UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

Tema: "Auditoria de seguridad informática en la florícola Galápagos Flores S.A"

Trabajo de titulación previa la obtención del
título de Ingeniera en Ciencias de la Computación

AUTORA: Quishpe Pillajo Heidy Selena

TUTOR: Msc. Marco Antonio Yandún Velasteguí

Tulcán, 2022

CERTIFICADO JURADO EXAMINADOR

Certifico que la estudiante Quishpe Pillajo Heidy Selena con el número de cédula 1755068929 ha elaborado el trabajo de titulación: "Auditoria de seguridad informática en la florícola Galápagos Flores S.A."

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva

f.....

Yandún Velasteguí Marco Antonio, MSc.

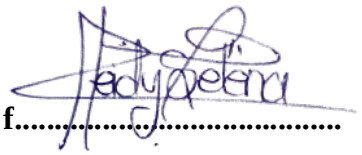
TUTOR

Tulcán, septiembre de 2022

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de **Ingeniera** en la Carrera de computación de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Quishpe Pillajo Heidy Selena con cédula de identidad número 1755068929 declaro: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.



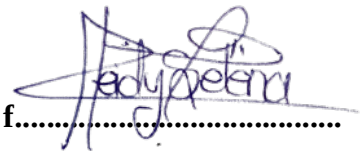
f.....

Quishpe Pillajo Heidy Selena
AUTORA

Tulcán, septiembre de 2022

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Yo, Quishpe Pillajo Heidy Selena declaro ser autor/a de los criterios emitidos en el trabajo de investigación: “Auditoria de seguridad informática en la florícola Galápagos Flores S.A.” y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.



f.....
Quishpe Pillajo Heidy Selena
AUTORA

Tulcán, septiembre de 2022

AGRADECIMIENTO

A Dios, por permitirme cumplir uno de mis principales objetivos de vida.

A mis padres y hermano, por apoyarme siempre en cada decisión que he tomado y se han mantenido firmes conmigo.

A la Universidad Politécnica Estatal del Carchi por darme la oportunidad formarme como profesional.

A mis docentes, en especial al MSc. Marco Yandún, tutor del proyecto, por el apoyo y guía para el desarrollo de este proyecto de titulación.

A la florícola Galápagos Flores S.A, de manera especial al Ing. José Sosa, por su apertura y colaboración en la realización del presente proyecto de titulación.

Heidy Selena Quishpe Pillajo

DEDICATORIA

A mis padres Walter y Silvana ya que esto además de ser un logró mío es suyo, gracias por su esfuerzo y apoyo brindado para poder convertirme en una profesional. Sus valores inculcados con amor y paciencia son los que me han llevado a terminar este proceso educativo.

A mi hermano Jhordyn luz de mi vida, mi mayor inspiración, la persona por la que jamás me he rendido sin antes dar pelea, todo esto siempre será por ti.

Heidy Selena Quishpe Pillajo

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

RESUMEN

El presente proyecto evaluó la situación de los controles de seguridad que mantienen actualmente la florícola Galápagos Flores S.A, mediante la aplicación de una auditoria informática basada en la norma ISO 27001:2013 y la Metodología OSSTMM (Manual de la Metodología Abierta de Testeo de Seguridad) que fue desarrollada en el Área de Sistemas. De acuerdo con la investigación inicial realizada se consideró la información como el activo más importante, en donde se pudo evidenciar que los controles de acceso a la misma son débiles y se encuentran al alcance de todos generando vulnerabilidades en los procesos de manera total o parcial. El objetivo de la investigación fue realizar la auditoria de seguridad informática, además, desarrollar y socializar el informe final con los hallazgos y el plan de mitigación de riesgos. Para llevar a cabo la auditoria se tomó en cuenta un enfoque cualitativo y cuantitativo, la cual permitió el análisis de la documentación solicitada al área auditada, la verificación de cumplimiento de controles ISO 27001:2013 y la fundamentación teórica en la metodología. Los instrumentos utilizados para la investigación fueron la encuesta, que se aplicó al personal operativo y la entrevista que fue realizada al encargado del área de sistemas en donde se obtuvo información fundamental para el desarrollo de la investigación. Finalmente, se emitió un documento de resultados de auditoria con el nivel de cumplimiento actual de los controles correspondientes, de un total de 106 controles aplicables a la florícola se obtuvo los siguientes resultados: 48 conformidades, 51 no conformidades y 8 observaciones. Se precedió a realizar un comparativo de seguridad informática utilizando la Metodología abierta OSSTMM obteniendo un nivel de seguridad de 80,81 RAVS, es decir, la florícola mantiene controles de seguridad, sin embargo, no están siendo efectivos.

Palabras Claves: auditoria informática, mitigación de riesgos, norma ISO 27001:2013, Metodología OSSTM

ABSTRACT

The present study assessed the security controls currently run in the Galápagos Flores S.A flower farm through the application of a computer audit based on the ISO 27001: 2013 standard and the OSSTMM Methodology (Open Security Testing Methodology Manual) which was developed in the Systems Area. According to the data obtained, the same was considered as the most important asset. On the other hand, the access controls to information are weak and are available to everyone which generates vulnerabilities in the processes in a total or partial way. The goal of the investigation was to conduct the computer security audit as well as to develop and socialize the final report with the findings and the risk mitigation plan. To run the audit, a qualitative and quantitative approach was used, which analyzed the documentation requested from the audited area, the verification of compliance with ISO 27001:2013 controls and the theoretical foundation in the methodology. The tools used in the research was a survey which was addressed to personnel and an interview applied to the in charge of the system management area. Finally, it was handled a document with the audit results which showed the accomplishment of the current controls. From a total of 106 controls applicable to the flower farm, here the results: 48 conformities and 8 observations. Then, it was done a safety comparison by using the opened methodology OSSTMM so that, it was got 80,81 RAVS of safety. In other words, the flower farm maintains safety controls, but they are not being efficient.

Keywords: computer audit, risk mitigation, ISO 27001: 2013 standard, OSSTM Methodology

INTRODUCCIÓN

La florícola Galápagos Flores S. A, objeto de estudia es una empresa orgullosamente ecuatoriana dedicada al cultivo y exportación de flores cumpliendo toda la normativa legal con un liderazgo comprometido y sólido para ofrecer un trabajo digno, inclusivo, seguro, gestionando la protección de la salud y confort de sus colaboradores, tanto empleados como trabajadores. Se encuentra ubicada en el cantón Pedro Moncayo, Panamericana sur 28B.

En su estructura funcional cuentan con el Área de Sistemas cuyas funciones están relacionadas con el soporte técnico, administración de red y seguridad de la información, además de contribuir con tecnología al cumplimiento de los procesos funcionales. Sin embargo, el activo más importante con el que cuenta la florícola, que es la información, no cuenta con los controles de seguridad necesarios quedando vulnerable ante un daño parcial o total.

La presente investigación tuvo como finalidad realizar una auditoría de seguridad informática basándose en la norma ISO 27001:2013, que pretende verificar los controles de seguridad implementados dentro de la institución y determinar los problemas de seguridad de la información que podrían tener un impacto negativo en los procesos. La metodología con la que se desarrolló la auditoria fue con el ciclo de Deming el cual consta de cuatro etapas, siendo la etapa “actuar” en donde se expuso los resultados encontrados mediante el informe de auditoría y a su vez se emitió las estrategias de mitigación para cada riesgo encontrado. Al acoger la propuesta del plan de mitigación de riesgos, se pretende reducir los controles no funcionales que generan un impacto negativo en la seguridad informática.

El plan de investigación se desarrolló en cinco capítulos que se describen a continuación:

En el capítulo uno se muestra la problemática de estudio, justificación de la investigación, objetivos establecidos y preguntas de investigación. El capítulo dos trata acerca de la fundamentación teórica, donde se describen los antecedentes de investigaciones similares, además, el marco teórico define la terminología con la finalidad de sustentar el trabajo de investigación. El tercer capítulo describe el enfoque metodológico utilizado, los tipos de investigación, idea a defender, operacionalización de variables de estudio y métodos necesarios para la recolección de información. El capítulo cuatro describe los resultados de la información y discusión en donde se da a conocer los datos informativos

de la florícola, el proceso de auditoria informática en sus etapas, informe de auditoría y plan de mitigación. El capítulo cinco expone las conclusiones y recomendaciones en las que se ha llegado con el proceso de investigación. El capítulo sexto y séptimo muestran las referencias bibliográficas y anexos respectivamente.

I.PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

La transformación digital en la empresa implica una serie de desafíos: a pesar de algunas ventajas, existen otras que pueden conllevar riesgos para la seguridad. Según un análisis realizado ESET (2019) menciona que los datos suministrados por empresas de toda Latinoamérica, se logró observar que el 61% de las mismas sufrió por lo menos un incidente de seguridad, siendo la infección con códigos maliciosos el más recurrente, es decir 2 de cada 5 empresas sufrieron una infección de malware, incluyendo ransomware, en el año 2018. Además, la mitad de estos eventos está relacionado con ransomware, lo que significa que al menos una décima parte de la información de la empresa ha sido secuestrada entre las empresas encuestadas en toda América Latina.

Según Monteros (2017) afirma que, a escala mundial, la auditoría informática se ha convertido en un pilar fundamental en donde las organizaciones, los sistemas y las estructuras físicas deben cumplir un control de calidad, esto debido a que las computadoras son el objeto del procesamiento de datos propenso a la delincuencia, el terrorismo o el espionaje. Mediante la auditoría informática se puede ver y evaluar los controles, sistemas, procedimientos informáticos, equipos de cómputo, su uso, eficiencia, seguridad y protección de la organización involucrada en el proceso. Esto con el fin de utilizar de manera eficiente y segura para una adecuada toma de decisiones.

Así mismo ESET (2019) afirma que, durante 2017 esta actividad amenazante cuando el número de detecciones y la tasa de producción de nuevas variantes se ha incrementado exponencialmente. Ese año, un tercio de las actividades de investigación se concentró en países / regiones de América Latina. Donde Perú (25%) fue el país más afectado de la región.

Actualmente en Ecuador la eficacia de las auditorias informáticas para un buen desempeño de los sistemas tanto en organizaciones públicas o privadas en gran parte no se realiza, esto debido a dos factores; en primer lugar el alto costo que resulta llevar a cabo este proceso y el segundo y el más importante es el desconocimiento, ya que se piensa que una auditoria es un método para evaluar al personal y conllevara a un removimiento de cargo, lo cual no es de agrado para el personal de cualquier organización (Olmedo y León, 2018).

Cuando una empresa que presta servicios se ve afectada por el robo de información, afectará directamente la confianza de sus clientes. Según los resultados de la encuesta recabados en la investigación de ESET en el año 2019, en el caso de robo de información, el 62,9% de los usuarios dejarán de utilizar el servicio, es decir, por una protección insuficiente de su información, la empresa perderá seis de cada diez clientes.

