna

SISTEMA DE GESTIÓN INTEGRADO			
TÍTULO DEL DOCUMENTO:		**PROCEDIMIENTO DE AUDITORIA INTERNA**	
CÓDIGO DEL DOCUMENTO:			
VERSIÓN:	**01**	**FECHA DE CREACIÓN:**	**24/03/2015**
INFORMACIÓN SOBRE RESPONSABLES			
	Fecha	**Nombre Responsable**	**Cargo**
Elaboración			
Revisión			
Aprobación			

OBJETIVO

Este procedimiento tiene el objetivo de entregar una completa guía de auditoría al proceso del cumplimiento de condiciones, con las cuales se adopta la implementación del SGSI (Sistema de Gestión de Seguridad de la Información) de la compañía.

ALCANCE

Este procedimiento es creado para la auditoria del proceso cumplimiento de condiciones, en los aspectos de verificación al cumplimiento en la documentación existente en el SGSI, la debida implementación y control de los procesos sometidos en el mismo.

REFERENCIAS

RECURSOS

ENCARGADO de servicios de ti O GERENTE GENERAL

Analista de calidad auditor, GERENTE GENERAL, O ENCARGADO POR LA DIRECCIÓN

Analista informática auditor, GERENTE GENERAL O ENCARGADO POR LA DIRECCIÓN

Analista de CONTROL INTERNO, GERENTE GENERAL O ENCARGADO POR LA DIRECCIÓN

CONTENIDO

Definir cronograma anual de auditoria

Responsable: Encargado de servicios de TI o Gerente general

El Responsable o designado por parte de la compañía, debe programar una reunión con todos los involucrados en el proceso de auditoría, a saber:

- Analista de control interno o responsable designado
- Analista de Informática auditor o responsable designado
- Analista de Calidad auditor o responsable designado
- Encargado de Servicios TI o responsable designado

Esta reunión tiene como objetivo definir y conciliar con todos los involucrados el cronograma dentro del cual se realizará la auditoria al proceso del cumplimiento de condiciones, y debe dividirse en seis etapas para tratar los temas de la documentación exigida en el SGSI, bajo las premisa de la ISO/IEC 27001:2013. Se define como política, que la auditoria se realiza anualmente.

Tabla 64 Cronograma

	Auditoria Políticas, objetivos y alcance	**Auditoria a la metodología, evaluación y tratamiento del riesgo**	**Auditoria a planificación, operación y control de procesos de S.I.**	**Auditoria a la eficacia de controles**	**Evaluación de Hallazgos e Informe**	**Iniciar Ciclo de Mejora Continua**
Etapa 1	Semana 1					
Etapa 2		Semana 1				
Etapa 3			Semana 1			
Etapa 4				Semana 2		
Etapa 5					Semana 2	
Etapa 6						**Semana 2**

DEFINIR EL TAMAÑO Y CARACTERISTICAS DE LA MUESTRA

Responsable: Partes Interesadas en el Proceso de Auditoria

La muestra a considerar será la información recopilada durante el periodo comprendido por el año inmediatamente anterior y debe tomarse de la evaluación hecha a los distintos procesos de S.I.

PRIMERA ETAPA: AUDITORÍA POLÍTICAS, OBJETIVOS Y ALCANCE

Responsable: Analista de Calidad auditor o responsable designado

La auditoría evalúa las políticas, objetivos y alcance del SGSI, verificando que estén acorde a lo dispuesto por la compañía, con el fin de garantizar que se controlan los procedimientos y procesos establecidos, y así lograr encontrar un equilibrio entre lo que está escrito y lo que se hace.

SEGUNDA ETAPA: AUDITORÍA METODOLOGIA, EVALUACION Y TRATAMIENTO DEL RIESGO

Responsable: Analista de control interno o responsable designado

Esta auditoría evalúa los procesos que involucran lo referente a los riesgos y a su tratamiento, permite determinar si la gestión de los riesgos se hace de acuerdo a lo que está implementado, y si cumple con las leyes y regulaciones vigentes que son aplicables a los procesos y a la información.

TERCERA ETAPA: AUDITORÍA PLANIFICACIÓN, OPERACIÓN Y CONTROL DE PROCESOS DE S.I

Responsable: Analista Calidad auditor o responsable designado

Esta tercera etapa se encarga de verificar que cada uno de los procesos estén planificados, coordinados y ejecutados bajo los parámetros establecidos y con controles definidos para un funcionamiento adecuado y un resultado enfocado a los objetivos de la compañía.

CUARTA ETAPA: AUDITORÍA A LA EFICACIA DE CONTROLES

Responsable: Analista de control interno y analista de informática auditor o responsable designado

En esta etapa se tiene como objetivo verificar la eficacia de los controles en los procesos de seguridad de la información donde sobresale la gestión de los riesgos y los controles asociados a estos, esta etapa debe determinar si dichos controles son efectivos para mantener los SI seguros o si de lo contrario es necesario reevaluarlos y redefinirlos.

EVALUAR HALLAZGOS

Responsable: Analista Calidad auditor, analista de informática auditor o responsable designado

Los responsables deben diligenciar un informe de auditoría de manera individual relacionando las evaluaciones y las observaciones de cada etapa auditada.

Los responsables deben generar unas recomendaciones que permitan disminuir los riesgos de S.I en los que se puedan incurrir debido a actividades como: mala ejecución de los procesos de S.I, falta de toma de acciones preventivas en cuanto a la revisión y control de los procesos y riesgos asociados, falta de compromiso en el cumplimiento de la política de S.I.

REALIZAR INFORME DE AUDITORIA

Responsable: Analista Calidad auditor, analista de informática auditor o responsable designado

Esta etapa, va orientada a entregar un informe de hallazgos de auditoría al SGSI implementado en la compañía. Este consolidado de auditorías deberá contribuir con la elaboración de planes de mejora y actividades de mejora continua.

Registro:

Formato de Informe ejecutivo de auditoría de Incidentes

INICIAR CICLO DE MEJORA CONTINUA

Responsable: Encargado de Servicios de TI o responsable designado

El Encargado de Servicios de TI o responsable designado, es responsable por el registro, la elaboración, ejecución y seguimiento de las Acciones Correctivas, Preventivas y de Mejora derivadas de la auditoria.

El registro de cada una se realiza en el formato de Acciones correctivas.

Las acciones correctivas documentadas reciben un monitoreo de estado, responsable y grado de cumplimiento en el Formato de monitoreo de Acciones Correctivas.

Registro:

Formato Acciones correctivas

Formato de monitoreo de Acciones Correctivas

REGISTROS

ANEXOS

12.6.4. Procedimiento de acción correctiva

Procedimiento de Acción Correctiva	Código:	P-SGSI-01-004
	Versión:	1
	Vigencia:	Marzo de 2015
	Página:	1 de 1

1. Objetivo
2. Alcance
3. Definiciones y abreviaturas
4. Procedimiento
5. Registro

1. OBJETIVO

Verificar que acorde a lo documentado, se ejecuten de manera pertinente las acciones correctivas definidas por la dirección, y que permitan mitigar los efectos de las amenazas materializadas en los activos de información de la compañía.

2. ALCANCE

El alcance de este procedimiento involucra todos los activos de información, y las acciones correctivas implementadas para tratar las amenazas detectadas, igualmente aplicable a las no conformidades encontradas en los procesos de auditoria interna.

3. DEFINICIONES Y ABREVIATURAS

SGSI: Sistema de Gestión de Seguridad de la Información.

5. PROCEDIMIENTO

La dirección o el responsable asignado, tendrán una lista o archivo digital con datos de las no conformidades (salen de la auditoria interna), vulnerabilidades, riesgos, o posibles amanezcas a las que se encuentra expuesta la compañía, una vez definida esta información se procede de la siguiente manera:

- Se verifica el evento o suceso ocasionado.
- Se informa a la dirección y se documenta el evento.
- Se informa al responsable de tomar las acciones correctivas (bien sea interno o externo).
- Se registran las acciones realizadas para corregir el evento o la no conformidad.
- Se documentan y se toman otras acciones en caso de ser necesario y avaladas por la dirección.

6. REGISTRO

Los registros que se obtienen de poner en práctica este procedimiento, se generan cuando las personas encargadas actualizan o realizan cambios en los documentos asociados, de estos queda el registro del documento activo con todas sus actualizaciones y demás cambios realizados, en dichos registros se involucran los formatos de acciones correctivas y el de monitoreo de acciones correctivas ligados al procedimiento de auditoria interna.

12.6.5. Procedimiento de acción preventiva

Procedimiento de Acción Preventiva	Código:	P-SGSI-01-005
	Versión:	1
	Vigencia:	Marzo de 2015
	Página:	1 de 1

1. Objetivo
2. Alcance
3. Definiciones y abreviaturas
4. Procedimiento
5. Registro

1. OBJETIVO

Verificar que acorde a lo documentado, se ejecuten de manera pertinente las acciones de carácter preventivo definidas por la dirección, y que permitan evitar al máximo que los riesgo, vulnerabilidades y amenazas a los que está expuesta la compañía, se materialicen, e impidan el normal funcionamiento de la misma o ponga en riesgo el futuro de esta.

2. ALCANCE

El alcance de este procedimiento involucra todos los activos de información, y las acciones preventivas implementadas para tratar a tiempo las posibles amenazas antes de que se materialicen.

3. DEFINICIONES Y ABREVIATURAS

SGSI: Sistema de Gestión de Seguridad de la Información.

5. PROCEDIMIENTO

La dirección o el responsable asignado, tendrán una lista o archivo digital con datos de las vulnerabilidades, riesgos, o posibles amanezcas a las que se encuentra expuesta la compañía, una vez definida esta información se procede de la siguiente manera:

- Se hace seguimiento o monitoreo a los activos de información y al cumplimiento de la política de seguridad.
- Se informa a la dirección y se documenta acerca de los posibles incumplimientos.
- Se informa al responsable de tomar las acciones preventivas (bien sea interno o externo) en caso de tener que adoptarlas.
- Se registran las acciones realizadas en cada activo de información.
- Se documentan y se toman otras acciones en caso de ser necesario y avaladas por la dirección.

6. REGISTRO

Los registros que se obtienen de poner en práctica este procedimiento, se generan cuando las personas encargadas actualizan o realizan cambios en los documentos asociados, de estos queda el registro del documento activo con todas sus actualizaciones y demás cambios realizados.

12.6.6. Procedimiento de gestión de incidentes

Procedimiento de Gestión de incidentes	Código:	P-SGSI-01-006
	Versión:	1
	Vigencia:	Marzo de 2015
	Página:	1 de 1

1. Objetivo
2. Alcance
3. Definiciones y abreviaturas
4. Procedimiento
5. Registro

1. OBJETIVO

Determinar la manera de gestionar los incidentes de Seguridad de la Información, ocurridos durante los procesos en los que intervienen activos de información

2. ALCANCE

El alcance de este procedimiento involucra todos los activos de información, y a la manera en que se dará gestión a los incidentes ocurridos en estos.

3. DEFINICIONES Y ABREVIATURAS

SGSI: Sistema de Gestión de Seguridad de la Información.

5. PROCEDIMIENTO

Se tendrá un documento con los pasos secuenciales a seguir para dar gestión oportuna a los incidentes resultantes de la aplicación diaria de los procesos en la compañía, se determina que los pasos a seguir para la gestión son:

- Nivel de Prioridad: Impacto y Urgencia, determina la importancia del incidente y cómo afecta los procesos, además del tiempo máximo que se pretende para dar solución al mismo.
- Registro: Determina la documentación del incidente reportado.
- Clasificación: Acorde al impacto y urgencia se determina el nivel de prioridad y los recursos asignados a este.
- Análisis, Resolución y Cierre: Sugiere el proceso completo y datado, desde que se generó el incidente hasta su solución.

6. REGISTRO

Los registros que se obtienen de poner en práctica este procedimiento, se generan cuando las personas encargadas documentan cada acción realizada durante el proceso de gestión de incidentes, estos registros quedan asociados al formato de gestión de incidentes de la compañía.

13. CONCLUSIONES

Con los resultados obtenidos durante la etapa de identificación, auditoría y lista de chequeo, se puede dimensionar herramientas de software, protocolos, procedimientos y actividades que mitiguen el riesgo en las empresas Color Shop y Guille Sport, implementando el desarrollo de acciones preventivas y correctivas en cada uno de los dominios seleccionados para garantizar en un porcentaje alto un óptimo funcionamiento de la organización con respecto a la seguridad informática.

El riesgo informático es un factor que puede determinar la permanencia en el mercado o la desaparición gradual o inmediata de las empresas del mismo, basados en el poder mantener o no la integridad, confiabilidad y disponibilidad de los activos de información y su relación con los procesos de la compañía.

Herramientas como las auditorías, permiten visualizar el grado de protección o desprotección en que se encuentran los activos de información en las organizaciones, los cuales ayudan a determinar las alternativas adecuadas para implementar metodologías o estructuras, que disminuyan las posibilidades de que las amenazas, riesgos y vulnerabilidades a las que se someten día a día las compañías, se materialicen y puedan causar daños irreversibles en las mismas, acoplando un plan de contingencia o política de seguridad.

Identificando los riesgos, amenazas y vulnerabilidades de cada una de las empresas, se evidencian similitudes en cuanto al desconocimiento de metodologías y procesos para gestionar la seguridad informática, por lo tanto las gráficas representan y dimensionan la falta de procesos en cada empresa para controlar las actividades y acciones, por ende es importante emparejar cada uno de los riesgos asociados a los dominios de la ISO 27002 para implementar los controles adecuados.

La implementación de un sistema de gestión de la seguridad informática (SGSI), proporciona herramientas para cada uno de los activos informáticos, recursos humanos y aquellas áreas que por sus actividades requieren de la utilización e implementación de las tecnologías de la información (TI) para desarrollar la gestión de cada uno de sus procesos, por ende se deben utilizar técnicas, estándares y metodologías como las ISO 27001, 27002 y 27005 para detectar, implementar y proporcionar herramientas que mitiguen los riesgos.

La investigación de este proyecto permitió determinar que las PYMES, no dimensionan en un alto grado, lo importante que es hoy, mantener segura la información y los activos que se interrelacionan con esta, y la importancia de llevar a cabo procesos bien estructurados y documentados, que ayuden a minimizar cualquier tipo de riesgo que ponga en peligro la continuidad del negocio.

La matriz de riesgo ayuda a determinar las acciones correctivas y preventivas para cada uno de los riesgos identificados y asociados durante la etapa de análisis de cada una de las empresas, ya que proporciona una visión general de cuál es el comportamiento de las vulnerabilidades y amenazas a partir de la caracterización en prospectiva de los escenarios más catastróficos y la probabilidad de ocurrencia.

Los cambios constantes y las dinámicas del negocio, hacen que se generen nuevas amenazas y vulnerabilidades, por lo tanto se debe mantener una capacitación constante y la aplicación de los procedimientos para mitigar los riesgos al interior y exterior de las empresas, para que se mantenga la continuidad del negocio expandiendo su cobertura.

Un Sistema de Gestión de Seguridad de la Información (SGSI), es una estructura dentro de la compañía, que permite minimizar los riesgos internos y externos a los que se expone esta, y dar un mayor grado de confiabilidad a la dirección, clientes y proveedores.

Una política de seguridad bien planteada, permite mantener control hacia procesos en los que se interactúa de forma directa o indirecta con los activos de información, y ayuda a determinar responsabilidades de los colaboradores ante dichos activos.

14. REFERENCIAS BIBLIOGRÁFICAS E INFOGRAFÍA

Acevedo, Hector. *SOC Security Operations Center. Tercerización de la seguridad*. [en línea]. [18 de noviembre del 2013]. Disponible en: http://contaduriapublica.org.mx/?p=3403

ALEGSA. Definición de vulnerabilidad. [en línea]. [15 de mayo del 2014]. Disponible en: http://www.alegsa.com.ar/Dic/vulnerabilidad.php

Artículos. *Reglamento sobre seguridad informática*. [en línea]. [02 de marzo del 2014]. Disponible en: http://www.di.sld.cu/documentos/resol/resol_6_96.pdf

Bisongo, Maria. *Metodología para el aseguramiento de entornos informatizados.* [en línea]. [02 de marzo del 2014]. Disponible en: http://materias.fi.uba.ar/7500/bisogno-tesisdegradoingenieriainformatica.pdf

Blog. *¿Qué es un mapa estratégico y para qué sirve?.* [en línea]. [16 de mayo del 2014]. Disponible en: http://www.blogtrw.com/2011/12/que-es-un-mapa-estrategico-y-para-que-sirve/

Blog. *Gestión empresarial*. [en línea]. [12 de mayo del 2014]. Disponible en: http://gestionempresarial4.wordpress.com/174-2/

Canal UPCT. *Metodología de la investigación*. [en línea]. [18 de noviembre del 2013]. Disponible en: http://www.youtube.com/watch?v=BI1Ie-edBzY

ClubEnsayos. *Seguridad Informática*. [en línea]. [07 de diciembre del 2013]. Disponible en: http://clubensayos.com/Tecnolog%C3%ADa/Seguridad-Inform%C3%A1tica/1132093.html

Comisión Europea. *¿Qué es una Pyme?.* [en línea]. [15 de mayo del 2014]. Disponible en: http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_es.htm

Concepto. *Oficina juridicial nacional*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.legal.unal.edu.co/sisjurun/normas/Norma1.jsp?i=42011

Cruz, Erik, Rodríguez, Diana. *Modelo de seguridad para la medición de vulnerabilidades y reducción de riesgos en redes de datos*. [en línea]. [02 de marzo del 2014]. Disponible en: http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/8428/1/IF2.52.pdf

Cuervo, J. *Aspectos jurídicos de internet y el comercio electrónico.* [en línea]. [13 de mayo del 2014]. Disponible en: http://www.informatica-juridica.com/trabajos/Aspectos_juridicos_de_Internet_y_el_comercio_electronico.asp

Daza, Manuel. *Seguridad informática para Pymes: ¿Gasto o inversión?.* [en línea]. [2 de Mayo de 2014]. Disponible en: http://www.baquia.com/tecnologia-y-negocios/entry/emprendedores/seguridad-informatica-para-Pymes-gasto-o-inversion

Decreto. *Artículo 160 del Decreto ley 19 de 2012*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.sic.gov.co/documents/10165/2142817/DECRETO+333+DEL+19+DE+FEBRERO+DE+2014+VIG+ENTES+ACREDITAC.pdf/3dcd1c36-533a-48fa-a72c-7fcb2181e771

DELTA. *Ley de delitos informáticos en Colombia*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

Departamento administrativo de la función pública. *Guía de diagnóstico para implementar el sistema de gestión de la calidad bajo la norma técnica de calidad en la gestión pública*. [en línea]. [11 de mayo del 2014]. Disponible en: http://portal.dafp.gov.co/form/formularios.retrive_publicaciones?no=408

Ebilio UNAD. *Biblioteca virtual*. [en línea]. [01 de diciembre del 2013]. Disponible en: http://biblioteca.unad.edu.co/

Ebilio UNAD. Lección 11: Riesgos informáticos. [en línea]. [12 de diciembre del 2014]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_11_riesgos_informticos.html

Flórez, Wilmar, Arboleda, Carlos, & Cadavid, John. *Solución integral para las PYMES mediante un UTM*. [en línea]. [3 de Mayo de 2014]. Disponible en: http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf

García, Juan. *Dinámica de Sistemas Historia*. [en línea]. [13 de noviembre del 2013]. Disponible en: http://www.dinamica-de-sistemas.com/wds5.htm

Gestion.ORG. *¿Qué es el control de gestión?.* [en línea]. [16 de mayo del 2014]. Disponible en: http://www.gestion.org/estrategia-empresarial/4594/que-es-el-control-de-gestion/

Gómez, Joel. *La seguridad y la confidencialidad de la información es obligación de todos*. [en línea]. [02 de marzo del 2014]. Disponible en: http://www.merca20.com/la-seguridad-y-confidencialidad-de-la-informacion-es-obligacion-de-todos/

Gómez, Yessica. *Seguridad de la Información*. [en línea]. [09 de diciembre del 2013]. Disponible en: http://www.slideshare.net/hvillas/seguridaddela-informacion-17506228

Hugo. *Tesis Marco Teórico*. [en línea]. [07 de diciembre del 2013]. Disponible en: http://problema.blogcindario.com/2008/10/00014-marco-teorico.html

Implementación SIG. *El ciclo de Deming*. [en línea]. [16 de mayo del 2014]. Disponible en: http://www.implementacionsig.com/index.php/generalidades-sig/55-ciclo-de-

INEGI. *Estándares Internacionales*. [en línea]. [02 de marzo del 2014]. Disponible en: http://www.youtube.com/watch?v=vIDG_moCXKo

INSEMOT. *Que información protege la gestión de la seguridad de la información*. [en línea]. [13 de noviembre del 2013]. Disponible en: http://www.insemot.eu/es/gesti%C3%B3n-de-un-si/217-what-information-is-protected-by-information-security-management

Instituto tecnológico de Sonora. Diseño de un sistema de gestión de calidad de una empresa dedicada a la elaboración y comercialización de frituras. [en línea]. [11 de mayo del 2014]. Disponible en: http://www.itson.mx/publicaciones/pacioli/Documents/no65/24.pdf

INTECO. *Implantación de un SGSI en la empresa*. [en línea]. [07 de diciembre del 2013]. Disponible en: http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO 27000. *El directorio de la norma ISO 27000.* [en línea]. [13 de mayo del 2014]. Disponible en: http://www.27000.org/other.htm

ISO. *Gestión de la seguridad de la información - 27001 ISO / IEC.* [en línea]. [12 de mayo del 2014]. Disponible en: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO27000.ES. *Que es un SGSI*. [en línea]. [12 de Noviembre del 2013]. Disponible en: http://www.iso27000.es/sgsi.html#section2a

ISO27000.ES. *Sistema de gestión de la seguridad de la información*. [en línea]. [14 de Noviembre del 2013]. Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

Jaramillo, Alfredo. *Manual de derecho de autor*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.derechodeautor.gov.co/documents/10181/331998/Cartilla+derecho+de+autor+(Alfredo+Vega).pdf/e99b0ea4-5c06-4529-ae7a-152616083d40

Logisman. *Familia de las ISO 27000: seguridad de la información*. [en línea]. [15 de mayo del 2014]. Disponible en: http://custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/

Mantilla, Samuel. *Estándares Internacionales de Auditoría*. [en línea]. [02 de marzo del 2014]. Disponible en: http://www.youtube.com/watch?v=_wWo3N8Oa2Y

Meadows, Dennis. *Los Límites del Crecimiento*. [en línea]. [13 de noviembre del 2013]. Disponible en: http://www.ayto-toledo.org/medioambiente/a21/limitescrecimiento.pdf

Ministerio de Comunicaciones. *Modelo de seguridad de la información*. [en línea]. [13 de noviembre del 2013]. Disponible en: http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

Muñoz, Hernán. *Diseño de sistema de gestión de seguridad informática.* [en línea]. [02 de marzo del 2014]. Disponible en: http://www.dspace.espol.edu.ec/bitstream/123456789/6962/8/Tesis%20de%20grado.pdf

Pallas, Gustavo. *Metodología de implementación de un SGSI en un grupo empresarial jerárquico*. [en línea]. [31 de marzo de 2014]. Disponible en: http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

Resolución. *Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5793

Resolución. *Resolución 305 de 2008*. [en línea]. [02 de marzo del 2014]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486

Ríos, Julio. *Seguridad Informática*. [en línea]. [17 de Septiembre de 2013]. Disponible en: http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml#introducca#ixzz2fCGghfuG

Rodríguez, Andrea, Erazo, Leydy, Guzmán, Luis, Acevedo, Julián. *Guía práctica para la implementación de un sistema de gestión de calidad en PYMES.* [en línea]. [11 de mayo del 2014]. Disponible en: http://www.hiperion.com.co/Guia.pdf

Santos, Alan y Tarazona, Juan. *Estudio de factibilidad para la implementación y puesta en marcha de una empresa de consultoría para organizaciones PYMES en la ciudad de Bucaramanga y su área metropolitana.* [en línea]. [11 de mayo del 2014]. Disponible en: http://repository.upb.edu.co:8080/jspui/bitstream/123456789/317/1/digital_16272.pdf

Santos, Luz. *Guía para la evaluación de seguridad en un sistema*. [en línea]. [02 de marzo del 2014]. Disponible en: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&ved=0CHYQFjAJ&url=http%3A%2F%2Fwww.acis.org.co%2Fmemorias%2FJornadasSeguridad%2FIIJNSI%2Fpamplona.doc&ei=2o8TU_zIJMKSkQf06IGICQ&usg=AFQjCNFakSrKbN2XFGBRRIvlaZ77VA8grA&sig2=Wlp21VTk_tLG6m3Ss7q6_g&bvm=bv.62286460,d.eW0

Santos, Mateo. Los retos de seguridad para las PYMES. [en línea]. [03 de mayo del 2014]. Disponible en: http://www.enter.co/#!/especiales/enterprise/los-retos-de-seguridad-para-las-Pymes/

TIME. *Dinámica Empresarial*. [en línea]. [13 de noviembre del 2013]. Disponible en: http://timerime.com/en/event/1348664/Dinmica+Empresarial+John+David+Sterman/

Web and macros. *Los activos tangibles e intangibles - ejemplos*. [en línea]. [13 de mayo del 2014]. Disponible en: http://www.webandmacros.com/activos_cuadro_mando_integral.htm

Web. *Ciclo PHVA – Planear – hacer – verificar – actuar*. [en línea]. [12 de mayo del 2014]. Disponible en: http://guajiros.udea.edu.co/fnsp/cvsp/Practica%20procesos/Metodologias%20procesos/CicloPHVA.pdf

15. ANEXOS

15.1. Carta de aceptación de Guille Sport

Ilustración 74 Carta aceptación Guille Sport

CARTA DE ACEPTACIÓN DE LA EMPRESA PARA PROYECTOS DE INVESTIGACIÓN

Medellín, 10 de Marzo de 2015

Señores

COMITÉ DE PROGRAMA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA DE LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

De manera atenta manifestamos nuestro interés y conocimiento de la propuesta de Proyecto de investigación titulada:

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA – SGSI –, PARA EMPRESAS DEL ÁREA TEXTIL EN LAS CIUDADES DE ITAGÜÍ, MEDELLÍN Y BOGOTÁ D.C. A TRAVÉS DE LA AUDITORÍA

Elaborada por el(los) estudiante(s):

Alexander Guzmán García C.C # 1030548291
Carlos Alberto Taborda Bedoya C.C # 98639837

En este sentido, nos comprometemos a participar en este proceso ofreciendo la información y el apoyo necesario para el desarrollo de la propuesta. Como documento académico conocemos que los resultados del trabajo serán registrados en la UNAD. Conocemos y aceptamos el reglamento y disposiciones sobre la realización de opciones de grado de la Universidad en mención, información suministrada por los estudiantes que realizan el proyecto.