El Ingeniero José Sosa menciona que considerando que el cantón Pedro Moncayo es una zona de crecimiento florícola razón por la cual sería recomendable hacer Auditorias informáticas a organizaciones públicas y privadas, esto con el fin de mejorar en desenvolvimiento de estas, sin embargo, esta práctica no se realiza puesto que es un ámbito desconocido.

En la florícola Galápagos Flores S.A es una empresa privada la cual lleva 30 años de experiencia produciendo más de 70 variedades de rosas, busca conseguir logros de servicio en todos los aspectos social, cultural y otros, buscando siempre el propósito de servir a la sociedad y brindar calidad en el producto final (comunicación personal, 8 de enero de 2021).

Galápagos Flores S.A está al tanto que los procesos que lleva a cabo los diferentes departamentos de los cuales se componen son de vital importancia para la florícola debido a que la producción realizada en la misma es 90% de exportación, por ende, realizar un examen crítico y detección de errores con el propósito de evaluar la eficiencia y eficacia tanto del manejo de la información como del equipo informático es fundamental.

De acuerdo con una investigación de campo realizada en la florícola se puede determinar que, considerando la información como el activo más importante de cualquier empresa, la florícola en cuestión no cuenta con restricción de acceso a la información más importante, es decir, archivos contables, archivos de ventas, registros de producción, registros de embarques, etc. Puesto que, dicha información se encuentra almacenada en carpetas compartidas en donde cualquier usuario al conectarse a la red, puede tener acceso a esta información. Además, la red que actualmente está estructurada en la florícola no cuenta con un firewall que proteja ante cualquier ataque, lo que podría conllevar a un robo de información o un ciber ataque.

De igual manera, los equipos informáticos no se encuentran restringidos solo para el personal autorizado ya que estos están junto a la Gerencia Financiera en donde cualquier usuario podría ingresar y manipular ocasionando grabes daños en la red.

1.2 FORMULACIÓN DEL PROBLEMA

El desconocimiento de los beneficios del desarrollo de una auditoría de seguridad informática genera un limitado número de controles de seguridad, ocasionando incremento en los riesgos asociados al manejo de la información en la florícola Galápagos Flores S.A en el periodo 2021-2022

1.3 JUSTIFICACIÓN

La información es parte del activo más importante de cualquier empresa, al mismo tiempo es uno de los recursos más vulnerables y es esencial proteger la información de amenazas internas y externas. Actualmente, las empresas requieren que la información que procesan esté siempre disponible sin cambiar sus datos y asegurando su confiabilidad. Mediante el análisis de la seguridad de la información, Galápagos Flores S.A podrá conocer y aplicar las medidas de control de seguridad que gestiona dentro de la empresa para asegurar que la información se utilice correctamente y que solo el personal autorizado pueda acceder a ella.

Por ello, la auditoría informática es de gran interés, ya que permitirá realizar un informe detallando de los puntos críticos de la florícola en el ámbito tecnológico y que permita tomar acciones correctivas para asegurar la confiabilidad, confidencialidad y disponibilidad de la información en los departamentos auditados.

En la florícola Galápagos Flores S.A del cantón Pedro Moncayo es de interés ya que se puede controlar la manipulación de la tecnología de información que es de importancia para la organización convirtiéndose en un factor determinante por el cual pueden ocasionar problemas debido al filtro de información confidencial. A demás, existe factibilidad para realizar la investigación ya que se cuenta con el consentimiento de la florícola para acceder a la información que se necesite para la investigación. Finalmente, el beneficiario es principalmente la entidad privada porque puede obtener Políticas claras de control de la tecnología de la información y buenas prácticas.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

- Realizar una auditoría de seguridad informática mediante el ciclo de deming para los riesgos asociados al manejo de la información en la florícola Galápagos Flores S.A

1.4.2. Objetivos Específicos

- Fundamentar bibliográficamente la investigación de la seguridad informática y auditoria informática.
- Aplicar el ciclo de deming en los procesos críticos relacionados en la seguridad de la información.
- Generar el informe y plan de mitigación de riesgos de la auditoria de seguridad de la información en la florícola Galápagos Flores S.A

1.4.3. Preguntas de Investigación

- ¿Como se realizan los procesos en la florícola?
- ¿Cómo es la clasificación de la información?
- ¿Cuáles son los estándares de seguridad de información en las florícolas?
- ¿Qué acciones mantiene la florícola para la seguridad informática?
- ¿Cuáles son las normas y estándares que aplican las florícolas?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

Gavino (2018) en su investigación realizada previo a la obtención del título de Ingeniero Informático de la Universidad Nacional José Faustino Sánchez Carrión denominado, "AUDITORIA EN SEGURIDAD INFORMÁTICA Y GESTION DE RIESGO EN EL HOSPITAL REGIONAL DE HUACHO, 2018" en donde el principal objetivo fue realizar el análisis de auditoría de seguridad de informática para determinar su relación con la gestión de riesgos en el Hospital Provincial de Huacho, 2018. El autor pudo determinar la vulnerabilidad que tiene el personal en relación con las contraseñas y backups que maneja el Hospital Regional de Huacacho. Llegando a la conclusión de que dicha institución a pesar de contar con administradores a cargo del sistema informático, no cuentan con protocolos de seguridad para mantener a salvo la información que maneja el hospital.

En el año 2017 el Ing. Becerra en su investigación realizada previo a la obtención del título de Magister en Informática Empresarial de la UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES "UNIANDES", denominado "AUDITORÍA INFORMÁTICA BASADA EN NORMA ISO 27004 PARA EL CONTROL DEL PARQUE TECNOLÓGICO DE UNIANDES PUYO." Teniendo como objetivo general realizar una Auditoria informática basada en norma ISO 27004 para el control del parque tecnológico de Unidades Puyo. En donde el autor determina el funcionamiento óptimo de los sistemas de información y comunicación, y si éstos contribuyen a la seguridad de la información generada en las distintas áreas, así como su estado y características, entonces también existirán protocolos de operación que identifiquen problemas y brinden soluciones a corto plazo. No afecta la productividad de la empresa. Llegando a la conclusión que la Norma ISO 27004 permitió verificar el cumplimiento de las medidas de seguridad en los sistemas informáticos de Uniandes Puyo.

Bracho y Cuzme (2018) en su investigación previo al título de Ingenieros en Sistemas en la Universidad Técnica del Norte denominada "Auditoría de seguridad informática siguiendo la metodología OSSTMMv3". Teniendo como objetivo auditar el Gobierno Autónomo Descentralizado del Cantón Mira utilizando la metodología abierta OSSTMMM para medir la seguridad del mismo. Los resultados obtenidos le permitieron comprender los controles deficientes que el Gobierno Autónomo Descentralizado del Cantón Mira presentaba siendo un punto importante para controlar las debilidades.

2.2 MARCO TEÓRICO

2.2.1 Auditoria

La competitividad de las empresas globales, la gestión y el control de empresas actividades económicas y financieras de cualquier institución (ya sea una institución pública o una institución privada); desarrollado en base a auditorías y evaluaciones actividades financieras, económicas y administrativas de la institución generalmente realizados por expertos externos (Villardefrancos Alvarez & Rivera, 2006).

La auditoría es el proceso de verificar o confirmar el cumplimiento de las actividades de acuerdo con los planes y las pautas prescritas. Es un proceso independiente, documentado y sistemático que permite obtener evidencia de auditoría y realizar evaluaciones objetivas para determinar en qué medida se han logrado los objetivos. La auditoría tiene la finalidad de diagnosticar e identificar que actividades cumplen con las políticas u objetivas establecidos y cuales son susceptibles a mejoras.

2.2.2 Auditoria en TIC's

La auditoría de TIC es un conjunto de valoraciones y valoraciones. Control total o parcial de sistemas informáticos, telecomunicaciones, redes o equipo para proteger actividades y recursos, verifica que las actividades son efectivas y cumplen con las regulaciones informáticas y estudios generales de cada empresa o institución para lograr la eficiencia requerido por la organización. (Cuellar Triana et al., 2015)

Es decir, la función de la auditoria en TIC´S es evitar desvíos, modificación o manipulación de la información, analizar el control de las funciones informáticas, analizar la eficiencia de los sistemas informáticos, verificar el cumplimiento de la normativa general, revisar materiales, gestión de recursos humanos e informáticos, niveles de seguridad, etc.

2.2.3 Auditoria Informática

Para entender de mejor manera el concepto de auditoria informática, se procederá a desglosar de la siguiente manera:

- **Auditoria:** Verificar información financiera, operativa y administrativa. Las declaraciones son confiables, verdaderas y oportunas, revisan hechos, fenómenos y operar según lo planeado a través de políticas. Estándares establecidos y cumplir con

las normas financieras, legales y provisiones generales. (Gonzales, 2018)

- **Informática:** Se deriva del vocablo francés automatique d'informations (información automática) que es la ciencia del uso de tecnología, procesos y máquinas (computadoras) para apoyar la búsqueda automática de información. Y mejorar su memoria, capacidad de pensamiento y comunicación. (Gonzales, 2018)

Según lo antes mencionado por el autor, podemos definir a la auditoria informática como el proceso de recopilación, agrupación y evaluación de evidencia para determinar si el sistema de información protege los activos de la entidad, además que mantenga la integridad de los datos y ejecute de manera efectiva. Es decir, organiza y utiliza eficazmente los recursos.

2.2.3.1. Procesos de la Auditoria Informática

Cortes Robles (2017) menciona que el objetivo del proceso de auditoría informática es mantener los activos, para asegurar la integridad de los datos, la realización de los objetivos de gestión y el uso eficaz de los recursos, para lo cual se requiere la recolección y evaluación de evidencias.

Estos procesos deben seguir la siguiente secuencia:

Planificación de la Auditoria Informática: Esto comienza en la etapa de planificación con la participación de las partes interesadas. El departamento bajo revisión para determinar los recursos necesarios que se permitirán el trabajo a realizar, estableciendo metas, tales como:

- Evaluación de los sistemas y procedimientos
- Evaluación de los equipos de cómputo
- Evaluación del proceso de Datos

Adquirir un conocimiento inicial de la entidad establecerá metas, revisión del trabajo, personas involucradas en el proyecto, presupuesto financiero, y la fecha y el método del informe de actividad.

Ejecución de la Auditoria Informática. Consiste en recopilación de información y elementos suficientes. Confirme los comentarios, conclusiones y recomendaciones sobre TI mediante los siguientes métodos, formas de utilizar tecnología y herramientas:

- Entrevistas
- Encuestas
- Cuestionarios
- Análisis de la Información Documentada
- Revisión y Análisis de Estándares

Finalización de la Auditoria Informática. Los resultados de la auditoría de TI se reflejan en el informe de conclusión, debe ser escrito y entregado a la autoridad competente de la organización. Evaluación para que antes de que se publique el informe final exista un borrador para descubrir fallas en la evaluación de auditoría.