Cordialmente,

Representante legal o su delegado:

Firma Guillermo Jimenez

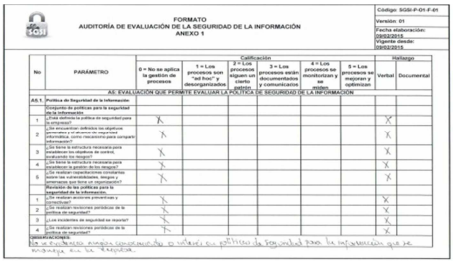
Nombres y Apellidos: Guillermo Jimenez

Nombre de la Empresa: Guille Sport

Creaciones GUILLE SPORT

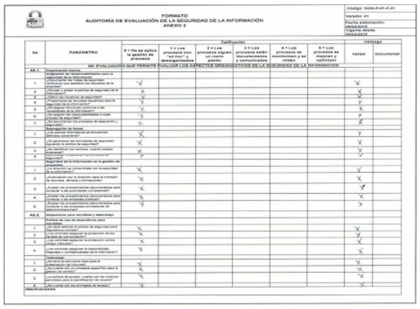
15.1.1. Anexos de auditoría Guille Sport

Ilustración 75 auditoría anexo 1 Guille Sport



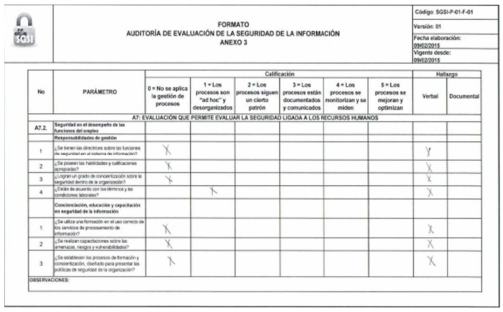
FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 1

Ilustración 76 auditoría anexo 2 Guille Sport



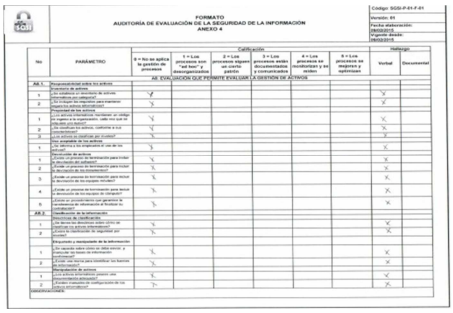
FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 2

Ilustración 77 auditoría anexo 3 Guille Sport



FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 3

Ilustración 78 auditoría anexo 4 Guille Sport



FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 4

Ilustración 79 auditoría anexo 5 Guille Sport

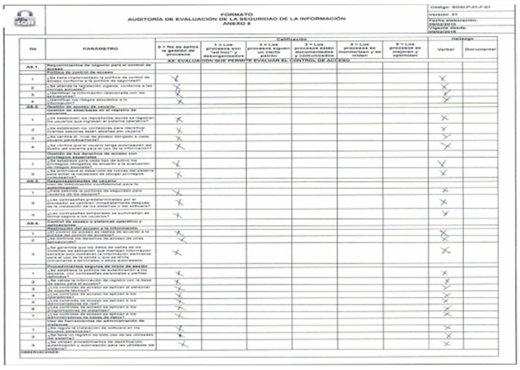
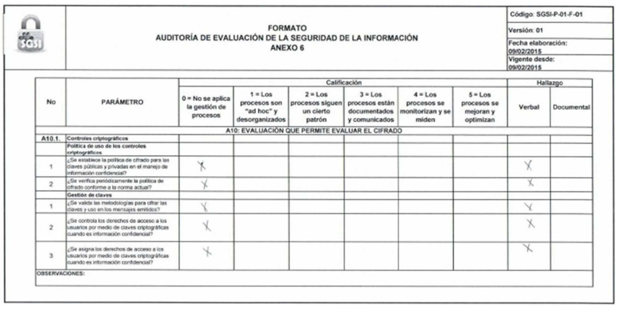


Ilustración 80 auditoría anexo 6 Guille Sport



FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 6

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A10: EVALUACIÓN QUE PERMITE EVALUAR EL CIFRADO									
A10.1.	Controles criptográficos								
	Política de uso de los controles criptográficos								
1	¿Se establece la política de cifrado para las claves públicas y privadas en el manejo de información confidencial?	X						X	
2	¿Se verifica periódicamente la política de cifrado conforme a la norma actual?	X						X	
	Gestión de claves								
1	¿Se valida las metodologías para cifrar las claves y uso en los mensajes emitidos?	X						X	
2	¿Se controla los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?	X						X	
3	¿Se asigna los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?	X						X	
OBSERVACIONES:									

Ilustración 81 auditoría anexo 7 Guille Sport

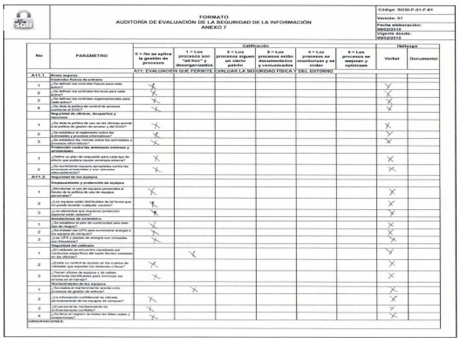


Ilustración 82 auditoría anexo 8 Guille Sport

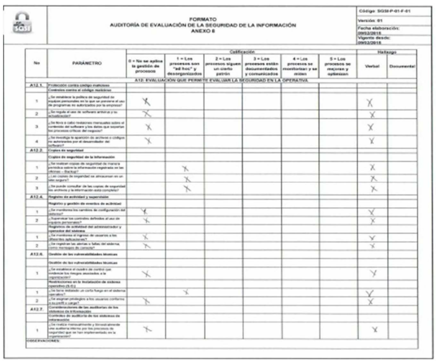


Ilustración 83 auditoría anexo 9 Guille Sport

FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 9

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A13: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LAS TELECOMUNICACIONES									
A13.2.	**Intercambio de información**								
	Mensajería electrónica								
1	¿Se establecen los protocolos para enviar la información por los canales de comunicación?	X						X	
2	¿Se verifica los canales de comunicación mensualmente identificando los canales de transmisión por el internet?	X						X	
	Acuerdos de confidencialidad y secreto								
1	¿Se documenta donde se establecen los acuerdos de confidencialidad?	X						X	
2	¿Se documenta donde se establecen las políticas de confidencialidad?	X						X	
3	¿Se monitorea el cumplimiento de los acuerdos?	X						X	
OBSERVACIONES:									

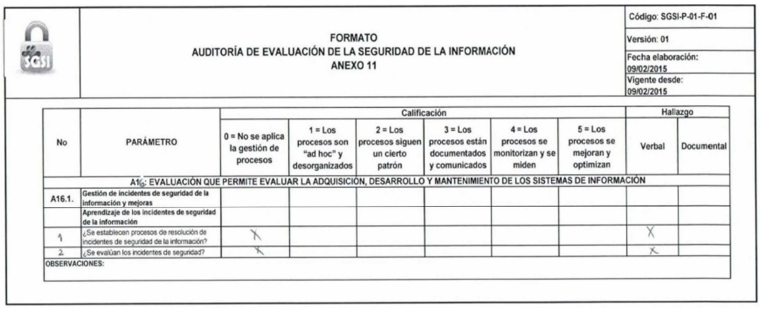
Ilustración 84 auditoría anexo 10 Guille Sport

FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 10

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A14: EVALUACIÓN QUE PERMITE EVALUAR LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN									
A14.1.	**Gestión de incidentes de seguridad de la información y mejoras**								
	Aprendizaje de los incidentes de seguridad de la información								
1	¿Se verifican las amenazas, riesgos y vulnerabilidades asociados a la empresa?	X						X	
2	¿De acuerdo a las amenazas, riesgos y vulnerabilidades se debe establecer una propuesta para disminuir el riesgo?	X						X	
A14.3.	**Datos de prueba**								
	Protección de los datos utilizados en pruebas								
1	¿Se realizan pruebas a los activos informáticos, estableciendo los mejores alternativas para mitigar los riesgos?	X						X	
2	¿Se realizan pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial?	X						X	
OBSERVACIONES:									

Ilustración 85 auditoría anexo 11 Guille Sport



FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 11

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A16: EVALUACIÓN QUE PERMITE EVALUAR LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN									
A16.1.	**Gestión de incidentes de seguridad de la información y mejoras**								
	Aprendizaje de los incidentes de seguridad de la información								
1	¿Se establecen procesos de resolución de incidentes de seguridad de la información?	X						X	
2	¿Se evalúan los incidentes de seguridad?	X						X	
OBSERVACIONES:									

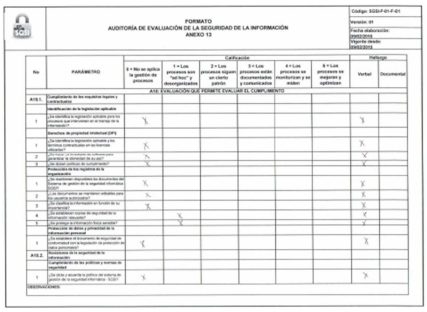
Ilustración 86 auditoría anexo 12 Guille Sport

FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 12

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A17: EVALUACIÓN QUE PERMITE EVALUAR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO									
A17.1.	**Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**								
	Planificación de la continuidad de la seguridad de la información								
1	¿Se define el plan de gestión de continuidad del negocio?	X						X	
2	¿Se define los directrices de continuidad del negocio de conformidad con la política de seguridad de la información?	X						X	
3	¿Se garantiza la seguridad del personal, la protección de los servicios y procesos de información?	X						X	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información								
1	¿Se define los planes de continuidad del negocio de acuerdo al orden de prioridades?	X						X	
2	¿Se implementa los planes de continuidad del negocio de acuerdo al orden de prioridades?	X						X	
OBSERVACIONES:									

Ilustración 87 auditoría anexo 13 Guille Sport



FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 13

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/03/2015
Vigente desde: 09/03/2015

No	PARÁMETRO	Calificación: 0 = No se aplica la gestión de procesos	1 = Los procesos son "así hoy" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Hallazgo: Verbal	Documental
	AXE: EVALUACIÓN QUE PERMITE EVALUAR EL CUMPLIMIENTO								
A18.1.	Cumplimiento de los requisitos legales y contractuales								
	Identificación de la legislación aplicable								
1	¿Se identifica la legislación aplicable para los servicios contratados en el manejo de la información?	X						X	
	Derechos de propiedad intelectual (DPI)								
1	¿Se identifica la legislación aplicable y los derechos contratados en las licencias	X						X	
2	¿Se realizan auditorías de software para garantizar la eliminación de su uso?	X						X	
3	¿Se protegen los registros de la organización?	X						X	
	Protección de los registros de la organización								
1	¿Se encuentran disponibles los documentos del Sistema de gestión de la seguridad informática (SGSI)?	X						X	
2	¿Los documentos se mantienen validados para su buena accesibilidad?	X						X	
3	¿Se clasifica la información en función de su importancia?	X						X	
4	¿Se establecen niveles de seguridad de la información?		X					X	
5	¿Se protege la información física sensible?		X					X	
	Protección de datos y privacidad de la información personal								
1	¿Se establece el encuentro de seguridad de conformidad con la legislación de protección de datos?	X						X	
A18.2.	Revisiones de la seguridad de la información								
	Revisión de las políticas y normas de seguridad								
1	¿Se dicta y acuerda la política del sistema de gestión de la seguridad informática - SGSI?	X						X	

OBSERVACIONES:

15.1.2. Anexos de Checklist Guille Sport

Ilustración 88 Checklist anexo 1 Guille Sport

FORMATO
CUESTIONARIO DE CONTROL
ANEXO 1

Código: SGSI-P-02-F-02
Versión: 01
Fecha elaboración: 02/03/2015
Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A5: EVALUAR LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN			
A5.1.	Política de Seguridad de la Información			
	Conjunto de políticas para la seguridad de la información			
1	¿Está definida la política de seguridad para la empresa?		X	
2	¿Se encuentran definidos los objetivos generales y el alcance de seguridad informática, como mecanismo para compartir información?		X	
3	¿Se tiene la estructura necesaria para establecer los objetivos de control, evaluando los riesgos?		X	
4	¿Se tiene la estructura necesaria para establecer la gestión de los riesgos?		X	
5	¿Se realizan capacitaciones constantes sobre las vulnerabilidades, riesgos y amenazas que tiene una organización?		X	
	Revisión de las políticas para la seguridad de la información.			
1	¿Se realizan acciones preventivas y correctivas?		X	
2	¿Se realizan revisiones periódicas de la política de seguridad?		X	
3	¿Los incidentes de seguridad se reporta?		X	
4	¿Se realizan revisiones periódicas de la política de seguridad?		X	

OBSERVACIONES:

Ilustración 89 Checklist anexo 2 Guille Sport

FORMATO
CUESTIONARIO DE CONTROL
ANEXO 2

Código: SGSI-P-02-F-02
Versión: 01
Fecha elaboración: 02/03/2015
Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A6: EVALUAR LOS ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
A6.1.	Organización interna			
	Asignación de responsabilidades para la seguridad de la información			
1	¿Documentar las metas de seguridad, verificando que satisface los requisitos de la empresa?		X	
2	¿Revisar y probar la política de seguridad de la información?		X	
3	¿Definir las iniciativas de seguridad?		X	
4	¿Proporciona los recursos requeridos para la seguridad de la información?		X	
5	¿Se asignan funciones conforme a las necesidades de la información?		X	
6	¿Se asignan las responsabilidades a cada proceso de seguridad?		X	
7	¿Se documentan los procesos de asignación y seguridad?		X	
	Segregación de tareas			
1	¿Los activos informáticos se encuentran definidos claramente?		X	
2	¿Se garantizan las actividades de seguridad, siguiendo la política de seguridad?		X	
3	¿Se identifican los cambios, cuando existen amenazas?		X	
4	¿Se evalúan y coordinan los controles de seguridad?		X	
	Seguridad de la información en la gestión de proyectos			
1	¿La dirección se compromete con la seguridad de la información?		X	
2	¿Autorización por la dirección para la inversión de recursos, tiempos y formaciones?		X	
3	¿Existen los procedimientos documentados para contactar a las autoridades competentes?		X	
4	¿Existen los procedimientos documentados para contactar a las entidades públicas?		X	
5	¿Existen los procedimientos documentados para contactar a las empresas proveedoras de telecomunicaciones?		X	
A6.2.	Dispositivos para movilidad y teletrabajo			
	Política de uso de dispositivos para movilidad			
1	¿Se tiene definida la política de seguridad para dispositivos móviles?		X	
2	¿Los controles aseguran la protección de los canales de comunicación?		X	
3	¿Los controles aseguran la protección contra código malicioso?		X	
4	¿Los controles aseguran la disponibilidad, integridad y confidencialidad de la información?		X	
	Teletrabajo			
1	¿Se tiene la estructura clara para la presentación de informes?			X
2	¿Se cuenta con unos procesos específicos para la gestión de cambio?			X
3	¿La política de acceso, cuenta con los módulos permitidos para la identificación de usuario?			X
4	¿Se cuenta con los privilegios de acceso?			X

OBSERVACIONES:

Ilustración 90 Checklist anexo 3 Guille Sport

FORMATO CUESTIONARIO DE CONTROL ANEXO 3	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A7: EVALUAR LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
A7.2.	**Seguridad en el desempeño de las funciones del empleo**			
	Responsabilidades de gestión			
1	¿Se tienen las directrices sobre las funciones de seguridad en el sistema de información?		X	
2	¿Se poseen las habilidades y calificaciones apropiadas?		X	
3	¿Logran un grado de concientización sobre la seguridad dentro de la organización?		X	
4	¿Están de acuerdo con los términos y las condiciones laborales?	X		
	Concienciación, educación y capacitación en seguridad de la información			
1	¿Se utiliza una formación en el uso correcto de los servicios de procesamiento de información?		X	
2	¿Se realizan capacitaciones sobre las amenazas, riesgos y vulnerabilidades?		X	
3	¿Se establecen los procesos de formación y concientización, diseñado para presentar las políticas de seguridad de la organización?		X	
OBSERVACIONES:				

Ilustración 91 Checklist anexo 4 Guille Sport

FORMATO CUESTIONARIO DE CONTROL ANEXO 4	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A8: EVALUAR LA GESTIÓN DE ACTIVOS			
A8.1.	**Responsabilidad sobre los activos**			
	Inventario de activos			
1	¿Se establece un inventario de activos informáticos por categoría?		X	
2	¿Se incluyen los requisitos para mantener seguro los activos informáticos?		X	
	Propiedad de los activos			
1	¿Los activos informáticos mantienen un código de ingreso a la organización, cada vez que se adquiere uno nuevo?		X	
2	¿Se clasifican los activos, conforme a sus características?		X	
3	¿Los activos se clasifican por niveles?		X	
	Uso aceptable de los activos			
1	¿Se informa a los empleados el uso de los activos?		X	
	Devolución de activos			
1	¿Existe un proceso de terminación para incluir la devolución del software?		X	
2	¿Existe un proceso de terminación para incluir la devolución de los documentos?		X	
3	¿Existe un proceso de terminación para incluir la devolución de los equipos móviles?		X	
4	¿Existe un proceso de terminación para incluir la devolución de los equipos de cómputo?		X	
5	¿Existe un procedimiento que garantice la transferencia de información al finalizar su contratación?		X	
A8.2.	**Clasificación de la información**			
	Directrices de clasificación			
1	¿Se tienen las directrices sobre cómo se clasifican los activos informáticos?		X	
2	¿Existe la clasificación de seguridad por niveles?		X	
	Etiquetado y manipulado de la información			
1	¿Se capacita sobre cómo se debe enviar, y manipular las bases de información confidencial?		X	
2	¿Existe una marca para identificar las fuentes de información?		X	
	Manipulación de activos			
1	¿Los activos informáticos poseen una documentación adecuada?		X	
2	¿Existen manuales de configuración de los activos informáticos?		X	
OBSERVACIONES:				

Ilustración 92 Checklist anexo 5 Guille Sport

FORMATO CUESTIONARIO DE CONTROL ANEXO 5	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

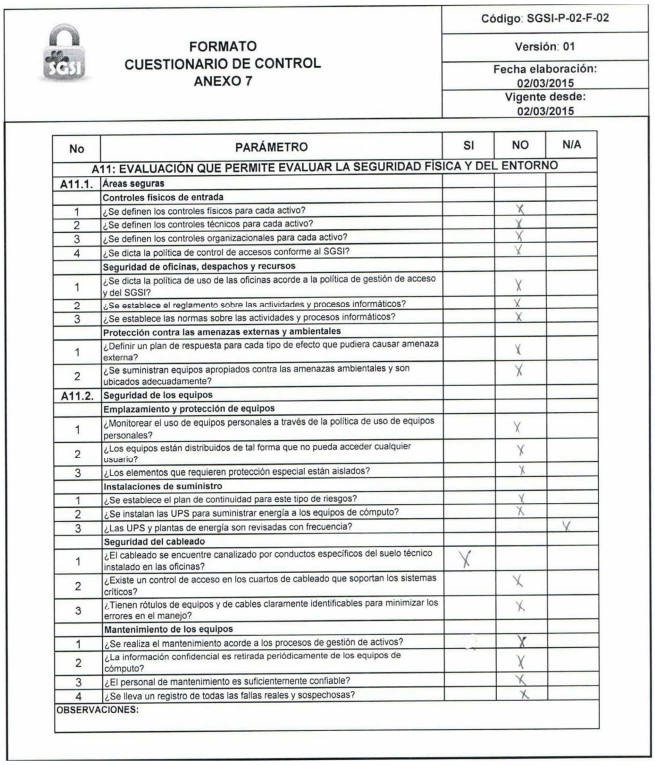
No	PARÁMETRO	SI	NO	N/A
	A9: EVALUACIÓN QUE PERMITE EVALUAR EL CONTROL DE ACCESO			
A9.1.	**Requerimientos de negocio para el control de acceso**			
	Política de control de acceso			
1	¿Se tiene implementado la política de control de acceso conforme a la política de seguridad?		X	
2	¿Se atiende la legislación vigente, conforme a las normas actuales?		X	
3	¿Identificar la información relacionada con las aplicaciones?		X	
4	¿Identificar los riesgos asociados a la información?		X	
A9.2.	**Gestión de acceso de usuario**			
	Gestión de altas/bajas en el registro de usuarios			
1	¿Se establecen los repositorios donde se registran los usuarios que ingresan al sistema operativo?		X	
2	¿Se establecen los contadores para identificar cuantas sesiones están abiertas por usuario?		X	
3	¿Se verifica el nivel de acceso otorgado a cada usuario periódicamente?		X	
4	¿Se verifica que el usuario tenga autorización del dueño del sistema para el uso de la información?		X	
	Gestión de los derechos de acceso con privilegios especiales			
1	¿Se establece para cada tipo de activo los privilegios otorgados de acuerdo a la evaluación de riesgos asociada?		X	
2	¿Se promueve el desarrollo de rutinas del sistema para evitar la necesidad de otorgar privilegios innecesarios?		X	
A9.3.	**Responsabilidades de usuario**			
	Uso de información confidencial para la autenticación			
1	¿Está definida la políticas de seguridad para usuarios de los equipos?		X	
2	¿Las contraseñas predeterminadas por el proveedor se cambian inmediatamente después de la instalación de los sistemas o del software?		X	
3	¿Las contraseñas temporales se suministran de forma segura a los usuarios?		X	
A9.4.	**Control de acceso a sistemas operativo y aplicaciones**			
	Restricción del acceso a la información			
1	¿El control de acceso se realiza de acuerdo a la política del control de accesos?		X	
2	¿Se controla los derechos de acceso de otras aplicaciones?		X	
3	¿Se garantiza que los datos de salida de los sistemas de aplicación que manejan información sensible solo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados?		X	
	Procedimientos seguros de inicio de sesión			
1	¿Se establece la política de autenticación a los equipos, con contraseñas personales y perfiles definidos?		X	
2	¿Se valida la información de registro con la base de datos para el acceso?		X	
3	¿Los controles de acceso se aplican al personal de soporte técnico?		X	
4	¿Los controles de acceso se aplican a los operadores?		X	
5	¿Los controles de acceso se aplican a los administradores de red?		X	
6	¿Los controles de acceso se aplican a los programadores de sistemas?		X	
7	¿Los controles de acceso se aplican a los administradores de bases de datos?		X	
	Uso de herramientas de administración de sistemas			
1	¿Se regula la instalación de software en los equipos personales?		X	
2	¿Se lleva un registro de todo uso de las utilidades del sistema?		X	
3	¿Se utilizan procedimientos de identificación, autenticación y autorización para las utilidades del sistema?		X	
OBSERVACIONES:				

Ilustración 93 Checklist anexo 6 Guille Sport

FORMATO CUESTIONARIO DE CONTROL ANEXO 6	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A10: EVALUACIÓN QUE PERMITE EVALUAR EL CIFRADO			
A10.1.	**Controles criptográficos**			
	Política de uso de los controles criptográficos			
1	¿Se establece la política de cifrado para las claves públicas y privadas en el manejo de información confidencial?		X	
2	¿Se verifica periódicamente la política de cifrado conforme a la norma actual?		X	
	Gestión de claves			
1	¿Se valida las metodologías para cifrar las claves y uso en los mensajes emitidos?		X	
2	¿Se controla los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?		X	
3	¿Se asigna los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?		X	
OBSERVACIONES:				

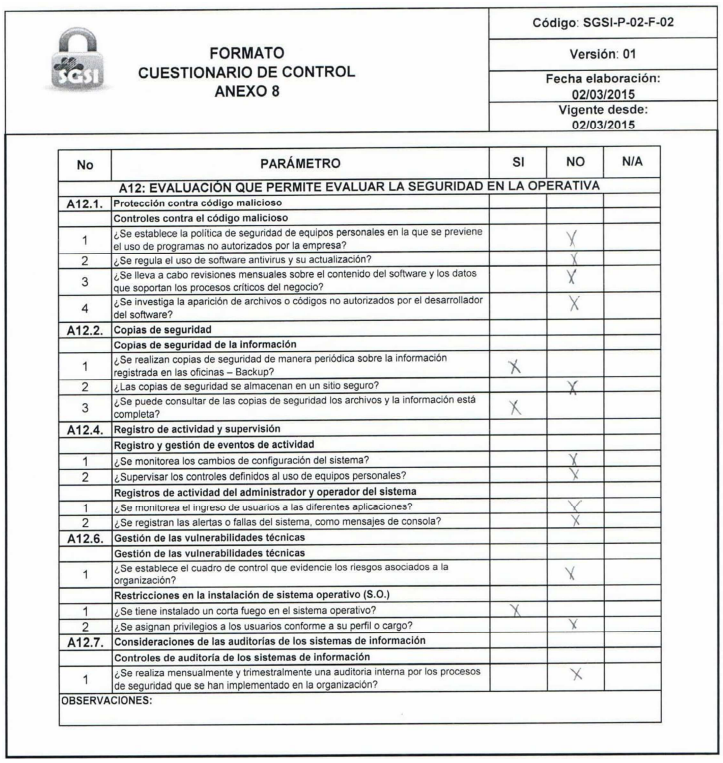
Ilustración 94 Checklist anexo 7 Guille Sport



FORMATO CUESTIONARIO DE CONTROL ANEXO 7	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A11: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD FÍSICA Y DEL ENTORNO				
A11.1.	**Áreas seguras**			
	Controles físicos de entrada			
1	¿Se definen los controles físicos para cada activo?		X	
2	¿Se definen los controles técnicos para cada activo?		X	
3	¿Se definen los controles organizacionales para cada activo?		X	
4	¿Se dicta la política de control de accesos conforme al SGSI?		X	
	Seguridad de oficinas, despachos y recursos			
1	¿Se dicta la política de uso de las oficinas acorde a la política de gestión de acceso y del SGSI?		X	
2	¿Se establece el reglamento sobre las actividades y procesos informáticos?		X	
3	¿Se establece las normas sobre las actividades y procesos informáticos?		X	
	Protección contra las amenazas externas y ambientales			
1	¿Definir un plan de respuesta para cada tipo de efecto que pudiera causar amenaza externa?		X	
2	¿Se suministran equipos apropiados contra las amenazas ambientales y son ubicados adecuadamente?		X	
A11.2.	**Seguridad de los equipos**			
	Emplazamiento y protección de equipos			
1	¿Monitorear el uso de equipos personales a través de la política de uso de equipos personales?		X	
2	¿Los equipos están distribuidos de tal forma que no pueda acceder cualquier usuario?		X	
3	¿Los elementos que requieren protección especial están aislados?		X	
	Instalaciones de suministro			
1	¿Se establece el plan de continuidad para este tipo de riesgos?		X	
2	¿Se instalan las UPS para suministrar energía a los equipos de cómputo?		X	
3	¿Las UPS y plantas de energía son revisadas con frecuencia?			X
	Seguridad del cableado			
1	¿El cableado se encuentre canalizado por conductos específicos del suelo técnico instalado en las oficinas?	X		
2	¿Existe un control de acceso en los cuartos de cableado que soportan los sistemas críticos?		X	
3	¿Tienen rótulos de equipos y de cables claramente identificables para minimizar los errores en el manejo?		X	
	Mantenimiento de los equipos			
1	¿Se realiza el mantenimiento acorde a los procesos de gestión de activos?		X	
2	¿La información confidencial es retirada periódicamente de los equipos de cómputo?		X	
3	¿El personal de mantenimiento es suficientemente confiable?		X	
4	¿Se lleva un registro de todas las fallas reales y sospechosas?		X	
OBSERVACIONES:				

Ilustración 95 Checklist anexo 8 Guille Sport



FORMATO CUESTIONARIO DE CONTROL ANEXO 8	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A12: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LA OPERATIVA				
A12.1.	**Protección contra código malicioso**			
	Controles contra el código malicioso			
1	¿Se establece la política de seguridad de equipos personales en la que se previene el uso de programas no autorizados por la empresa?		X	
2	¿Se regula el uso de software antivirus y su actualización?		X	
3	¿Se lleva a cabo revisiones mensuales sobre el contenido del software y los datos que soportan los procesos críticos del negocio?		X	
4	¿Se investiga la aparición de archivos o códigos no autorizados por el desarrollador del software?		X	
A12.2.	**Copias de seguridad**			
	Copias de seguridad de la información			
1	¿Se realizan copias de seguridad de manera periódica sobre la información registrada en las oficinas – Backup?	X		
2	¿Las copias de seguridad se almacenan en un sitio seguro?		X	
3	¿Se puede consultar de las copias de seguridad los archivos y la información está completa?	X		
A12.4.	**Registro de actividad y supervisión**			
	Registro y gestión de eventos de actividad			
1	¿Se monitorea los cambios de configuración del sistema?		X	
2	¿Supervisar los controles definidos al uso de equipos personales?		X	
	Registros de actividad del administrador y operador del sistema			
1	¿Se monitorea el ingreso de usuarios a las diferentes aplicaciones?		X	
2	¿Se registran las alertas o fallas del sistema, como mensajes de consola?		X	
A12.6.	**Gestión de las vulnerabilidades técnicas**			
	Gestión de las vulnerabilidades técnicas			
1	¿Se establece el cuadro de control que evidencie los riesgos asociados a la organización?		X	
	Restricciones en la instalación de sistema operativo (S.O.)			
1	¿Se tiene instalado un corta fuego en el sistema operativo?	X		
2	¿Se asignan privilegios a los usuarios conforme a su perfil o cargo?		X	
A12.7.	**Consideraciones de las auditorías de los sistemas de información**			
	Controles de auditoría de los sistemas de información			
1	¿Se realiza mensualmente y trimestralmente una auditoria interna por los procesos de seguridad que se han implementado en la organización?		X	
OBSERVACIONES:				

Ilustración 96 Checklist anexo 9 Guille Sport

FORMATO CUESTIONARIO DE CONTROL ANEXO 9	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A13: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LAS TELECOMUNICACIONES				
A13.2.	Intercambio de información			
	Mensajería electrónica			
1	¿Se establecen los protocolos para enviar la información por los canales de comunicación?		X	
2	¿Se verifica los canales de comunicación mensualmente identificando los canales de transmisión por el internet?		X	
	Acuerdos de confidencialidad y secreto			
1	¿Se documenta donde se establecen los acuerdos de confidencialidad?		X	
2	¿Se documenta donde se establecen las políticas de confidencialidad?		X	
3	¿Se monitorea el cumplimiento de los acuerdos?		X	
OBSERVACIONES:				

Ilustración 97 Checklist anexo 10 Guille Sport

FORMATO CUESTIONARIO DE CONTROL ANEXO 10	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A14: EVALUACIÓN QUE PERMITE EVALUAR LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE				
A14.1.	Gestión de incidentes de seguridad de la información y mejoras			
	Aprendizaje de los incidentes de seguridad de la información			
1	¿Se verifican las amenazas, riesgos y vulnerabilidades asociados a la empresa?		X	
2	¿De acuerdo a las amenazas, riesgos y vulnerabilidades se debe establecer una propuesta para disminuir el riesgo?		X	
A14.3.	Datos de prueba			
	Protección de los datos utilizados en pruebas			
1	¿Se realizan pruebas a los activos informáticos, estableciendo las mejores alternativas para mitigar los riesgos?		X	
2	¿Se realizan pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial?		X	
OBSERVACIONES:				