2.2.4 Seguridad Informática

La información es el activo básico del progreso actual, para mantener el mercado de cualquier organización, así que indiscutiblemente uno de los objetivos prioritarios de cualquier empresa es asegurar la información y el sistema que procesa la información.
La seguridad informática se refiere a la protección de la infraestructura. Pueden usarse para lograr su propósito, es decir, no tienen daño o cambio por factores o entornos externos es una definición útil. Comprender el significado de los conceptos de seguridad informática como peligro o daño a todo aquello que pueda afectar su funcionamiento directo o los resultados obtenidos de ella. (Romero et al., 2018)

2.2.4.1 Seguridad Física. La seguridad física se trata de evitar el acceso de personas no autorizadas, porque si alguien puede entrar en una sala de ordenadores y sentarse frente a un equipo y empezar a trabajar sin decirle nada, el problema está en el control de acceso, permitiendo que alguien robe o destruya datos del equipo. (Carrillo, 2018)

2.2.4.2 Seguridad Lógica. Hace referencia a la aplicación de mecanismos y barreras para mantener la protección e integridad de la información en un sistema informático, respaldada por la seguridad física. La seguridad lógica se puede proteger con técnicas de seguridad que las organizaciones deben tener en cuenta. (Carrillo, 2018)
Por ejemplo:

- Restringir el acceso a los programas y archivos.
- Hay que asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

- La información transmitida sea recibida sólo por el destinatario al cual ha sido enviada.
- Que la información recibida sea la misma que ha sido transmitida.

2.2.5 Estándares

Los estándares son especificaciones sobre cómo se deben realizar tareas o funciones específicas y se basan en acuerdos entre una o más entidades o grupos específicos de personas, en este caso se mencionará al estándar ISO 27001:2013 y la Metodología Abierta de Testeo de Seguridad (OSSTMM, Open Source Security Testing Methodology Manual)

2.2.5.1 ISO 27001:2013.

La norma ISO 27001 que sus siglas significan Tecnhnology Security Techniques es el desarrollo del estándar de buenas prácticas ISO creado en 1995, para la cual conlleva un proceso de certificable llamado estándar 27001. Es decir, este tipo de certificación facilitará a la Seguridad Informática al momento de establecer, implantar, operar, supervisar, manejar, mejorar un SGSI que en siglas significa Sistema de Gestión de la Seguridad de la Información. (Organización Internacional de Normalización [ISO], 2013)

Funcionamiento de la Norma ISO 27001. Es un estándar de seguridad de la información para salvaguardar los datos que se encuentran en la organización. Para ello se implementó el SGI (Sistemas de Gestión Integrado) con el estándar 27001 para la protección de la información con la finalidad de brindar confidencialidad, disponibilidad e integridad de los datos para su correcto uso. (ISO, 2015)

Confidencialidad de datos. El usuario de la empresa garantiza la confidencialidad al momento de ingresar los datos, al no revelar esta información a personas ajenas a la empresa, de esta forma encontrará la manera de llegar a donde las personas pueden acceder a los datos es el administrador o encargado del sistema.

Disponibilidad de datos. El acceder a la información de la empresa en horarios no establecidos con el fin de alterar, actualizar o respaldar datos de suma importancia y no tener pérdidas financieras

Integridad de datos. Hace énfasis a que los datos no pueden ser alterados ni manipulados por ningún tipo de personal, solo por la alta gerencia o a su vez administradores del sistema. Para lograr este fin es necesario tener un propio tipo de seguridad que ayude al correcto manejo de los datos para beneficio propio de la empresa.

Estructura de la norma ISO 27001:2013

1. Objeto y campo de aplicación: Comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar.
2. Referencias Normativas: Revisión de ciertos documentos indispensables para la aplicación de ISO 27001:2013.
3. Términos y Definiciones: Describe la terminología aplicable a este estándar.
4. Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.
5. Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.
6. Planificación: En esta sección se pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.
7. Soporte: Recalca el funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada

pertinente en cada caso.

8. Operación: Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.
9. Evaluación del Desempeño: Se establece la necesidad y forma en que se establece el seguimiento, la medición, el análisis, la evaluación, la evaluación interna y la revisión de la gestión de un sistema de gestión de la seguridad de la información para garantizar que el sistema funcione según lo previsto.
10. Mejora: Se encuentran las obligaciones que tendrá una organización cuando encuentre una *no conformidad* y la importancia de mejorar continuamente la conveniencia.

2.2.5.2 Metodología OSSTMM (MANUAL DE LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD).

Es una técnica hecha por INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM), proporciona un medio para realizar una prueba o evaluación de seguridad integral, con un enfoque abierto. Esta metodología se puede aplicar junto con normas y reglamentos reconocidos global o localmente y la versión 3.0 está en vigor. Esta metodología busca cuantificar la seguridad mediante métricas cuantitativas, para esto se divide los aspectos a auditar en canales los mismo que se agrupan en 3 clases. (Herzong,2019)

Tabla 1. Clasificación de los canales

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humano	Comprende el elemento humano de la comunicación

	Físico	Comprende los elementos tangibles, no electrónicos.
Seguridad de espectro (SPECSEC)	Inalámbrico	Abarca las comunicaciones mediante ondas electromagnéticas
Seguridad de comunicaciones (COMSEC)	Telecomunicaciones	Abarca las redes de telecomunicaciones sobre líneas telefónicas
	Redes de datos	Comprende los sistemas electrónicos y cableado que constituyen las redes de datos.

Para evaluar cada canal se cuenta con criterios separados en 3 grupos: Operaciones, Controles y limitaciones. En donde cada grupo forma parte del funcionamiento y seguridad de un sistema o infraestructura al igual que las falencias.

Tabla 2. Mapeo de los criterios de Operaciones y Control con los de Limitaciones

Categoría		**Seguridad Operacional**	**Limitaciones**
Operaciones		Visibilidad	Exposición
		Acceso	Vulnerabilidad
		Confianza	
Controles	Clase A	Autentificación Indemnización Resistencia Subyugación Continuidad	Debilidad
	Clase B	No repudio Confidencialidad Privacidad	Preocupación

Integridad Alarma
Anomalía

Los criterios mostrados anteriormente en la "Tabla 2" nos permiten obtener los RAV (Risk Assesemet Value, Valor de Evaluación de Riesgos), es decir, es una escala de medida de un posible ataque el cual es calculado como un balance cuantitativo entre las operaciones, controles y limitaciones. El valor del RAV debe ser cercano al 100%, un valor menor muestra las debilidades que existen en la seguridad, mientras que un valor mayor indica que existen más controles de seguridad de los necesarios.

2.2.5.3 ISO 9001:2015

ISO 9001 es una norma internacional adoptada por empresas de todo tipo y tamaño en todo el mundo. Esta norma define los requisitos para la implementación de un sistema de gestión de la calidad e incluye las mejores prácticas para el uso con fines internos, de certificación y contractuales.

Además, es compatible con otros sistemas de gestión, como el sistema de gestión ambiental definido por la norma ISO 14001. La importancia de la aplicación de la norma ISO 9001:2015 se refleja principalmente en tres puntos: confianza del cliente y diferenciación de marca, mayor estabilidad en el desarrollo y fomento de la participación y gestión de la empresa o de los empleados. organizar. Si se implementan y gestionan correctamente, los sistemas de gestión de la calidad pueden ayudar a las organizaciones a mejorar la satisfacción del cliente mediante el establecimiento de objetivos que tengan en cuenta sus necesidades y expectativas, y las organizaciones dirigen sus esfuerzos para ofrecer productos o servicios que cumplan con los requisitos reglamentarios aplicables y cumplan con los requisitos. demandas y requerimientos que los clientes puedan tener o necesitar en el futuro. (Medina, F. L. C., Díaz, A. D. P. L., & Cardenas, C. R.,2017).

La gestión de calidad dentro de una empresa nos permite reducir la improvisación, debido a que la Norma permite llevar una trazabilidad de los procesos, de tal manera que se puede identificar en cualquier momento como actuar en situaciones de funcionamiento normales, óptimas y adversas. Cabe recalcar que, la gestión de calidad brinda una

oportunidad clave y no solo para la planificación, sino también para la determinación de mecanismos para el seguimiento, control y la mejora continua de cada proceso.

Dentro de la ISO 9001:2015, se presentan normas las cuales establecen las directrices para la realización de auditorías. Teniendo en cuenta la importancia de la auditoría del sistema de calidad, ISO ha desarrollado estándares específicos para auditorías de calidad que definen los procedimientos y requisitos que deben seguir los auditores.

La norma ISO 10011-1:2018 proporciona las reglas generales para la auditoría y normaliza los procesos de auditoría de sistemas de calidad la cual presenta la siguiente metodología:

1. **Preparación de la auditoria**

- Establecimiento del alcance: Es el primer paso para realizar en donde se determina que elementos del sistema de calidad, localidades físicas y que actividades organizacionales serán auditadas.
- Selección del auditor: Se designa al personal que llevará a cabo la auditoria.
- Identificación de documentos aplicables: Se debe identificar los documentos del sistema de calidad que correspondan al alcance de la auditoria.
- Revisión de documentación: El propósito es comprender de la mejor manera como se están llevando a cabo las actividades dentro del sistema.
- Revisión de auditorías previas: En caso de haber auditorías previas, el auditor debe revisar la documentación con la finalidad de estar alerta en los errores u observaciones de esas auditorías.
- Preparación de la guía de auditoria: El auditor o grupo de auditores prearán una guía con preguntas que serán usadas en la auditoría, esto con la finalidad de indagar a fondo alguna inconformidad.

2. Realización de la auditoria

- Apertura de la auditoria: La realización de la auditoria comienza con la reunión de apertura, la cual no debe durar mas de 10 minutos. El propósito es presentar al equipo auditor, revisar los alcances y objetivos de la auditoria, un breve resumen de los métodos y procedimientos que serán utilizados, confirmar que estén disponibles los recursos necesarios para el auditor, confirmar la fecha y horario de la sesión de cierre.

- Obtención de evidencias: Son recolectadas a través de entrevistas, examinación de documentos y registros, mediante la observación y condiciones del área al alcance de la auditoría.
- Registro de las observaciones: Todas las observaciones deben ser registradas por el auditor o equipo auditor, las cuales deberán revisar para determinar las conformidades y no conformidades.
- Cierre de la auditoría: Al finalizar la auditoria se deberá realizar una sesión de cierre con el propósito de comentar las observaciones encontradas durante el proceso.

2.2.6 Clasificación de los activos de información

De acuerdo con la norma ISO 27001:2013, es fundamental realizar un inventario y clasificación de la información de la empresa como parte del cumplimiento del Modelo de Seguridad y Privacidad de la información. Para conseguir generar de forma adecuada la clasificación de los activos se debe tomar como referente los tres pilares específicos para la información: confidencialidad, integridad y disponibilidad. (Mintic,2017)

2.2.6.1 De acuerdo con la Confidencialidad. Se refiere a que la información no debe ser revelada o expuesta a personal no autorizado. Se clasifica de bajo los siguientes criterios:

Tabla 3. Clasificación de los activos por Confidencialidad

Información restringida	Es aquella información que solo se encuentra disponible para un proceso específico de la organización, por lo que de ser accedida por un tercero puede tener un impacto negativo interno
Información privada	Es la información accesible para los procesos que integran la empresa, en caso de ser accedido por terceros puede generar un impacto negativo en los procesos internos
Información publica	Es aquella que se encuentra a disposición tanto del personal interno como externo y que no trae consecuencias negativas en los procesos internos

2.2.6.2 De acuerdo con la Integridad. Es la disposición completa y exacta que debe mantener la información. De esta manera se garantiza que la información sea completa, exacta y precisa.

Tabla 4. Clasificación de los activos por Integridad

A - ALTA	En caso de pérdida completa de la información ocasionara que tenga un impacto negativo en lo referente a lo legal, económico, interrumpir la operación total de los procesos.
M – MEDIA	En caso de pérdida completa de la información ocasionara que tenga un impacto negativo en lo referente a lo legal y demorar las operaciones en los procesos
B - BAJA	En caso de pérdida completa de la información no representaría un impacto mayor dentro de la organización.
No clasificada	Hace referencia a los activos de información que deben ser parte del inventario, pero aún no se encuentran clasificados.

2.2.6.3 De acuerdo con la Disponibilidad. La información siempre debe estar accesible para el personal autorizado, además debe ser útil en tiempo y forma según las requieran.

Tabla 5. Clasificación de los activos por Disponibilidad

1 - ALTA	Al no tener disponible la información puede ocasionar un impacto negativo en relación con criterios económicos, retrasar los procesos y actividades desarrolladas.
2 – MEDIA	Al no tener disponible la información puede ocasionar un impacto negativo en relación con criterios económicos, interrupción y demorar de actividades operativas.

3 - BAJA	Al no tener disponible la información puede afectar la continuidad de actividades de la empresa. Sin embargo, no tiene implicaciones de tipo legal.
4 - No clasificada	Son aquellos activos de información, que se deben incluir en el inventario y que no han sido clasificada.

2.2.7 Manejo de la información.

Permite a las organizaciones documentar de manera efectiva sus activos y cómo se relacionan con cada una de las operaciones de la organización.

Durante el desarrollo se debe tener en cuenta los activos que tienen significación operativa para la empresa, es decir, todos aquellos que resultan fundamentales y permiten de forma práctica y efectiva cumplir con los objetivos estratégicos.

2.2.7.1 Criticidad de los activos. Mediante la siguiente tabla podemos determinar qué tan crítico resulta un activo para la empresa.

Tabla 6. Criterios de Criticidad

Confidencialidad	Integridad	Disponibilidad
Información restringida	Alta	Alta
Información privada	Media	Media
Información pública	Baja	Baja
Información no pública	No clasificada	No clasificada

En base a la "Tabla 6" podemos decir que la criticidad de activos es:

Tabla 7. Criticidad de Activos

ALTA	Son aquellos activos en los cuales en dos o todas las propiedades (confidencialidad, integridad y disponibilidad) se clasifica como alta
MEDIA	Son aquellos activos de información para en los que al menos una propiedad es clasificada como nivel medio
BAJA	Son los activos de información en lo que su clasificación en cualquiera de los niveles es considerada como baja

2.2.8 Plan de mitigación de riesgos

2.2.8.1 Definición. Benavides (2017) menciona que, se denomina plan de mitigación a las estrategias establecidas por la empresa que tratan de reducir la incidencia de riesgos y el impacto que estos puedan causar. El objetivo de principal del plan de mitigación de riesgos es reducir la exposición al riesgo con la intención de llevarlos a umbrales aceptables para cada organización.

En base a lo antes mencionado podemos decir que la estrategia de mitigación esta referida a las acciones que se toman por adelantado. La probabilidad de ocurrencia del riesgo y su impacto se puede identificar en una fase temprana.

2.2.8.2 Características. Podemos describir las características del plan de mitigación, tomando en cuenta lo mencionado en la Metodología para la gestión de riesgos del Ministerio de Finanzas del Ecuador (2017):

> En el plan de mitigación de riesgos se desarrollará una estrategia de gestión, que incluya su proceso e implementación. Se definirán objetivos y metas, asignando responsabilidades para áreas específicas, identificando conocimientos técnicos, describiendo el proceso de evaluación de riesgos y las áreas a considerar, detallando indicadores de riesgos, delineando procedimientos para las estrategias del manejo, estableciendo lineamientos para el monitoreo y definiendo los reportes, documentos y las comunicaciones necesarias. (p.6)

2.2.9 Ciclo de Deming

El nombre del ciclo PDCA (o PHVA) proviene de las siglas Plan, Do, Verify. con actuarios, "planificar, ejecutar, verificar, ejecutar" en inglés. También llamado como ciclo de Deming, como su autor Edwards Deming. Esta metodología describe los cuatro pasos básicos que se deben realizar en un proceso. Lograr sistemáticamente la mejora continua, entendida como tal mejora la calidad continua (reducir fallas, mejorar la efectividad y eficiencia, resuelve problemas, predice y eliminar riesgos potenciales). El ciclo de deming consta de 4 etapas, por lo que después de la etapa final, se debe volver al primero y repetir el ciclo nuevamente para que la actividad pueda reevaluar periódicamente para incorporar nuevas mejoras. (1&1 IONOS España S.L.U., 2020)

2.2.9.1 Planificar. En este apartado se determina metas y objetivos

- Definición de políticas y objetivos
- Determinación del alcance
- Valoración de activos
- Análisis de riesgo
- Gestionar los riesgos
- Seleccionar los controles ISO 27001:2013 y OSSTM

2.2.9.2 Hacer. Incluye asegurar la educación y el entrenamiento e implementar el trabajo, y estas son:

- Definir e implementar un plan de gestión de riesgos
- Implementar controles seleccionados y sus indicadores
- Implementar el sistema de gestión
- Lista de verificaciones ISO 27001:2013

2.2.9.3 Chequear. Consiste en verificar los efectos de la implementación:

- Revisión Gerencial Desarrollar procesos de monitorización
- Realizar la matriz de riesgo
- Clasificación de los activos de la información

2.2.9.4 Actuar. Consiste en tomar la acción adecuada:

- Implementar las mejoras
- Adoptar acciones preventivas y correctivas
- Comunicar acciones y resultados
- Verificar que las mejoras cumplan el objetivo
- Socialización del informe de auditoría y plan de mitigación de riesgo

III. METODOLOGIA

3.1 ENFOQUE METODOLOGICO

3.1.1 Enfoque

La presente investigación contó con los siguientes enfoques:

Cualitativo

Sampieri (2016) menciona "Utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación, tiene como objetivo la descripción de las cualidades de un fenómeno"

La presente investigación tuvo un enfoque cualitativo ya que por medio de la entrevista se conoció el sistema de seguridad de la información que mantiene la florícola Galápagos Flores S.A.

Cuantitativo

Hernández, Fernández y Baptista (2017) definen los métodos cuantitativos como una serie de procesos secuenciales y evidénciales en los que se determinan hipótesis y se miden variables en función de la realidad o fenómenos, de modo que las conclusiones emergen cuando se obtienen los resultados de la medición.

Además, es de carácter cuantitativo ya que se usó procesos estadísticos para el análisis de los datos obtenidos de encuestas el cual nos brindó un panorama general del estado actual de la florícola, dichos datos fueron tabulados.

3.1.2 Tipo de Investigación

El trabajo al ser basado en un enfoque cuantitativo y cualitativo se utilizó los siguientes tipos de investigación:

- **Bibliográfica documental**

Es de tipo bibliográfico documental debido a que fue basada en tesis, proyectos y artículos científicos, los cuales permitieron fundamentar el proceso de auditoria informática, las normas que fueron usadas y la metodología con la cual fue desarrolladas, además de elaborar el marco teórico.

Según Hernández, Fernández y Baptista (2017):

"La investigación documental es detectar, obtener y consultar información bibliográfica que aporten con conocimiento y/o información recogida moderadamente de

cualquier realidad, de manera selectiva, de modo que pueden ser útiles para los propósitos del estudio."

- **Descriptivo**

Se aplico una investigación descriptiva ya que nos permitió obtener información verídica de la seguridad informática que ofrece dicha florícola, además se pudo describir de manera detallada los procesos que cada departamento realiza mediante el sistema. Según Guevara, et al. (2020) menciona que:

> "El objetivo es describir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permitan establecer la estructura o el comportamiento de los fenómenos en estudio, proporcionando información sistemática y comprobable con la de otras fuentes".

Es así, como se inició desde los involucrados en la investigación como el encargado y personal operativo de la florícola que procuren a ofrecer información del qué, cómo, cuándo y dónde, del problema de investigación.

- **De Campo**

Fue una investigación de campo ya que recogió y registró los datos ordenadamente como objeto de estudio directamente de la florícola Galápagos Flores S.A, en el cual se aplicó los instrumentos que permitieron controlar los fenómenos como la entrevista dirigida al encargado del área de sistemas y la encuesta al personal operativo. Baena (2017), afirma que:

> "La investigación de campo consiste en la exploración del terreno , que en realidad es el contacto directo con el objeto de estudio fundamentándose en el acopio de testimonios, orales y escritos, sentimientos, pensamientos, estados de ánimo de personas vivas" (p. 70).

3.2 IDEA A DEFENDER

La auditoría de seguridad informática favorecerá los controles de seguridad disminuyendo los riesgos asociados al manejo de la información.

3.3 OPERALIZACIÓN DE VARIABLES

3.3.1 Definición de las variables

De acuerdo con el problema de investigación se ha definido las siguientes variables:

- Variable Independiente: Auditoria de seguridad informática Variable Dependiente: Riesgos asociados al manejo de la información

3.3.2 Operacionalización de variables

Tabla 8. Operacionalización de variables

Tipo de Variable	Variable	Dimensión	Indicadores	Técnica	Instrumento
Independiente	Auditoria de seguridad informática	Proceso	Matriz de riesgo	Entrevista Observación	Cuestionario CheckList
		Evidencia	Controles de acceso, actas de compromiso, confidencialidad		
		Sistemas de información	Fallas tecnológicas		
Dependiente	Riesgos asociados al manejo de la información	Proceso	Disponibilidad, integridad y confidencialidad	Encuesta	Cuestionario
		Información	Políticas de privacidad, actas formales, clasificación de la información		
		Equipo informático	Software de control, chequeos periódicos		

3.4 MÉTODOS A UTILIZAR

3.4.1 Métodos

Rodríguez y Pérez (2017), señalaron que el método inductivo-deductivo consta de dos procesos inversos: inducción y deducción. La inducción es una forma de razonamiento en la que las personas pasan del conocimiento de un caso particular a un conocimiento más amplio, que refleja el terreno común en los fenómenos individuales. Se basa en la repetición de hechos y fenómenos, encontrando características comunes en un determinado grupo, con el fin de sacar conclusiones que los caracterice.