Ilustración 98 Checklist anexo 11 Guille Sport

FORMATO CUESTIONARIO DE CONTROL ANEXO 11	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A16: EVALUACIÓN QUE PERMITE EVALUAR LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO				
A16.1.	Gestión de incidentes de seguridad de la información y mejoras			
	Aprendizaje de los incidentes de seguridad de la información			
	¿Se establecen procesos de resolución de incidentes de seguridad de la información?		X	
	¿Se evalúan los incidentes de seguridad?		X	
OBSERVACIONES:				

Ilustración 99 Checklist anexo 12 Guille Sport

FORMATO CUESTIONARIO DE CONTROL ANEXO 12	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A17: EVALUACIÓN QUE PERMITE EVALUAR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN				
A17.1.	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio			
	Planificación de la continuidad de la seguridad de la información			
1	¿Se define el proceso de gestión de continuidad del negocio?		X	
2	¿Se define las directrices de continuidad del negocio de conformidad con la política de seguridad de la información?		X	
3	¿Se garantiza la seguridad del personal, la protección de los servicios y procesos de información?		X	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información			
1	¿Se define los planes de continuidad del negocio de acuerdo al orden de prioridades?		X	
2	¿Se implementa los planes de continuidad del negocio de acuerdo al orden de prioridades?		X	
OBSERVACIONES:				

Ilustración 100 Checklist anexo 13 Guille Sport

	FORMATO **CUESTIONARIO DE CONTROL** **ANEXO 13**	**Código: SGSI-P-02-F-02** **Versión: 01** **Fecha elaboración: 02/03/2015** **Vigente desde: 02/03/2015**

No	PARÁMETRO	SI	NO	N/A
	A18: EVALUACIÓN QUE PERMITE EVALUAR EL CUMPLIMIENTO			
A18.1.	**Cumplimiento de los requisitos legales y contractuales**			
	Identificación de la legislación aplicable			
1	¿Se identifica la legislación aplicable para los procesos que intervienen en el manejo de la información?		X	
	Derechos de propiedad intelectual (DPI)			
1	¿Se identifica la legislación aplicable y los términos contractuales en las licencias utilizadas?	X		
2	¿Se hace un inventario de software para garantizar la idoneidad de su uso?		X	
3	¿Se dictan políticas de cumplimiento?		X	
	Protección de los registros de la organización			
1	¿Se mantienen disponibles los documentos del Sistema de gestión de la seguridad informática - SGSI?		X	
2	¿Los documentos se mantienen editables para los usuarios autorizados?		X	
3	¿Se clasifica la información en función de su importancia?	X		
4	¿Se establecen copias de seguridad de la información relevante?	X		
5	¿Se protege la información física sensible?	X		
	Protección de datos y privacidad de la información personal			
1	¿Se establece el documento de seguridad de conformidad con la legislación de protección de datos personales?		X	
A18.2.	**Revisiones de la seguridad de la información**			
	Cumplimiento de las políticas y normas de seguridad			
1	¿Se dicta y acuerda la política del sistema de gestión de la seguridad informática - SGSI?		X	
OBSERVACIONES:				

15.2. Carta de aceptación de Color Shop

Ilustración 101 Carta aceptación Color Shop

CARTA DE ACEPTACIÓN DE LA EMPRESA PARA PROYECTOS DE INVESTIGACIÓN

Medellín, 18 de Marzo de 2015

Señores

COMITÉ DE PROGRAMA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA DE LA UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

De manera atenta manifestamos nuestro interés y conocimiento de la propuesta de Proyecto de investigación titulada:

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD INFORMÁTICA – SGSI –, PARA EMPRESAS DEL ÁREA TEXTIL EN LAS CIUDADES DE ITAGÜÍ, MEDELLÍN Y BOGOTÁ D.C. A TRAVÉS DE LA AUDITORÍA

Elaborada por el(los) estudiante(s):

Alexander Guzmán García C.C # 1030548291
Carlos Alberto Taborda Bedoya C.C # 98639837

En este sentido, nos comprometemos a participar en este proceso ofreciendo la información y el apoyo necesario para el desarrollo de la propuesta. Como documento académico conocemos que los resultados del trabajo serán registrados en la UNAD. Conocemos y aceptamos el reglamento y disposiciones sobre la realización de opciones de grado de la Universidad en mención, información suministrada por los estudiantes que realizan el proyecto.

Cordialmente,

Representante legal o su delegado:

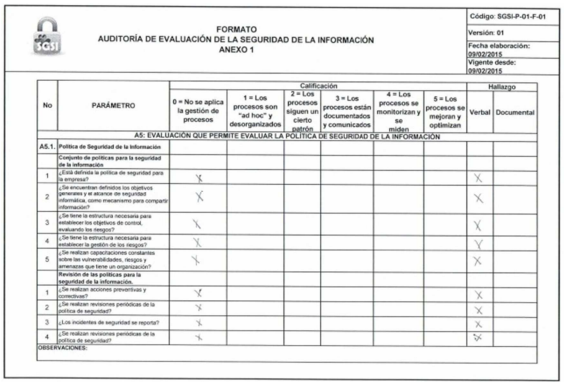
Firma _____

Nombres y Apellidos: Diego Alexander Polanco Quintero

Nombre de la Empresa: Color Shop

15.2.1. Anexos de auditoría Color Shop

Ilustración 102 auditoría anexo 1 Color Shop

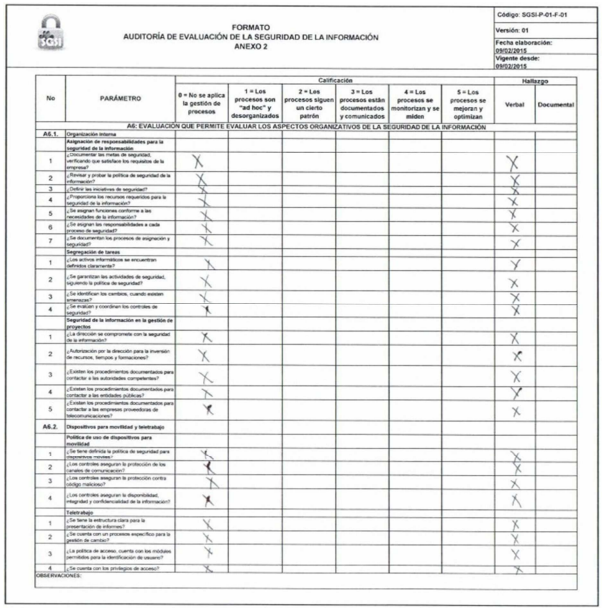


FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 1

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A5: EVALUACIÓN QUE PERMITE EVALUAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN									
A5.1.	**Política de Seguridad de la Información**								
	Conjunto de políticas para la seguridad de la información								
1	¿Está definida la política de seguridad para la empresa?		X					X	
2	¿Se encuentran definidos los objetivos generales y el alcance de seguridad informática, como mecanismo para compartir información?		X					X	
3	¿Se tiene la estructura necesaria para establecer los objetivos de control, evaluando los riesgos?		X					X	
4	¿Se tiene la estructura necesaria para establecer la gestión de los riesgos?		X					X	
5	¿Se realizan capacitaciones constantes sobre las vulnerabilidades, riesgos y amenazas que tiene un organización?		X					X	
	Revisión de las políticas para la seguridad de la información.								
1	¿Se realizan acciones preventivas y correctivas?		X					X	
2	¿Se realizan revisiones periódicas de la política de seguridad?		X					X	
3	¿Los incidentes de seguridad se reporta?		X					X	
4	¿Se realizan revisiones periódicas de la política de seguridad?		X					X	
OBSERVACIONES:									

Ilustración 103 auditoría anexo 2 Color Shop

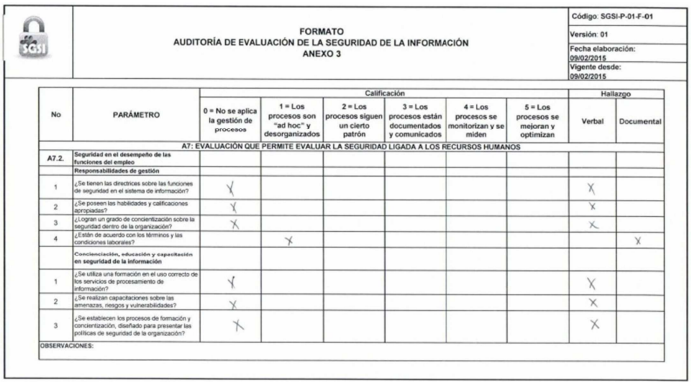


FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 2

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A6: EVALUACIÓN QUE PERMITE EVALUAR LOS ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN									
A6.1.	Organización interna								
	Asignación de responsabilidades para la seguridad de la información								
1	¿Documentar las metas de seguridad, verificando que satisfacen los requisitos de la empresa?	X						X	
2	¿Revisar y probar la política de seguridad de la información?	X						X	
3	¿Definir las iniciativas de seguridad?	X						X	
4	¿Proporciona los recursos requeridos para la seguridad de la información?	X						X	
5	¿Se asignan funciones conforme a las necesidades de la información?	X						X	
6	¿Se asignan las responsabilidades a cada proceso de seguridad?	X						X	
7	¿Se documentan los procesos de asignación y seguridad?	X						X	
	Segregación de tareas								
1	¿Las actitvas informáticas se encuentran definidos claramente?	X						X	
2	¿Se garantizan las actividades de seguridad, siguiendo la política de seguridad?	X						X	
3	¿Se identifican los cambios, cuando existen amenazas?	X						X	
4	¿Se evalúan y coordinan los controles de seguridad?	X						X	
	Seguridad de la información en la gestión de proyectos								
1	¿La dirección se compromete con la seguridad de la información?	X						X	
2	¿Autorización por la dirección para la inversión de recursos, tiempo y formaciones?	X						X	
3	¿Existen los procedimientos documentados para contactar a las autoridades competentes?	X						X	
4	¿Existen los procedimientos documentados para contactar a las entidades públicas?	X						X	
5	¿Existen los procedimientos documentados para contactar a las empresas proveedoras de telecomunicaciones?	X						X	
A6.2.	**Dispositivos para movilidad y teletrabajo**								
	Política de uso de dispositivos para movilidad								
1	¿Se tiene definida la política de seguridad para dispositivos móviles?	X						X	
2	¿Los controles aseguran la protección de los canales de comunicación?	X						X	
3	¿Los controles aseguran la protección contra código malicioso?	X						X	
4	¿Los controles aseguran la disponibilidad, integridad y confidencialidad de la información?	X						X	
	Teletrabajo								
1	¿Se tiene la estructura clara para la comercialización de informes?	X						X	
2	¿Se cuenta con un procesos específico para la gestión de control?	X						X	
3	¿La política de acceso, cuenta con los métodos permitidos para la identificación de usuario?	X						X	
4	¿Se cuenta con los privilegios de acceso?	X						X	
OBSERVACIONES:									

Ilustración 104 auditoría anexo 3 Color Shop

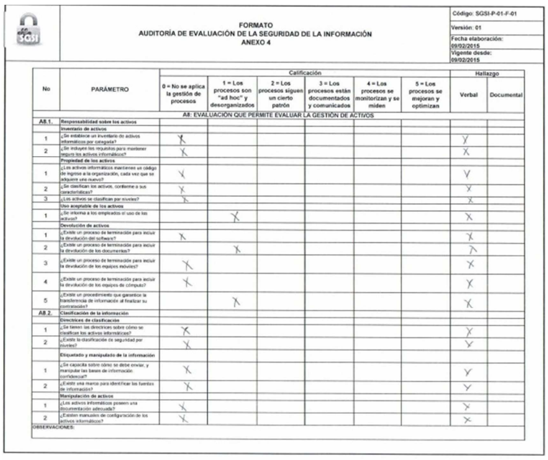


FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 3

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A7: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS									
A7.2.	**Seguridad en el desempeño de las funciones del empleo**								
	Responsabilidades de gestión								
1	¿Se tienen las directrices sobre las funciones de seguridad en el sistema de información?	X						X	
2	¿Se poseen las habilidades y calificaciones apropiadas?	X						X	
3	¿Logran un grado de concientización sobre la seguridad dentro de la organización?	X						X	
4	¿Están de acuerdo con los términos y las condiciones laborales?		X						X
	Concienciación, educación y capacitación en seguridad de la información								
1	¿Se utiliza una formación en el uso correcto de los servicios de procesamiento de información?	X						X	
2	¿Se realizan capacitaciones sobre las amenazas, riesgos y vulnerabilidades?	X						X	
3	¿Se establecen los procesos de formación y concientización, diseñado para presentar las políticas de seguridad de la organización?	X						X	
OBSERVACIONES:									