3.4.1.1 Método inductivo

Para la presente investigación se utilizó el método inductivo ya que, mediante la observación directa, la experimentación y las relaciones con los fenómenos del problema nos ayudó a separar los actos más elementales del problema y experimentarlos de forma individual. De acuerdo con Prieto (2018) este método:

> "Fundamentalmente consiste en estudiar u observar hechos o experiencias particulares con el fin de llegar a conclusiones que puedan inducir o permitir derivar de ello los fundamentos de una teoría".

3.4.1.2 Método deductivo

"Consiste en un análisis de los principios generales de un tema específico: una vez comprobado y verificado que determinado principio es válido, se procede a aplicarlo a contextos particulares" (Prieto,2018).

Se utilizó el método deductivo debido a que parte de un estudio de casos particulares para llegar a conclusiones que explicaron el problema de la investigación, además permitió describir lo que se está investigando por medio de principios o teorías ya aceptadas.

3.4.2 Técnicas de investigación

3.4.2.1 Entrevista

De acuerdo con Palella y Martins (2012):

> "La ventaja esencial de la entrevista reside en que son los mismos actores sociales quienes proporcionan los datos relativos a sus conducidas opiniones, deseos, actitudes, expectativas, en fin, informaciones, que, por su misma naturaleza es casi imposible obtener desde afuera" (p.119).

Es así, como se utilizó la técnica de la entrevista no estructurada al jefe del departamento de sistemas, para determinar los procesos que se mantienen para la seguridad de la información dentro de la florícola.

3.4.2.2 Encuesta

La encuesta es una técnica de recolección de datos que según Hernández, Fernández y Baptista (2017) afirman que "consiste en un conjunto de preguntas respecto de una o más variables a medir" (pág. 217).

Se usó la técnica de la encuesta mediante la aplicación de un cuestionario con la única finalidad de recolectar información que fue importante para la investigación, le encuesta fue aplicada al personal que tiene acceso a un equipo tecnológico dentro de la florícola.

3.5 ANÁLISIS ESTADÍSTICO

3.5.1 Población y muestra

La población para la presente investigación se ha seleccionada a la florícola Galápagos Flores S.A, con un número alrededor de 300 personas entre personal de cultivo, departamento de contabilidad, departamento de ventas, departamento de compras, departamento de procesos, departamento de seguridad, departamento de logística y departamento de postcosecha.

En donde se seleccionó una muestra por conveniencia de 15 personas abarcando el personal administrativo y de postcosecha, esto debido a que son usuarios que se encuentran en contacto con los equipos de cómputo y por lo tanto la información brindada mediante la encuesta aportó a la investigación. Por otro lado, se excluyó al personal de cultivo ya que los usuarios no manejan equipos informáticos, es decir, desconocen los procesos, capacitaciones brindas por el área de sistemas, acceso a la información, entre otros.

Tabla 9. Población y muestra

Muestra por conveniencia	***Muestra (numero)***	***Técnica***
Departamento de ventas	3	Encuesta
Departamento de contabilidad y finanzas	2	Encuesta
Jefe del departamento de		Encuesta

compras	1	
Jefe del departamento de logística	1	Encuesta
Departamento de bodega	1	Encuesta
Personal de postcosecha	5	Encuesta
Departamento de Recursos Humanos	2	Encuesta
Jefe del departamento de sistemas	1	Entrevista

La tabla 9 presenta la población y la muestra escogida por conveniencia para la presente investigación.

La encuesta fue realizada a la una muestra de 15 personas, debido a que están en contacto con los equipos informáticos que mantiene la empresa. El personal se encuentra distribuido entre, jefes de área, personal de postcosecha y empaque.

Una vez aplicada la encuesta a la muestra escogida por conveniencia para la presente investigación, se muestra los siguientes resultados.

- **Pregunta 1:** ¿Con que frecuencia se mantiene un control de los procesos que realiza el computador?

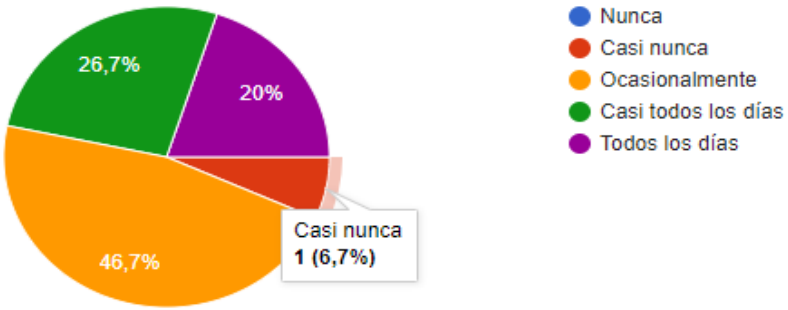


Figura 1. Resultados primera pregunta de la encuesta

Análisis e interpretación. Con los resultados que se puede apreciar en la gráfica podemos decir que el área de sistemas no realizada los controles de procesos de acuerdo a la planificación que mantiene internamente.

- **Pregunta 2:** ¿Con que frecuencia recibe capacitaciones por parte del departamento de sistemas?

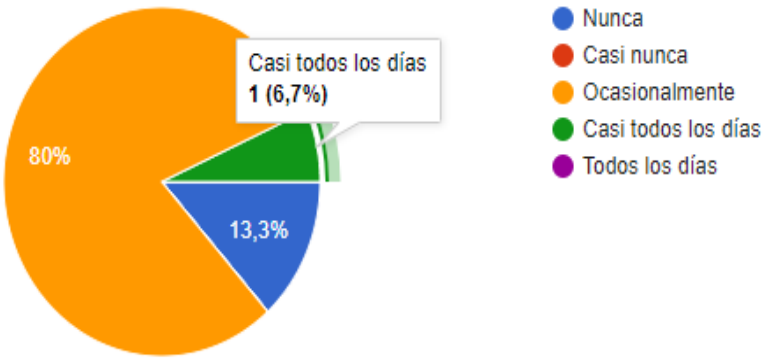


Figura 2. Resultados segunda pregunta de la encuesta

Análisis e interpretación. Los datos obtenidos en la encuesta nos muestran que el personal que maneja los equipos de cómputo recibe ocasionalmente capacitaciones del uso correcto de los equipos.

- **Pregunta 3:** ¿Para ingresar al sistema integrado FINANCONTRY requiere una contraseña?

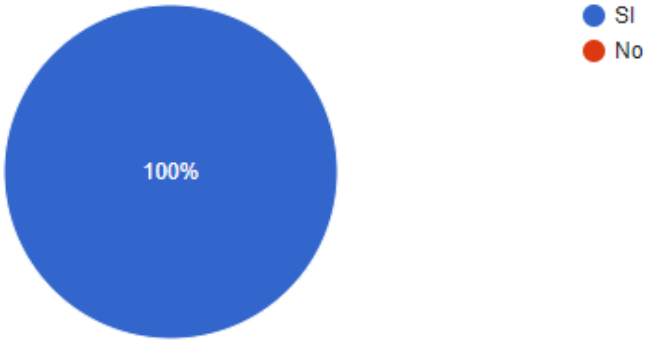


Figura 3. Resultados tercera pregunta de la encuesta

Análisis e interpretación. Como se puede apreciar en la gráfica todo el personal encuestado afirmó que para ingresar al sistema integrado FINANCONTRY requieren necesariamente de una contraseña.

- **Pregunta 4:** ¿Para iniciar sesión en su computador requiere una contraseña?

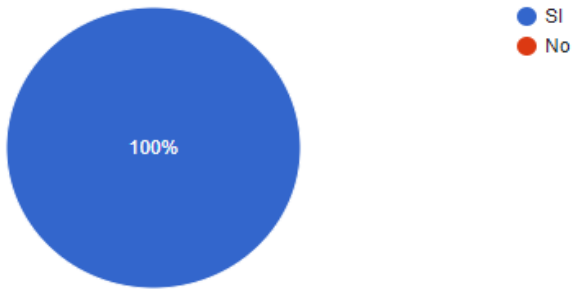


Figura *4*. Resultados cuarta pregunta de la encuesta

Análisis e interpretación. Al preguntar al personal encuestado de la florícola para el inicio de sesión en su computador requiere una contraseña, todos los usuarios afirmaron que se requiere una contraseña para el acceso de su equipo.

- **Pregunta 5:** ¿Los equipos de cómputo cumplen con las características para agilizar el proceso?

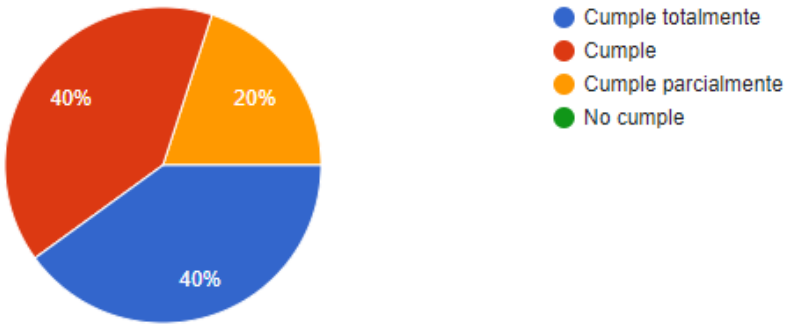


Figura 5. Resultados quinta pregunta de la encuesta

Análisis e interpretación. Los resultados obtenidos nos muestran que la mayoría del personal encuestado afirma que los equipos de cómputo que utilizan cuentan con las características necesarias para realizar su trabajo.

- **Pregunta 6:** ¿Tiene conocimiento de los programas instalados en el equipo de cómputo?

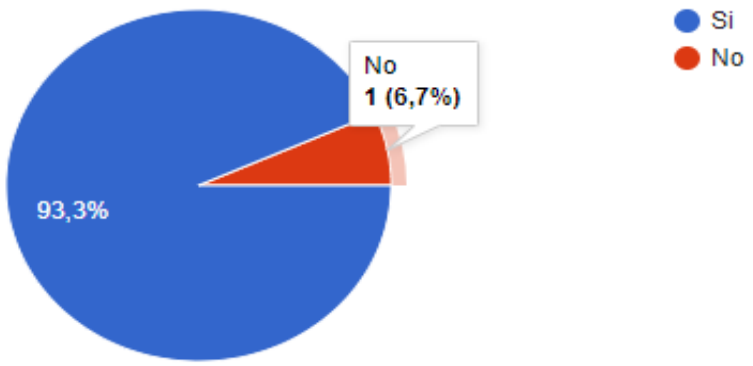


Figura 6 . Resultados sexta pregunta de la encuesta

Análisis e interpretación. Al grupo de encuestados en su mayoría tiene el conocimiento de los programas que se encuentran instalados en su equipo de cómputo.

- **Pregunta 7:** ¿Con que frecuencia se realiza mantenimiento técnico al equipo de cómputo?