Ilustración 105 auditoría anexo 4 Color Shop

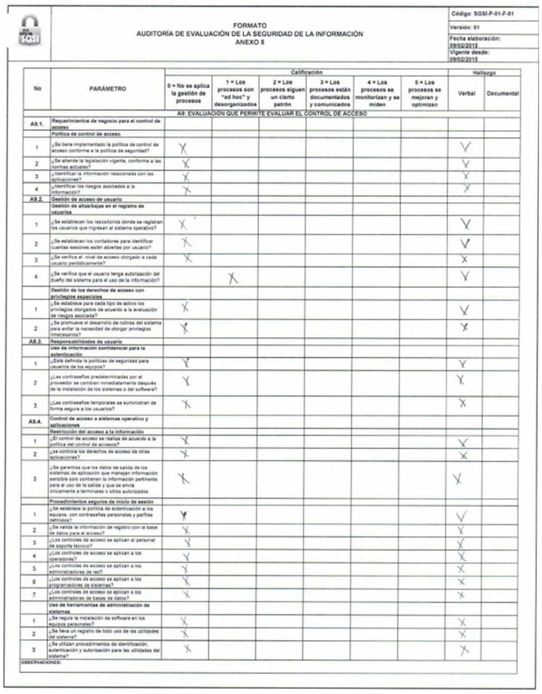


FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 4

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación: 0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Hallazgo: Verbal	Documental
	A8: EVALUACIÓN QUE PERMITE EVALUAR LA GESTIÓN DE ACTIVOS								
A8.1.	**Responsabilidad sobre los activos**								
	Inventario de activos								
1	¿Se establece un inventario de activos informáticos por categoría?	X						X	
2	¿Se incluyen los requisitos para mantener seguro los activos informáticos?	X						X	
	Propiedad de los activos								
1	¿Los activos informáticos mantienen un código de ingreso a la organización, cada vez que se adquiere uno nuevo?	X						X	
2	¿Se clasifican los activos, conforme a sus características?	X						X	
3	¿Los activos se clasifican por niveles?	X						X	
	Uso aceptable de los activos								
1	¿Se informa a los empleados el uso de los activos?		X					X	
	Devolución de activos								
1	¿Existe un proceso de terminación para incluir la devolución del software?	X						X	
2	¿Existe un proceso de terminación para incluir la devolución de los documentos?		X					X	
3	¿Existe un proceso de terminación para incluir la devolución de los equipos móviles?	X						X	
4	¿Existe un proceso de terminación para incluir la devolución de los equipos de cómputo?	X						X	
5	¿Existe un procedimiento que garantice la transferencia de información al finalizar su contratación?		X					X	
A8.2.	**Clasificación de la información**								
	Directrices de clasificación								
1	¿Se tienen las directrices sobre cómo se clasifican los activos informáticos?	X						X	
2	¿Existe la clasificación de seguridad por niveles?	X						X	
	Etiquetado y manipulado de la información								
1	¿Se capacita sobre cómo se debe enviar, y manipular las bases de información confidencial?	X						X	
2	¿Existe una marca para identificar las fuentes de información?	X						X	
	Manipulación de activos								
1	¿Los activos informáticos poseen una documentación adecuada?	X						X	
2	¿Existen manuales de configuración de los activos informáticos?	X						X	
OBSERVACIONES:									

Ilustración 106 auditoría anexo 5 Color Shop



FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 5

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación: 0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Hallazgo: Verbal	Documental
	A9: EVALUACIÓN QUE PERMITE EVALUAR EL CONTROL DE ACCESO								
A9.1.	**Requerimientos de negocio para el control de acceso**								
	Política de control de acceso								
1	¿Se tiene implementado la política de control de acceso conforme a la política de seguridad?	X						X	
2	¿Se atiende la legislación vigente, conforme a las normas actuales?	X						X	
3	¿Identificar la información relacionada con las aplicaciones?	X						X	
4	¿Identificar los riesgos asociados a la información?	X						X	
A9.2.	**Gestión de acceso de usuario**								
	Gestión de altas/bajas en el registro de usuarios								
1	¿Se establecen los repositorios donde se registran los usuarios que ingresan al sistema operativo?	X						X	
2	¿Se establecen los contadores para identificar cuantas sesiones están abiertas por usuario?	X						X	
3	¿Se verifica el nivel de acceso otorgado a cada usuario periódicamente?	X						X	
4	¿Se verifica que el usuario tenga autorización del dueño del sistema para el uso de la información?		X					X	
	Gestión de los derechos de acceso con privilegios especiales								
1	¿Se establece para cada tipo de activo los privilegios otorgados de acuerdo a la evaluación de riesgos asociada?	X						X	
2	¿Se promueve el desarrollo de rutinas del sistema para evitar la necesidad de otorgar privilegios innecesarios?	X						X	
A9.3.	**Responsabilidades de usuario**								
	Uso de información confidencial para la autenticación								
1	¿Está definida la políticas de seguridad para usuarios de los equipos?	X						X	
2	¿Las contraseñas predeterminadas por el proveedor se cambian inmediatamente después de la instalación de los sistemas o del software?	X						X	
3	¿Las contraseñas temporales se suministran de forma segura a los usuarios?	X						X	
A9.4.	**Control de acceso a sistemas operativo y aplicaciones**								
	Restricción del acceso a la información								
1	¿El control de acceso se realiza de acuerdo a la política del control de accesos?	X						X	
2	¿se controla los derechos de acceso de otras aplicaciones?	X						X	
3	¿Se garantiza que los datos de salida de los sistemas de aplicación que manejan información sensible solo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados	X						X	
	Procedimientos seguros de inicio de sesión								
1	¿Se establece la política de autenticación a los equipos, con contraseñas personales y perfiles definidos?	X						X	
2	¿Se valida la información de registro con la base de datos para el acceso?	X						X	
3	¿Los controles de acceso se aplican al personal de soporte técnico?	X						X	
4	¿Los controles de acceso se aplican a los operadores?	X						X	
5	¿Los controles de acceso se aplican a los administradores de red?	X						X	
6	¿Los controles de acceso se aplican a los programadores de sistemas?	X						X	
7	¿Los controles de acceso se aplican a los administradores de bases de datos?	X						X	
	Uso de herramientas de administración de sistemas								
1	¿Se regula la instalación de software en los equipos personales?	X						X	
2	¿Se lleva un registro de todo uso de las utilidades del sistema?	X						X	
3	¿Se utilizan procedimientos de identificación, autenticación y autorización para las utilidades del sistema?	X						X	
OBSERVACIONES:									

Ilustración 107 auditoría anexo 6 Color Shop

FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 6

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación: 0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Hallazgo: Verbal	Documental
	A10: EVALUACIÓN QUE PERMITE EVALUAR EL CIFRADO								
A10.1.	**Controles criptográficos**								
	Política de uso de los controles criptográficos								
1	¿Se establece la política de cifrado para las claves públicas y privadas en el manejo de información confidencial?	X						X	
2	¿Se verifica periódicamente la política de cifrado conforme a la norma actual?	X						X	
	Gestión de claves								
1	¿Se valida las metodologías para cifrar las claves y uso en los mensajes emitidos?	X						X	
2	¿Se controla los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?	X						X	
3	¿Se asigna los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?	X						X	
OBSERVACIONES:									

Ilustración 108 auditoría anexo 7 Color Shop

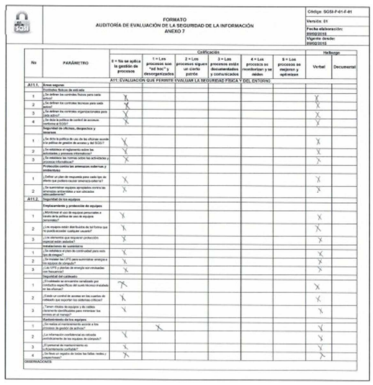


Ilustración 109 auditoría anexo 8 Color Shop

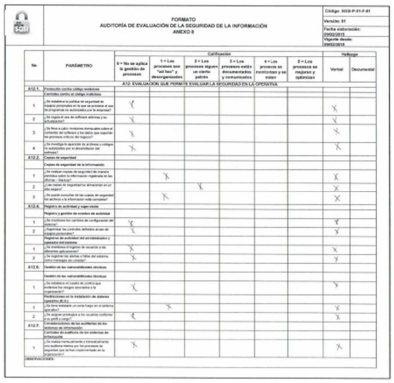
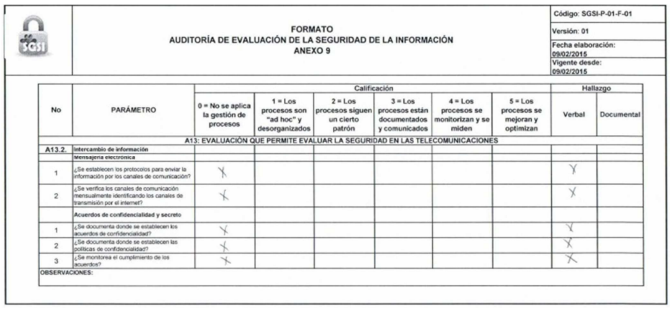


Ilustración 110 auditoría anexo 9 Color Shop



FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 9

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A13: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LAS TELECOMUNICACIONES									
A13.2.	**Intercambio de información mensajería electrónica**								
1	¿Se establecen los protocolos para enviar la información por los canales de comunicación?	X						Y	
2	¿Se verifica los canales de comunicación mensualmente identificando los canales de transmisión por el internet?	X						X	
	Acuerdos de confidencialidad y secreto								
1	¿Se documenta donde se establecen los acuerdos de confidencialidad?	X						Y	
2	¿Se documenta donde se establecen las políticas de confidencialidad?	X						X	
3	¿Se monitorea el cumplimiento de los acuerdos?	X						X	
OBSERVACIONES:									

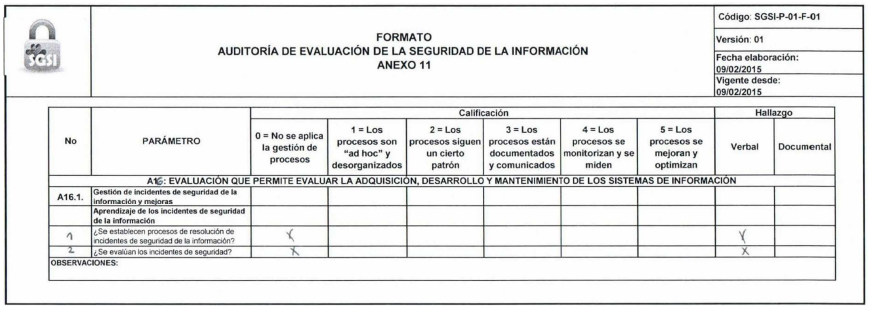
Ilustración 111 auditoría anexo 10 Color Shop

FORMATO
AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
ANEXO 10

Código: SGSI-P-01-F-01
Versión: 01
Fecha elaboración: 09/02/2015
Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A14: EVALUACIÓN QUE PERMITE EVALUAR LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN									
A14.1.	**Gestión de incidentes de seguridad de la información y mejoras**								
	Aprendizaje de los incidentes de seguridad de la información								
1	¿Se verifican las amenazas, riesgos y vulnerabilidades asociados a la empresa?	X						X	
2	¿De acuerdo a las amenazas, riesgos y vulnerabilidades se debe establecer una propuesta para disminuir el riesgo?	X						X	
A14.3.	**Datos de prueba**								
	Protección de los datos utilizados en pruebas								
1	¿Se realizan pruebas a los activos informáticos, estableciendo las mejores alternativas para mitigar los riesgos?	X						X	
2	¿Se realizan pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial?	X						X	
OBSERVACIONES:									

Ilustración 112 auditoría anexo 11 Color Shop



	FORMATO AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ANEXO 11	Código: SGSI-P-01-F-01 Versión: 01 Fecha elaboración: 09/02/2015 Vigente desde: 09/02/2015

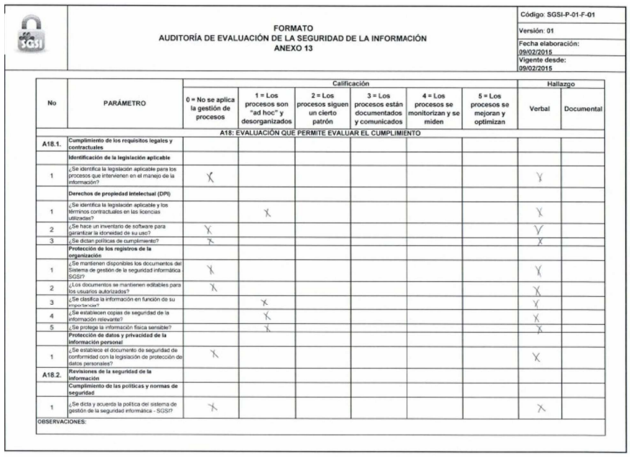
No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A16: EVALUACIÓN QUE PERMITE EVALUAR LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN									
A16.1.	**Gestión de incidentes de seguridad de la información y mejoras**								
	Aprendizaje de los incidentes de seguridad de la información								
1	¿Se establecen procesos de resolución de incidentes de seguridad de la información?	X						X	
2	¿Se evalúan los incidentes de seguridad?	X						X	
OBSERVACIONES:									

Ilustración 113 auditoría anexo 12 Color Shop

	FORMATO AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ANEXO 12	Código: SGSI-P-01-F-01 Versión: 01 Fecha elaboración: 09/02/2015 Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A17: EVALUACIÓN QUE PERMITE EVALUAR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO									
A17.1.	**Aspectos de la seguridad de la información en la gestión de la continuidad del negocio**								
	Planificación de la continuidad de la seguridad de la información								
1	¿Se define el proceso de gestión de continuidad del negocio?	X						X	
2	¿Se define las directrices de continuidad del negocio de conformidad con la política de seguridad de la información?	X						X	
3	¿Se garantiza la seguridad del personal, la protección de los servicios y procesos de información?	X						X	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información								
1	¿Se define los planes de continuidad del negocio de acuerdo al orden de prioridades?	X						X	
2	¿Se implementa los planes de continuidad del negocio de acuerdo al orden de prioridades?	X						X	
OBSERVACIONES:									

Ilustración 114 auditoría anexo 13 Color Shop

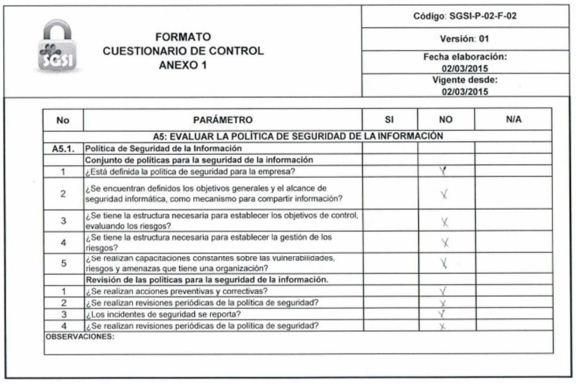


	FORMATO AUDITORÍA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ANEXO 13	Código: SGSI-P-01-F-01 Versión: 01 Fecha elaboración: 09/02/2015 Vigente desde: 09/02/2015

No	PARÁMETRO	Calificación						Hallazgo	
		0 = No se aplica la gestión de procesos	1 = Los procesos son "ad hoc" y desorganizados	2 = Los procesos siguen un cierto patrón	3 = Los procesos están documentados y comunicados	4 = Los procesos se monitorizan y se miden	5 = Los procesos se mejoran y optimizan	Verbal	Documental
A18: EVALUACIÓN QUE PERMITE EVALUAR EL CUMPLIMIENTO									
A18.1.	**Cumplimiento de los requisitos legales y contractuales**								
	Identificación de la legislación aplicable								
1	¿Se identifica la legislación aplicable para los procesos que intervienen en el manejo de la información?	X						X	
	Derechos de propiedad intelectual (DPI)								
1	¿Se identifica la legislación aplicable y los términos contractuales en las licencias utilizadas?		X					X	
2	¿Se hace un inventario de software para garantizar la idoneidad de su uso?	X						X	
3	¿Se dictan políticas de cumplimiento?	X						X	
	Protección de los registros de la organización								
1	¿Se mantienen disponibles los documentos del Sistema de gestión de la seguridad informática SGSI?	X						X	
2	¿Los documentos se mantienen editables para los usuarios autorizados?	X						X	
3	¿Se clasifica la información en función de su importancia?		X					X	
4	¿Se establecen copias de seguridad de la información relevante?		X					X	
5	¿Se protege la información física sensible?		X					X	
	Protección de datos y privacidad de la información personal								
1	¿Se establece el documento de seguridad de conformidad con la legislación de protección de datos personales?	X						X	
A18.2.	**Revisiones de la seguridad de la información**								
	Cumplimiento de las políticas y normas de seguridad								
1	¿Se dicta y acuerda la política del sistema de gestión de la seguridad informática - SGSI?	X						X	
OBSERVACIONES:									