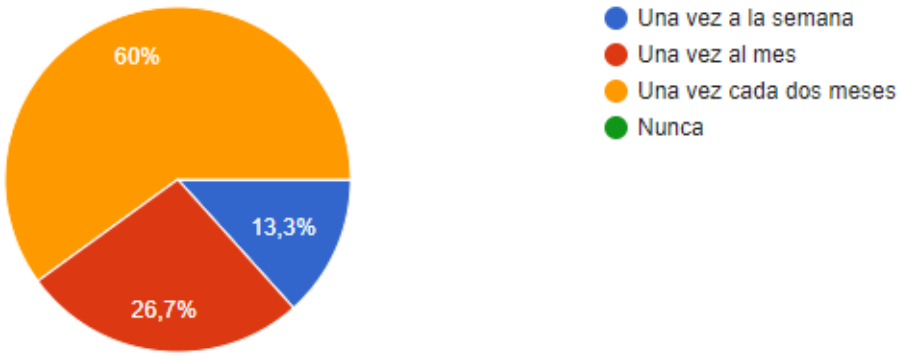


Figura 7. Resultados séptima pregunta de la encuesta

Análisis e interpretación. En cuanto a los resultados de esta pregunta, los encuestados afirman que los mantenimientos sí son realizados de acuerdo a la planificación que mantienen en el área de sistemas y el resto de los casos menciona que se realiza con menor frecuencia debido a que el equipo presenta fallas operativas.

- **Pregunta 8:** ¿Tiene conocimiento de las políticas de privacidad de la información que maneja la florícola?

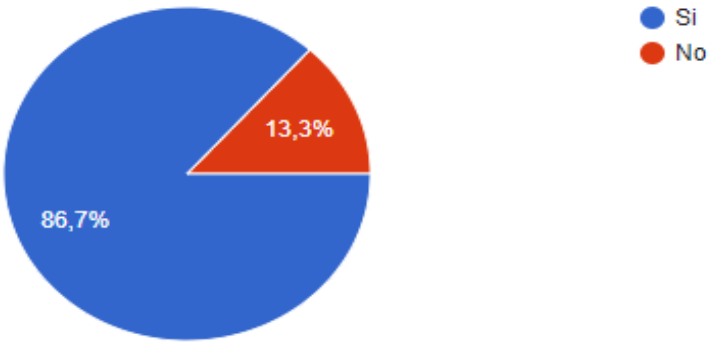


Figura 8. Resultados octava pregunta de la encuesta

Análisis e interpretación. Con respecto a las políticas de privacidad de la información que maneja la florícola 13 encuestados conocen dichas políticas, que fueron socializadas por el departamento de talento humano.

- **Pregunta 9:** ¿La administración está monitoreando su computadora todo el tiempo?

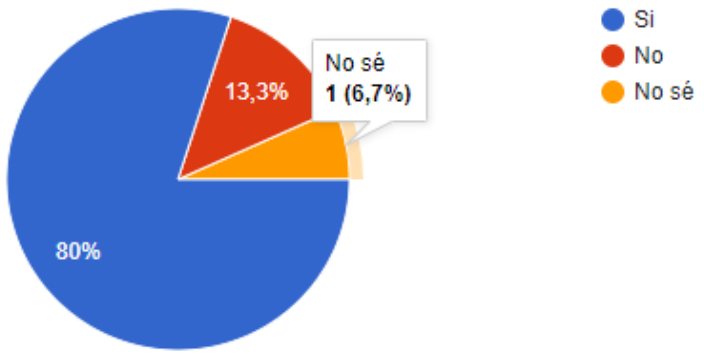


Figura 9. Resultados novena pregunta de la encuesta

Análisis e interpretación. De acuerdo a los datos recolectados en la presente pregunta, se puede evidenciar que el personal tiene en cuenta que su equipo siempre se encuentra monitoreado por el área de sistemas, es decir, mantienen un control de los procesos que se realizan.

- **Pregunta 10:** ¿Qué tan difícil es para usted identificar un virus informático?

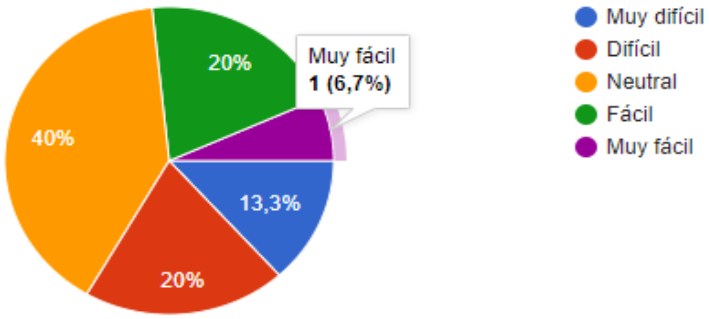


Figura 10. Resultados décima pregunta de la encuesta

Análisis e interpretación. Al preguntar en la florícola que tan fácil es identificar un virus informático a un grupo de encuestados de 15 personas, se obtuvo que para la mayoría del personal es difícil reconocer un virus informático debido a que hasta el momento no se han encontrado en esa situación, por otro lado, una mínima cantidad de los encuestados afirma saber cómo reconocer un virus informático.

IV. RESULTADOS Y DISCUSION

4.1. RESULTADOS

4.1.1. Datos informativos

GALÁPAGOS FLORES S.A

4.1.1.1. Logotipo.

Figura 11. Logotipo GALÁPAGOS FLORES S.A

Fuente: Galápagos Flores S.A (2021) Sitio web

4.1.1.2 Ubicación.

Provincia Pichincha, Cantón Pedro Moncayo, Parroquia Tabacundo, Barrio La Quinta, calle Pacifico Proaño 11019 e intersección secundaria.

4.1.1.3 Descripción**.**

Galápagos Flores S. A. Es una empresa orgullosamente ecuatoriana dedicada al cultivo y exportación de flores constituida cumpliendo toda la normativa legal con un liderazgo comprometido y sólido para ofrecer un trabajo digno, inclusivo, seguro, gestionando la protección de la salud y confort de sus colaboradores, tanto empleados como trabajadores. Tiene una producción sustentable, en un medio ambiente manejando los recursos naturales responsablemente, siguiendo normas de seguridad confiables para disuadir actividades ilícitas, corrupción y soborno a fin de mantenerse como una empresa líder en el sector florícola comprometida con la comunidad y una mejora continua.

4.1.1.4 Misión.

Somos una empresa líder dedicada a la producción y exportación en el área florícola: confiable, eficiente y ética; orientada a satisfacer las necesidades y aspiraciones de nuestros clientes, estableciendo relaciones de largo plazo. Somos un aporte positivo para la sociedad, generando empleo directo e indirecto dentro de un buen ambiente de trabajo, justo, pagando tributos y obteniendo un justo margen de utilidad. (GALAFLOR, 2021)

4.1.1.5 Visión.

Trabajar para ser los mejores en el sector florícola, satisfaciendo las necesidades de nuestros empleados, clientes, accionistas, capital humano y sociedad. Nuestro compromiso es la seguridad y excelencia, a través de acciones de calidad, servicio, innovación, eficiencia, rentabilidad y con responsabilidad frente al medio ambiente y la sociedad. GALÁPAGOS FLORES S.A, tiene como principio dentro de su visión gerencial poner los medios necesarios al alcance de su producción y a las entidades reguladoras y fiscalizadoras, para que se desarrollen las actividades propias de la exportación, dentro de la confianza y la seguridad posibles. Cumpliendo con las normas y requisitos establecidos a nivel nacional e internacional, todo esto soportado en la metodología propuesta en el programa del sistema de gestión de seguridad BASC y C-TPAT. (GALAFLOR, 2021)

4.1.1.6 Objetivo de negocio.

Ser un sistema, que permita establecer los procedimientos de seguridad en el 100% de acciones y actividades, que deben cumplir todos los empleados, trabajadores, visitantes, contratistas y proveedores de la empresa GALAPAGOS FLORES S.A. Establecer la comunicación entre todas las personas relacionadas con los controles del sistema de seguridad BASC y disminuir las ambigüedades para que este personal pueda realizar mejor su trabajo. Se hace énfasis en la prevención de ilícitos como tráfico de narcóticos, químicos controlados, mercancías para el lavado de dinero, robo de información y tráfico de armas en general. (GALAFLOR, 2021)

4.1.1.7 Objetivos Estratégicos Institucionales.

Galápagos Flores S.A es equipo de profesionales y mandos medios que velan por el óptimo desempeño de los diferentes procesos productivo donde buscamos:

1. Cumplimiento de los compromisos y metas.
2. Incremento de la productividad y rentabilidad.
3. Reducción de costos.
4. Mejora en la planeación.
5. Cumplimiento de los cronogramas.
6. Identificar necesidades y requerimientos.
7. Generar reportes útiles para la toma de decisiones.
8. Mejora en los procesos logísticos y de seguridad.
9. Desarrollar las actividades en un ambiente seguro.

4.1.1.8 Estructura Orgánica Funcional.

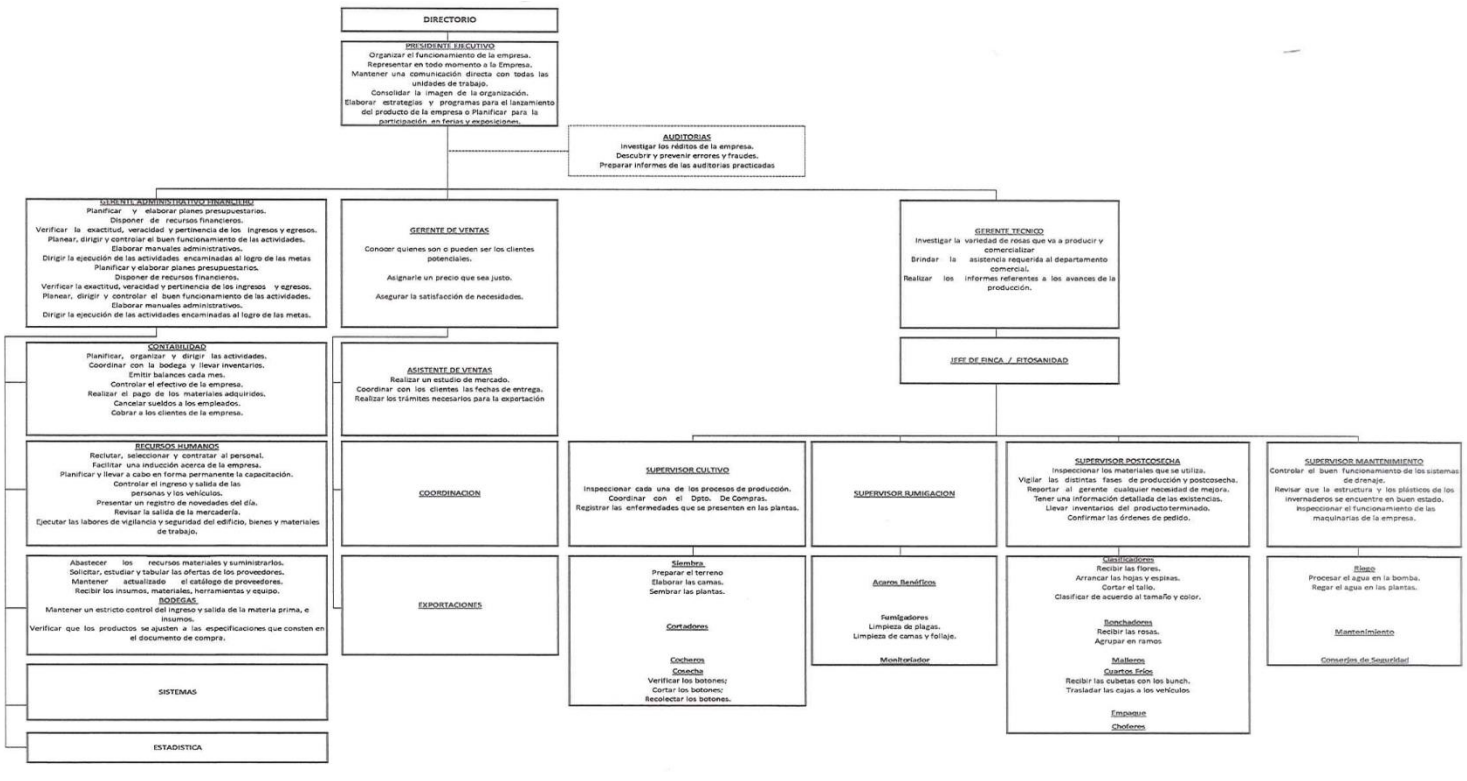


Figura 12. Estructura organización funcional

Fuente: Galápagos Flores S.A (2021) Sitio web

4.1.2 Auditoría Informática

El proceso de auditora se llevó a cabo de acuerdo con la metodología ISO 10011-1:2018, la cual contempla lo siguiente:

4.1.2.1 Preparación de la auditoría

Se realizó la auditoria mediante la coordinación del Gerente Financiero y encargado del área de sistemas, en donde se verificó la disponibilidad de tiempo para realizar las visitas. Además, se determinó el alcance, objetivo y justificación de la auditoría, así mismo, se realizó el cronograma de actividades. (Ver Anexo 10)

Equipo auditor

Auditor	Heidy Quishpe
Asesor	Ing. Marco Yandún, MSc.

Identificación de documentos aplicables

La auditoría de seguridad de la información en la florícola Galápagos Flores S.A fue llevada a cabo aplicando la normativa ISO 27001:2013.

En donde, de un total de 114 controles 8 no fueron aplicados a la revisión debido a que la florícola no cuenta con un ambiente de desarrollo, los mismos son enlistados a continuación:

- A.9.4.5. Control de Acceso a Códigos Fuente de Programas.
- A.12.1.4. Separación de los ambientes de desarrollo, ensayo y operación.
- A.14.2.1. Política de desarrollo seguro.
- A.14.2.2. Procedimiento de control de cambios en sistemas.
- A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones.
- A.14.2.4. Restricciones sobre los cambios de paquetes de software.
- A.14.2.5. Principios de construcción de sistemas de seguros.
- A.14.2.6. Ambiente de desarrollo seguro.

Dicho esto, los controles a revisar en la empresa son:

- A.5.1.1. Políticas para la Seguridad de la Información.
- A.5.1.2. Revisión de las Políticas para seguridad de la información
- A.6.1.1. Seguridad de la Información Roles y Responsabilidades.
- A.6.1.2. Separación de deberes.
- A.6.1.3. Contacto con las autoridades.
- A.6.1.4. Contacto con grupos de interés especial.
- A.6.1.5. Seguridad de la información en Gestión de Proyectos
- A.6.2.1. Política para dispositivos móviles.
- A.6.2.2. Teletrabajo.
- A.7.1.1. Selección.
- A.7.1.2. Términos y condiciones del empleo.
- A.7.2.1. Responsabilidades de la Dirección.
- A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información
- A.7.2.3. Proceso disciplinario.
- A.7.3.1. Terminación o cambio de responsabilidades de empleo.
- A.8.1.1. Inventario de Activos.
- A.8.1.2. Propiedad de los activos.
- A.8.1.3. Uso Aceptable de los Activos.
- A.8.1.4. Devolución de Activos.
- A.8.2.1. Clasificación de la Información.
- A.8.2.2. Etiquetado de la Información.
- A.8.2.3. Manejo de Activos.
- A.8.3.1. Gestión de medios de Soporte Removibles.
- A.8.3.2. Disposición de los medios de soporte.
- A.8.3.3. Transferencia de medios de soporte físicos.
- A.9.1.1. Política de Control de Acceso.
- A.9.1.2. Acceso a redes y a servicios en red.
- A.9.2.1. Registro y cancelación del registro de usuarios.
- A.9.2.2. Suministro de acceso de usuarios.
- A.9.2.3. Gestión de derechos de acceso privilegiado.

- A.9.2.4. Gestión de información de autenticación secreta de usuarios.
- A.9.2.5. Revisión de los derechos de acceso de usuarios.
- A.9.2.6. Cancelación o ajuste de los derechos de acceso.
- A.9.3.1.Uso de información secreta.
- A.9.4.1. Restricción de acceso a información.
- A.9.4.2. Procedimiento de Conexión Segura.
- A.9.4.3. Sistema de Gestión de Contraseñas.
- A.9.4.4. Uso de programas utilitarios privilegiados.
- A.10.1.1. Política sobre el uso de controles Criptográficos.
- A.10.1.2. Gestión de Claves.
- A.11.1.1. Perímetro de Seguridad Física.
- A.11.1.2. Controles Físicos de entrada
- A.11.1.3. Seguridad de oficinas, salones e instalaciones.
- A.11.1.4. Protección contra amenazas externas y ambientales.
- A.11.1.5. Trabajo en áreas seguras.
- A.11.1.6. Áreas de despacho y carga.
- A.11.2.1. Ubicación y protección de los equipos.
- A.11.2.2. Servicios Públicos de soporte.
- A.11.2.3. Seguridad del cableado.
- A.11.2.4. Mantenimiento de equipos.
- A.11.2.5. Retiro de Activos.
- A.11.2.6. Seguridad de equipos y activos fuera del predio.
- A.11.2.7. Disposición segura o reutilización de equipos.
- A.11.2.8. Equipos sin supervisión de los usuarios.
- A.11.2.9. Política de escritorio limpio y pantalla limpia.
- A.12.1.1. Procedimientos de operación documentadas.
- A.12.1.2. Gestión de Cambios.
- A.12.1.3. Gestión de Capacidad.
- A.12.2.1. Controles contra códigos maliciosos.
- A.12.3.1. Copias de respaldo de la información.
- A.12.4.1. Registro de eventos.
- A.12.4.2. Protección de la información de registro.

- A.12.4.3. Registros del administrador y del operador.
- A.12.4.4. Sincronización de relojes.
- A.12.5.1. Instalación de software en sistemas operativos.
- A.12.6.1. Gestión de las vulnerabilidades técnicas.
- A.12.6.2. Restricciones sobre la instalación de Software.
- A.12.7.1. Controles sobre auditorías de Sistemas de Información.
- A.13.1.1. Controles de redes.
- A.13.1.2. Seguridad de los servicios de red.
- A.13.1.3. Separación en las redes.
- A.13.2.1. Políticas y procedimientos de transferencia de información.
- A.13.2.2. Acuerdos sobre transferencia de información.
- A.13.2.3. Mensajes electrónicos.
- A.13.2.4. Acuerdos de confidencialidad o de no divulgación.
- A.14.1.1. Análisis y especificación de requisitos de seguridad de la información.
- A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas.
- A.14.1.3. Protección de transacciones de servicios de aplicaciones.
- A.14.2.7. Desarrollo contratado externamente.
- A.14.2.8. Pruebas de seguridad de sistemas.
- A.14.2.9. Pruebas de aceptación de sistemas.
- A.14.3.1. Protección de datos de ensayo.
- A.15.1.1. Política de seguridad de la información para las relaciones con proveedores.
- A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores.
- A.15.1.3. Cadena de suministro de tecnología de información y comunicación.
- A.15.2.1. Seguimiento y revisión de los servicios de los proveedores.
- A.15.2.2. Gestión de cambios a los servicios de los proveedores.
- A.16.1.1. Responsabilidades y procedimientos.
- A.16.1.2. Informe de eventos de seguridad de la información.
- A.16.1.3. Informe de debilidades de seguridad de la información.
- A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
- A.16.1.5. Respuesta a incidentes de seguridad de la información.

- A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información.
- A.16.1.7. Recolección de evidencia
- A.17.1.1. Planificación de la continuidad de la seguridad de la información
- A.17.1.2. Implementación de la continuidad de la seguridad de la información.
- A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- A.17.2.1. Disponibilidad de instalaciones de procesamiento de información
- A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables.
- A.18.1.2. Derechos de Propiedad Intelectual.
- A.18.1.3. Protección de registros.
- A.18.1.4. Privacidad y protección de la información identificable personalmente.
- A.18.1.5. Reglamentación de Controles Criptográficos.
- A.18.2.1. Revisión independiente de la seguridad de la información.
- A.18.2.2. Cumplimiento con las políticas y normas de seguridad.
- A.18.2.3. Revisión del Cumplimiento Técnico.

Estado de situación previo a la auditoría

Revisión de auditorías previas

No se encontró documentación, debido a que la florícola no ha contado con auditorias de seguridad informática.

Preparación de la guía de auditoría.

Se estableció la entrevista que fue aplicada el jefe del área de sistemas.

1.- ¿El área de sistemas cuenta con un Sistema de gestión de seguridad informática?

2.- ¿Cuenta con la formación académica necesaria para manejar el área de sistemas?

3.- ¿Mantiene un inventario de activos del área?

4.- ¿Existe una Matriz de riesgo de Seguridad Informática?

5.- ¿Se ha desarrollado Planes de mejoramiento de seguridad informática?

6.- ¿El área de sistemas cuenta con un Plan de contingencia de la seguridad de la información?

7.- ¿Qué procedimiento se realiza para la asignación de contraseñas a los usuarios?

8.- ¿Realizan una planificación del mantenimiento de activos informáticos?

Mediante la aplicación del instrumento se consiguió la siguiente información

Tabla 10. Documentos requeridos en la encuesta

REQUISITO	EVIDENCIA
Sistema de gestión de seguridad informática	No existe documentación
Certificación de estudios del jefe del departamento de sistemas	Certifica sus estudios como ingeniero en sistemas
Inventario de activos informáticos	El inventario se encuentra desactualizado desde el 2018
Matriz de riesgo de Seguridad Informática	Se miden siete riesgos, los cuales se encuentran inmersos en la matriz de área
Planes de mejoramiento de seguridad informática	No existe
Plan de contingencia de la seguridad de la información	El plan de contingencia se enfoca en el respaldo de la información del sistema integrado, sin embargo, la información que se maneja diariamente. Cuenta con un plan de contingencia básico para la información que actualmente se maneja.
Procedimiento de asignación de credenciales a los usuarios	No existe, se realiza de manera empírica
Procedimiento de asignación de contraseñas a la red WIFI	No existe, se realiza de manera empírica
Procedimiento de generación de contraseñas	No existe, se realiza de manera empírica
Procedimiento de ejecución de Backups	No existe, se realiza empíricamente.
Procedimiento de Manejo de discos extraíbles	No existe, se realiza empíricamente.