15.2.2. Anexos Checklist Color Shop

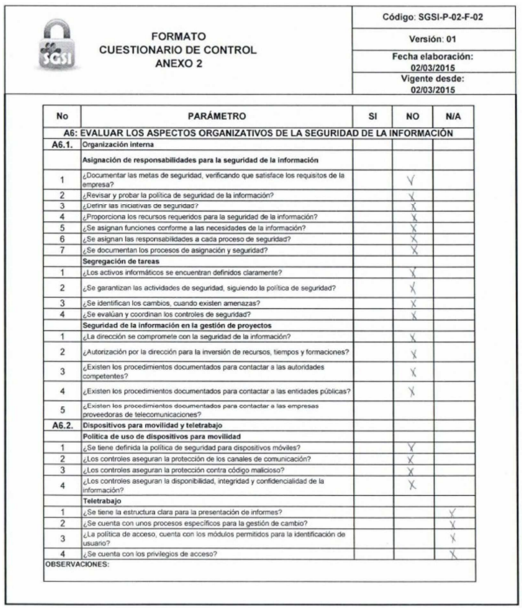
Ilustración 115 Checklist anexo 1 Color Shop



FORMATO CUESTIONARIO DE CONTROL ANEXO 1	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A5: EVALUAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN			
A5.1.	**Política de Seguridad de la Información**			
	Conjunto de políticas para la seguridad de la información			
1	¿Está definida la política de seguridad para la empresa?		√	
2	¿Se encuentran definidos los objetivos generales y el alcance de seguridad informática, como mecanismo para compartir información?		√	
3	¿Se tiene la estructura necesaria para establecer los objetivos de control, evaluando los riesgos?		√	
4	¿Se tiene la estructura necesaria para establecer la gestión de los riesgos?		√	
5	¿Se realizan capacitaciones constantes sobre las vulnerabilidades, riesgos y amenazas que tiene una organización?		√	
	Revisión de las políticas para la seguridad de la información.			
1	¿Se realizan acciones preventivas y correctivas?		√	
2	¿Se realizan revisiones periódicas de la política de seguridad?		√	
3	¿Los incidentes de seguridad se reporta?		√	
4	¿Se realizan revisiones periódicas de la política de seguridad?		√	
OBSERVACIONES:				

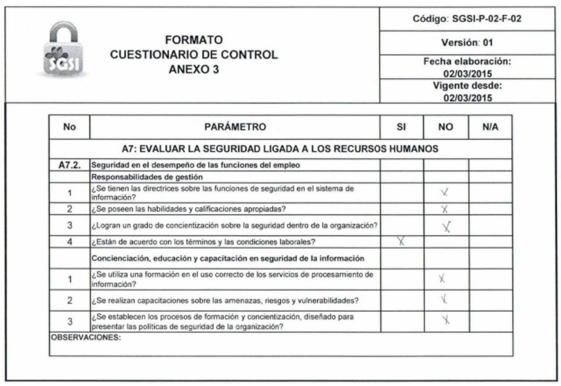
Ilustración 116 Checklist anexo 2 Color Shop



FORMATO CUESTIONARIO DE CONTROL ANEXO 2	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A6: EVALUAR LOS ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
A6.1.	**Organización interna**			
	Asignación de responsabilidades para la seguridad de la información			
1	¿Documentar las metas de seguridad, verificando que satisface los requisitos de la empresa?		√	
2	¿Revisar y probar la política de seguridad de la información?		√	
3	¿Definir las iniciativas de seguridad?		√	
4	¿Proporciona los recursos requeridos para la seguridad de la información?		√	
5	¿Se asignan funciones conforme a las necesidades de la información?		√	
6	¿Se asignan las responsabilidades a cada proceso de seguridad?		√	
7	¿Se documentan los procesos de asignación y seguridad?		√	
	Segregación de tareas			
1	¿Los activos informáticos se encuentran definidos claramente?		√	
2	¿Se garantizan las actividades de seguridad, siguiendo la política de seguridad?		√	
3	¿Se identifican los cambios, cuando existen amenazas?		√	
4	¿Se evalúan y coordinan los controles de seguridad?		√	
	Seguridad de la información en la gestión de proyectos			
1	¿La dirección se compromete con la seguridad de la información?		√	
2	¿Autorización por la dirección para la inversión de recursos, tiempos y formaciones?		√	
3	¿Existen los procedimientos documentados para contactar a las autoridades competentes?		√	
4	¿Existen los procedimientos documentados para contactar a las entidades públicas?		√	
5	¿Existen los procedimientos documentados para contactar a las empresas proveedoras de telecomunicaciones?			
A6.2.	**Dispositivos para movilidad y teletrabajo**			
	Política de uso de dispositivos para movilidad			
1	¿Se tiene definida la política de seguridad para dispositivos móviles?		√	
2	¿Los controles aseguran la protección de los canales de comunicación?		√	
3	¿Los controles aseguran la protección contra código malicioso?		√	
4	¿Los controles aseguran la disponibilidad, integridad y confidencialidad de la información?		√	
	Teletrabajo			
1	¿Se tiene la estructura clara para la presentación de informes?			√
2	¿Se cuenta con unos procesos específicos para la gestión de cambio?			√
3	¿La política de acceso, cuenta con los módulos permitidos para la identificación de usuario?			√
4	¿Se cuenta con los privilegios de acceso?			√
OBSERVACIONES:				

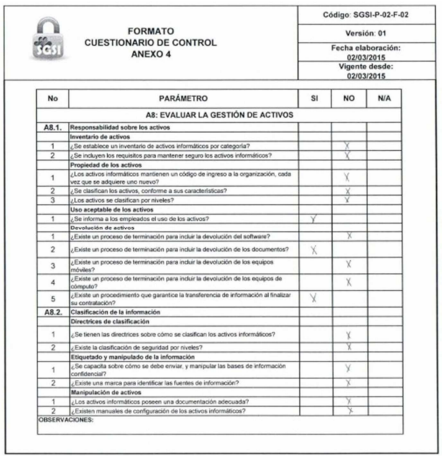
Ilustración 117 Checklist anexo 3 Color Shop



FORMATO CUESTIONARIO DE CONTROL ANEXO 3	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A7: EVALUAR LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
A7.2.	**Seguridad en el desempeño de las funciones del empleo**			
	Responsabilidades de gestión			
1	¿Se tienen las directrices sobre las funciones de seguridad en el sistema de información?		√	
2	¿Se poseen las habilidades y calificaciones apropiadas?		√	
3	¿Logran un grado de concientización sobre la seguridad dentro de la organización?		√	
4	¿Están de acuerdo con los términos y las condiciones laborales?	√		
	Concienciación, educación y capacitación en seguridad de la información			
1	¿Se utiliza una formación en el uso correcto de los servicios de procesamiento de información?		√	
2	¿Se realizan capacitaciones sobre las amenazas, riesgos y vulnerabilidades?		√	
3	¿Se establecen los procesos de formación y concientización, diseñado para presentar las políticas de seguridad de la organización?		√	
OBSERVACIONES:				

Ilustración 118 Checklist anexo 4 Color Shop



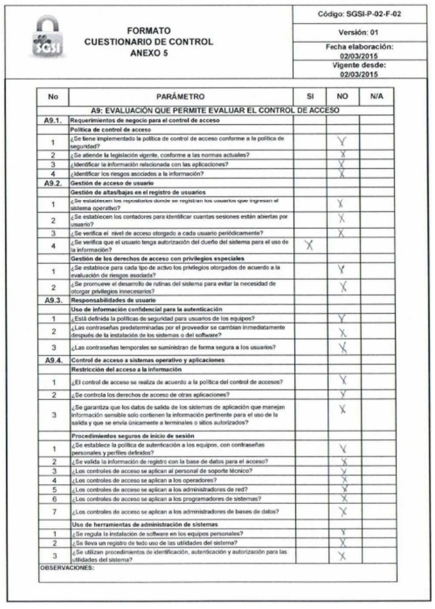
FORMATO
CUESTIONARIO DE CONTROL
ANEXO 4

Código: SGSI-P-02-F-02
Versión: 01
Fecha elaboración: 02/03/2015
Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A8: EVALUAR LA GESTIÓN DE ACTIVOS			
A8.1.	**Responsabilidad sobre los activos**			
	Inventario de activos			
1	¿Se establece un inventario de activos informáticos por categoría?		X	
2	¿Se incluyen los requisitos para mantener seguro los activos informáticos?		X	
	Propiedad de los activos			
1	¿Los activos informáticos mantienen un código de ingreso a la organización, cada vez que se adquiere uno nuevo?		X	
2	¿Se clasifican los activos, conforme a sus características?		X	
3	¿Los activos se clasifican por niveles?		X	
	Uso aceptable de los activos			
1	¿Se informa a los empleados el uso de los activos?	X		
	Devolución de activos			
1	¿Existe un proceso de terminación para incluir la devolución del software?		X	
2	¿Existe un proceso de terminación para incluir la devolución de los documentos?	X		
3	¿Existe un proceso de terminación para incluir la devolución de los equipos móviles?		X	
4	¿Existe un proceso de terminación para incluir la devolución de los equipos de cómputo?		X	
5	¿Existe un procedimiento que garantice la transferencia de información al finalizar su contratación?	X		
A8.2.	**Clasificación de la información**			
	Directrices de clasificación			
1	¿Se tienen las directrices sobre cómo se clasifican los activos informáticos?		X	
2	¿Existe la clasificación de seguridad por niveles?		X	
	Etiquetado y manipulado de la información			
1	¿Se capacita sobre cómo se debe enviar, y manipular las bases de información confidencial?		X	
2	¿Existe una marca para identificar las fuentes de información?		X	
	Manipulación de activos			
1	¿Los activos informáticos poseen una documentación adecuada?		X	
2	¿Existen manuales de configuración de los activos informáticos?		X	

OBSERVACIONES:

Ilustración 119 Checklist anexo 5 Color Shop



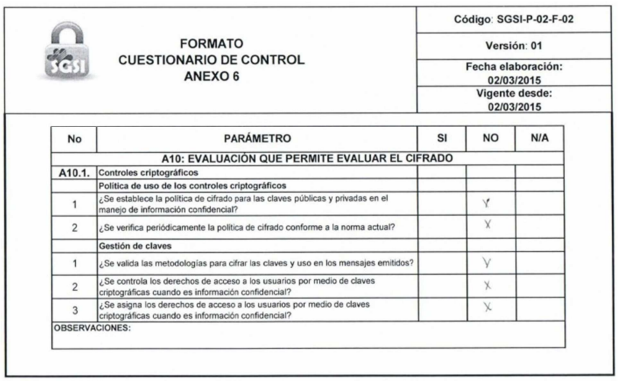
FORMATO
CUESTIONARIO DE CONTROL
ANEXO 5

Código: SGSI-P-02-F-02
Versión: 01
Fecha elaboración: 02/03/2015
Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A9: EVALUACIÓN QUE PERMITE EVALUAR EL CONTROL DE ACCESO			
A9.1.	**Requerimientos de negocio para el control de acceso**			
	Política de control de acceso			
1	¿Se tiene implementado la política de control de acceso conforme a la política de seguridad?		X	
2	¿Se atiende la legislación vigente, conforme a las normas actuales?		X	
3	¿Identificar la información relacionada con las aplicaciones?		X	
4	¿Identificar los riesgos asociados a la información?		X	
A9.2.	**Gestión de acceso de usuario**			
	Gestión de altas/bajas en el registro de usuarios			
1	¿Se establecen los repositorios donde se registran los usuarios que ingresen al sistema operativo?		X	
2	¿Se establecen los contadores para identificar cuantas sesiones están abiertas por usuario?		X	
3	¿Se verifica el nivel de acceso otorgado a cada usuario periódicamente?		X	
4	¿Se verifica que el usuario tenga autorización del dueño del sistema para el uso de la información?	X		
	Gestión de los derechos de acceso con privilegios especiales			
1	¿Se establece para cada tipo de activo los privilegios otorgados de acuerdo a la evaluación de riesgos asociada?		X	
2	¿Se promueve el desarrollo de rutinas del sistema para evitar la necesidad de otorgar privilegios innecesarios?		X	
A9.3.	**Responsabilidades de usuario**			
	Uso de información confidencial para la autenticación			
1	¿Está definida la políticas de seguridad para usuarios de los equipos?		X	
2	¿Las contraseñas predeterminadas por el proveedor se cambian inmediatamente después de la instalación de los sistemas o del software?		X	
3	¿Las contraseñas temporales se suministran de forma segura a los usuarios?		X	
A9.4.	**Control de acceso a sistemas operativo y aplicaciones**			
	Restricción del acceso a la información			
1	¿El control de acceso se realiza de acuerdo a la política del control de acceso?		X	
2	¿Se controla los derechos de acceso de otras aplicaciones?		X	
3	¿Se garantiza que los datos de salida de los sistemas de aplicación que manejan información sensible solo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados?		X	
	Procedimientos seguros de inicio de sesión			
1	¿Se establece la política de autenticación a los equipos, con contraseñas personales y perfiles definidos?		X	
2	¿Se valida la información de registro con la base de datos para el acceso?		X	
3	¿Los controles de acceso se aplican al personal de soporte técnico?		X	
4	¿Los controles de acceso se aplican a los operadores?		X	
5	¿Los controles de acceso se aplican a los administradores de red?		X	
6	¿Los controles de acceso se aplican a los programadores de sistemas?		X	
7	¿Los controles de acceso se aplican a los administradores de bases de datos?		X	
	Uso de herramientas de administración de sistemas			
1	¿Se regula la instalación de software en los equipos personales?		X	
2	¿Se lleva un registro de todo uso de las utilidades del sistema?		X	
3	¿Se utilizan procedimientos de identificación, autenticación y autorización para las utilidades del sistema?		X	

OBSERVACIONES:

Ilustración 120 Checklist anexo 6 Color Shop



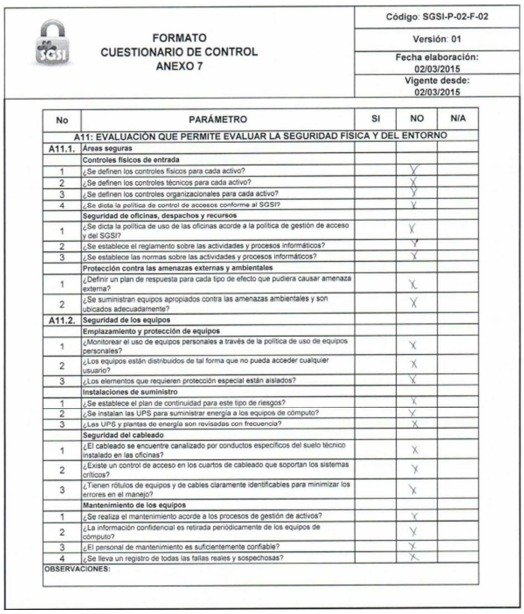
FORMATO
CUESTIONARIO DE CONTROL
ANEXO 6

Código: SGSI-P-02-F-02
Versión: 01
Fecha elaboración: 02/03/2015
Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
	A10: EVALUACIÓN QUE PERMITE EVALUAR EL CIFRADO			
A10.1.	**Controles criptográficos**			
	Política de uso de los controles criptográficos			
1	¿Se establece la política de cifrado para las claves públicas y privadas en el manejo de información confidencial?		X	
2	¿Se verifica periódicamente la política de cifrado conforme a la norma actual?		X	
	Gestión de claves			
1	¿Se valida las metodologías para cifrar las claves y uso en los mensajes emitidos?		X	
2	¿Se controla los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?		X	
3	¿Se asigna los derechos de acceso a los usuarios por medio de claves criptográficas cuando es información confidencial?		X	

OBSERVACIONES:

Ilustración 121 Checklist anexo 7 Color Shop

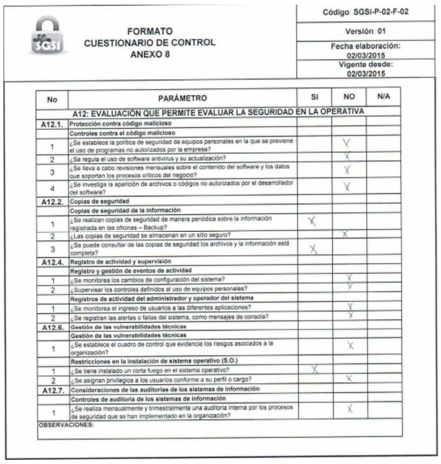


FORMATO
CUESTIONARIO DE CONTROL
ANEXO 7

Código: SGSI-P-02-F-02
Versión: 01
Fecha elaboración: 02/03/2015
Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A11: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD FISICA Y DEL ENTORNO				
A11.1.	**Áreas seguras**			
	Controles físicos de entrada			
1	¿Se definen los controles físicos para cada activo?		X	
2	¿Se definen los controles técnicos para cada activo?		X	
3	¿Se definen los controles organizacionales para cada activo?		X	
4	¿Se dicta la política de control de accesos conforme al SGSI?		X	
	Seguridad de oficinas, despachos y recursos			
1	¿Se dicta la política de uso de las oficinas acorde a la política de gestión de acceso y del SGSI?		X	
2	¿Se establece el reglamento sobre las actividades y procesos informáticos?		X	
3	¿Se establece las normas sobre las actividades y procesos informáticos?		X	
	Protección contra las amenazas externas y ambientales			
1	¿Definir un plan de respuesta para cada tipo de efecto que pudiera causar amenaza externa?		X	
2	¿Se suministran equipos apropiados contra las amenazas ambientales y son ubicados adecuadamente?		X	
A11.2.	**Seguridad de los equipos**			
	Emplazamiento y protección de equipos			
1	¿Monitorear el uso de equipos personales a través de la política de uso de equipos personales?		X	
2	¿Los equipos están distribuidos de tal forma que no pueda acceder cualquier usuario?		X	
3	¿Los elementos que requieren protección especial están aislados?		X	
	Instalaciones de suministro			
1	¿Se establece el plan de continuidad para este tipo de riesgos?		X	
2	¿Se instalan las UPS para suministrar energía a los equipos de cómputo?		X	
3	¿Las UPS y plantas de energía son revisadas con frecuencia?		X	
	Seguridad del cableado			
1	¿El cableado se encuentre canalizado por conductos específicos del suelo técnico instalado en las oficinas?		X	
2	¿Existe un control de acceso en los cuartos de cableado que soportan los sistemas críticos?		X	
3	¿Tienen rótulos de equipos y de cables claramente identificables para minimizar los errores en el manejo?		X	
	Mantenimiento de los equipos			
1	¿Se realiza el mantenimiento acorde a los procesos de gestión de activos?		X	
2	¿La información confidencial es retirada periódicamente de los equipos de cómputo?		X	
3	¿El personal de mantenimiento es suficientemente confiable?		X	
4	¿Se lleva un registro de todas las fallas reales y sospechosas?		X	
OBSERVACIONES:				

Ilustración 122 Checklist anexo 8 Color Shop

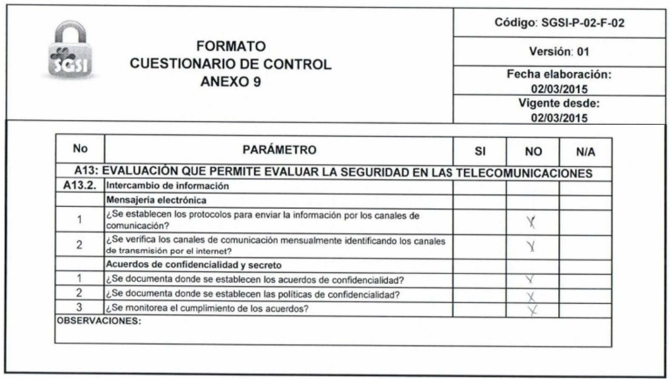


FORMATO
CUESTIONARIO DE CONTROL
ANEXO 8

Código: SGSI-P-02-F-02
Versión: 01
Fecha elaboración: 02/03/2015
Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A12: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LA OPERATIVA				
A12.1.	**Protección contra código malicioso**			
	Controles contra el código malicioso			
1	¿Se establece la política de seguridad de equipos personales en la que se previene el uso de programas no autorizados por la empresa?		X	
2	¿Se regula el uso de software antivirus y su actualización?		X	
3	¿Se lleva a cabo revisiones mensuales sobre el contenido del software y los datos que soportan los procesos críticos del negocio?		X	
4	¿Se investiga la aparición de archivos o códigos no autorizados por el desarrollador del software?		X	
A12.2.	**Copias de seguridad**			
	Copias de seguridad de la información			
1	¿Se realizan copias de seguridad de manera periódica sobre la información registrada en las oficinas – Backup?	X		
2	¿Las copias de seguridad se almacenan en un sitio seguro?		X	
3	¿Se puede consultar de las copias de seguridad los archivos y la información está completa?	X		
A12.4.	**Registro de actividad y supervisión**			
	Registro y gestión de eventos de actividad			
1	¿Se monitorea los cambios de configuración del sistema?		X	
2	¿Supervisar los controles definidos al uso de equipos personales?		X	
	Registros de actividad del administrador y operador del sistema			
1	¿Se monitorea el ingreso de usuarios a las diferentes aplicaciones?		X	
2	¿Se registran las alertas o fallas del sistema, como mensajes de consola?		X	
A12.6.	**Gestión de las vulnerabilidades técnicas**			
	Gestión de las vulnerabilidades técnicas			
1	¿Se establece el cuadro de control que evidencie los riesgos asociados a la organización?		X	
	Restricciones en la instalación de sistema operativo (S.O.)			
1	¿Se tiene instalado un corta fuego en el sistema operativo?	X		
2	¿Se asignan privilegios a los usuarios conforme a su perfil o cargo?		X	
A12.7.	**Consideraciones de las auditorías de los sistemas de información**			
	Controles de auditoría de los sistemas de información			
1	¿Se realiza mensualmente y trimestralmente una auditoria interna por los procesos de seguridad que se han implementado en la organización?		X	
OBSERVACIONES:				

Ilustración 123 Checklist anexo 9 Color Shop

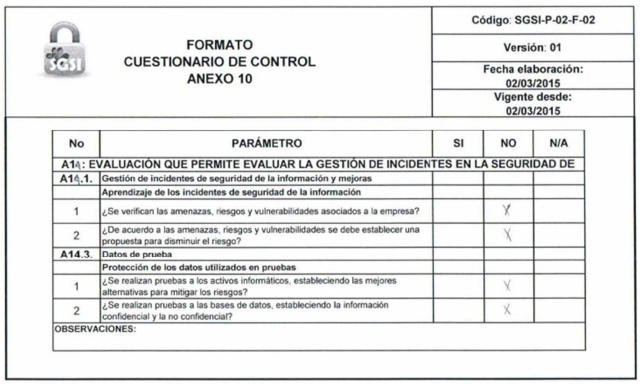


FORMATO
CUESTIONARIO DE CONTROL
ANEXO 9

Código: SGSI-P-02-F-02
Versión: 01
Fecha elaboración: 02/03/2015
Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A13: EVALUACIÓN QUE PERMITE EVALUAR LA SEGURIDAD EN LAS TELECOMUNICACIONES				
A13.2.	**Intercambio de información**			
	Mensajería electrónica			
1	¿Se establecen los protocolos para enviar la información por los canales de comunicación?		X	
2	¿Se verifica los canales de comunicación mensualmente identificando los canales de transmisión por el internet?		X	
	Acuerdos de confidencialidad y secreto			
1	¿Se documenta donde se establecen los acuerdos de confidencialidad?		X	
2	¿Se documenta donde se establecen las políticas de confidencialidad?		X	
3	¿Se monitorea el cumplimiento de los acuerdos?		X	
OBSERVACIONES:				

Ilustración 124 Checklist anexo 10 Color Shop



FORMATO CUESTIONARIO DE CONTROL ANEXO 10	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A14: EVALUACIÓN QUE PERMITE EVALUAR LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE				
A14.1.	Gestión de incidentes de seguridad de la información y mejoras			
	Aprendizaje de los incidentes de seguridad de la información			
1	¿Se verifican las amenazas, riesgos y vulnerabilidades asociados a la empresa?		X	
2	¿De acuerdo a las amenazas, riesgos y vulnerabilidades se debe establecer una propuesta para disminuir el riesgo?		X	
A14.3.	Datos de prueba			
	Protección de los datos utilizados en pruebas			
1	¿Se realizan pruebas a los activos informáticos, estableciendo las mejores alternativas para mitigar los riesgos?		X	
2	¿Se realizan pruebas a las bases de datos, estableciendo la información confidencial y la no confidencial?		X	
OBSERVACIONES:				

Ilustración 125 Checklist anexo 11 Color Shop

FORMATO CUESTIONARIO DE CONTROL ANEXO 11	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

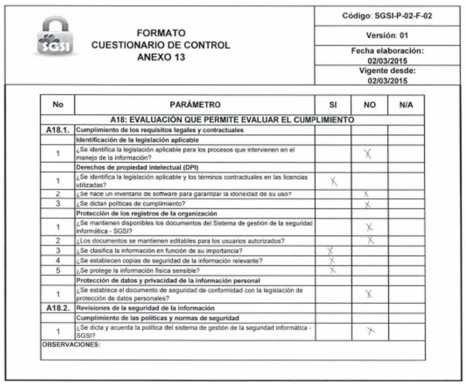
No	PARÁMETRO	SI	NO	N/A
A16: EVALUACIÓN QUE PERMITE EVALUAR LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO				
A16.1.	Gestión de incidentes de seguridad de la información y mejoras			
	Aprendizaje de los incidentes de seguridad de la información			
	¿Se establecen procesos de resolución de incidentes de seguridad de la información?		X	
	¿Se evalúan los incidentes de seguridad?		X	
OBSERVACIONES:				

Ilustración 126 Checklist anexo 12 Color Shop

FORMATO CUESTIONARIO DE CONTROL ANEXO 12	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A17: EVALUACIÓN QUE PERMITE EVALUAR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN				
A17.1.	Aspectos de la seguridad de la información en la gestión de la continuidad del negocio			
	Planificación de la continuidad de la seguridad de la información			
1	¿Se define el proceso de gestión de continuidad del negocio?		X	
2	¿Se define las directrices de continuidad del negocio de conformidad con la política de seguridad de la información?		X	
3	¿Se garantiza la seguridad del personal, la protección de los servicios y procesos de información?		X	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información			
1	¿Se define los planes de continuidad del negocio de acuerdo al orden de prioridades?		X	
2	¿Se implementa los planes de continuidad del negocio de acuerdo al orden de prioridades?		X	
OBSERVACIONES:				

Ilustración 127 Checklist anexo 13 Color Shop



FORMATO CUESTIONARIO DE CONTROL ANEXO 13	Código: SGSI-P-02-F-02
	Versión: 01
	Fecha elaboración: 02/03/2015
	Vigente desde: 02/03/2015

No	PARÁMETRO	SI	NO	N/A
A18: EVALUACIÓN QUE PERMITE EVALUAR EL CUMPLIMIENTO				
A18.1.	Cumplimiento de los requisitos legales y contractuales			
	Identificación de la legislación aplicable			
1	¿Se identifica la legislación aplicable para los procesos que intervienen en el manejo de la información?		X	
	Derechos de propiedad intelectual (DPI)			
1	¿Se identifica la legislación aplicable y los términos contractuales en las licencias utilizadas?	X		
2	¿Se hace un inventario de software para garantizar la idoneidad de su uso?		X	
3	¿Se dictan políticas de cumplimiento?		X	
	Protección de los registros de la organización			
1	¿Se mantienen disponibles los documentos del Sistema de gestión de la seguridad informática - SGSI?		X	
2	¿Los documentos se mantienen editables para los usuarios autorizados?		X	
3	¿Se clasifica la información en función de su importancia?	X		
4	¿Se establecen copias de seguridad de la información relevante?	X		
5	¿Se protege la información física sensible?	X		
	Protección de datos y privacidad de la información personal			
1	¿Se establece el documento de seguridad de conformidad con la legislación de protección de datos personales?		X	
A18.2.	Revisiones de la seguridad de la información			
	Cumplimiento de las políticas y normas de seguridad			
1	¿Se dicta y acuerda la política del sistema de gestión de la seguridad informática - SGSI?		X	
OBSERVACIONES:				