Procedimiento de control de acceso a internet	No existe, se realiza empíricamente.
Cronograma de mantenimiento de activos informáticos	Se realiza mediante una planificación anual que es aprobada a principios del año en curso.
Hojas de vida de activos informáticos	No existe
Compromiso de confidencialidad firmado por el personal	Existe el documento de confidencialidad el cual es firmado al realizar el contrato, dicho documento se encuentra anexado en cada carpeta del trabajador
Actas de capacitación a los usuarios internos en Seguridad Informática	No existe

De los documentos solicitados al área de sistemas se resume de la siguiente manera:

1. Se solicitó al jefe del departamento de sistemas la matriz de riesgos.

El Ing. José Barreiro manifestó que, los riesgos mostrados en la matriz para el área de sistemas se realizó conjunto con el mapa de riesgos de la empresa.
Se midieron los siguientes riesgos

- ✓ No hay comunicación entre CLIENTE-SERVIDOR
- ✓ Interrupción del fluido eléctrico durante la ejecución de procesos
- ✓ Indisponibilidad de los servidores que contienen almacenados los datos
- ✓ Pérdida del servicio de internet
- ✓ Falla de un servidor
- ✓ Substracción, robo o fuga de información confidencial
- ✓ Desactualización hardware/software

2. Se solicitó al jefe del departamento de sistemas los planes de mejoramiento de la seguridad de la información.

El Ing. José Barreiro mencionó que la falta de recursos limitó la realización de planes de mejoramiento, además, afirmó que con la pandemia COVID-19 la empresa tuvo que reducir su presupuesto dejando al departamento de sistemas como no prioritario.

3. Se solicitó al jefe del departamento de sistemas los inventarios de activos informáticos y su ubicación.

El jefe del departamento de sistemas mostró una hoja impresa de Excel, la cual no ha sido actualizada desde el año 2018, ante esto mencionó que los equipos no han sido actualizados desde dicho año. Luego de un recorrido por la finca se logró evidenciar que dos equipos fueron dados de baja y reemplazados por un computador, lo cual no se evidenció en la matriz de activos.

4. Se requirió al jefe del departamento de sistemas el plan de mantenimiento.

El departamento de sistemas mostró el plan anual realizado a inicios del año en curso el cual fue aprobado por Gerencia Técnica.

El cronograma de mantenimiento constaba de: la fecha, área, usuario a cargo y el procedimiento que se va a realizar. De igual manera, el cronograma se ajustaba a las temporadas altas en donde mencionó que los equipos deben estar en perfectas condiciones para no retrasar los procesos.

Se pudo verificar que el cronograma cumplía parcialmente, esto mediante las hojas de control firmadas por los usuarios a los que se realizó soporte técnico a los equipos.

4.1.2.2 Realización de la auditoría

Durante le reunión de apertura, se dio a conocer a todo el personal administrativo el calendario de actividades en donde se mostró las áreas a ser auditadas y las personas involucradas durante el proceso. De igual manera se detallaron los documentos que fueron requeridos para la auditoría.

Apertura de la auditoria

La reunión de apertura se llevó a cabo en las instalaciones de la florícola Galápagos Flores S.A a las 8h30am en donde se contó con la presencia del personal administrativo de las diferentes áreas.

Se presentó al equipo auditor, el objetivo y alcance de la auditoría, la normativa ISO 27001:2013 con los controles que fueron seleccionados para la revisión y la metodología con la que será ejecutada la auditoría. De igual manera se dio a conocer el cronograma

con el que se llevará a cabo y el personal involucrado. Así mismo, se dio a conocer los documentos que serán solicitados al área de sistemas los cuales son:

- Sistema de gestión de seguridad informática
- Inventario de activos informáticos
- Matriz de riesgo de Seguridad Informática
- Planes de mejoramiento de seguridad informática
- Procedimiento de asignación de credenciales a los usuarios
- Procedimiento de ingreso del personal a la empresa
- Procedimiento de generación de contraseñas
- Procedimiento de generación de Backups
- Procedimiento de manejo de discos extraíbles
- Procedimiento de control de acceso a internet
- Cronograma de mantenimiento de activos informáticos
- Reporte de mantenimiento de activos informáticos
- Hojas de vida de activos informáticos
- Compromiso de confidencialidad firmado por los funcionarios
- Actas de capacitación a los usuarios internos en Seguridad Informática

Finalizando la reunión de apertura se solventó todas las dudas expuestas por el personal.

Obtención de evidencias

A continuación, se realizó la clasificación de los activos de la información tomando en cuenta la categorización de la Tabla 12.

Tabla 11. Clasificación de activos de la información

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRITICIDAD
Información Restringida	A - Alta	1 - Alta	ALTA
Información Privada	M- Media	2 - Media	MEDIA
Información Pública	B- Baja	3 - Baja	BAJA
Información no publicada	No clasificada	4- No clasificada	

En base a lo mencionado en la “Tabla 12” se realizó la clasificación de los activos de información de la florícola.

Tabla 12 . Clasificación de activos de la información Galápagos Flores S.A

ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRITICIDAD
Documentos de Normatividad Institucional	Información Pública	Media	2	Media
Computadoras	Información Pública	Media	2	Media
Router	Información Restringida	Alta	1	Alta
Switch	Información Restringida	Alta	1	Alta
Servidor servicios web	Información Restringida	Alta	1	Alta
Servidor de aplicaciones	Información Restringida	Alta	1	Alta
Servidor sistema de Administración de Talento Humano	Información Privada	Alta	1	Alta
Servidor de base de datos	Información Restringida	Alta	1	Alta
Firewall	Información Restringida	Alta	1	Alta
Sistema Operativo Windows 10, Windows 8	Información Restringida	Media	2	Media
Sistema Integrado FINANCONTRY	Información Privada	Alta	1	Alta

Objetivos de control y controles ISO 27001:2013

A continuación, se describe la lista de cumplimiento de los dominios, objetivos y controles que permitió evaluar los riesgos y aplicar los controles necesarios para mitigarlos de acuerdo con la norma ISO 27001:2013.

ISO 27001:2013 GALÁPAGOS FLORES S.A					
OBJETIVOS DE CONTROL Y CONTROLES			**CUMPLE**		
			SI	**PARCIALMENT**	**NO**
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	**X**		
	Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	**x**		
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.			**X**
	Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.			**X**
		A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	**X**		
		A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.			**X**
		A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,			**X**
	A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	**X**		
	Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.		**X**	

A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1. Antes de asumir el empleo.	A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.			**X**
	Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	**x**		
	A.7.2. Durante la ejecución del empleo.	A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	**x**		
	Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	**x**		
		A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	**x**		
	A.7.3. Terminación y cambio de empleo.	A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	**x**		
	Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.				
	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.			**X**
	Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.	**x**		

		A.8.1.3. Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.			**X**
		A.8.1.4. Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	**x**		
	A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	**X**		
	Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.			**x**
		A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	**X**		
A.8. GESTIÓN DE ACTIVOS.	A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.		**X**	
	Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	**X**		
		A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.			**x**
	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	**x**		
	Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.			**x**

A.9. CONTROL DE ACCESO.	A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	**X**		
	Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	**X**		
		A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	**X**		
		A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.			**x**
		A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	**X**		
		A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	X		
	A.9.3. Responsabilidades de los usuarios.	A.9.3.1.Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.			**X**
	Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.				
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	**X**		
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.			**X**
		A.9.4.3. Sistema de Gestión de Contraseñas. Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.			**X**
		A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.			**X**

A.10. CRIPTOGRAFÍA	A.10.1. Controles Criptográficos.	A.10.1.1. Política sobre el uso de controles Criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.			**X**
	Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A.10.1.2. Gestión de Claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.			**X**
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1. Áreas Seguras.	A.11.1.1. Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	**X**		
	Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	**X**		
		A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	**X**		
		A.11.1.4. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.		**X**	
		A.11.1.5. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	**X**		
		A.11.1.6. Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	**X**		
	A.11.2. Equipos.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.			**x**
	Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.		**x**	
		A.11.2.3. Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.			**x**

		A.11.2.4. Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	x		
		A.11.2.5. Retiro de Activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	x		
		A.11.2.6. Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.			X
		A.11.2.7. Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reusó.	x		
		A.11.2.8. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.		X	
		A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.			x
	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.		X	
	Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.			X
		A.12.1.3. Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	x		
	A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.			X
	Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				
	A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	x		

A.12. SEGURIDAD DE LAS OPERACIONES.	Objetivo. Proteger contra la pérdida de datos.				
	A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.			**X**
	Objetivo. Registrar eventos y generar evidencia.	A.12.4.2. Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.			**x**
		A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	**x**		
		A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	**x**		
	A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.			**X**
	Objetivo. Asegurarse de la integridad de los sistemas operacionales.				
	A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	**x**		
	Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.			**x**
	A.12.7.1 Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.			**X**
	Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.				
	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.			**X**

A.13. SEGURIDAD DE LAS COMUNICACIONES.	Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.			**X**
		A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.			**X**
	A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.			**X**
	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.			**X**
		A.13.2.3. Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	**x**		
		A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	**x**		
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.			**X**
	Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	**x**		
		A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones sedebe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.	**x**		

	A.14.2. Seguridad en los procesos de desarrollo y de soporte.				
	Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.			
		A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.	**x**		
		A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.	**x**		
	A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	**x**		
	Objetivo. Asegurar la protección de los datos usados para ensayos.				
A.15. RELACIONES CON LOS PROVEEDORES.	A.15.1. Seguridad de la información en las relaciones con los proveedores.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.			**X**
	Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.			**X**
		A.15.1.3. Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.			**X**
	A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.			X
	Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos	A.15.2.2. Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.			**X**

	con los proveedores.				
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.			**X**
	Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	**x**		
		A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	**x**		
		A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.			**X**
		A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.			**X**
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	**x**		
		A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.			**X**
	A.17.1. Continuidad de seguridad	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.			**X**

	de la información				
	Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	A.17.1.2. Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.			**X**
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.			**X**
	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.			**X**
	Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.				
	A.18.1. Cumplimiento de requisitos legales y contractuales.	A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.		**X**	
	Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2. Derechos de Propiedad Intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.			**X**
		A.18.1.3. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	**x**		
A.18. CUMPLIMIENTO.		A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.		**X**	
		A.18.1.5. Reglamentación de Controles Criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos			**X**

	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	x		
	Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	A.18.2.2. Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.		X	
		A.18.2.3. Revisión del Cumplimiento Técnico. Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	X		

Figura 13 Check List ISO 27001:2013 Galápagos Flores S.A

Registro de las observaciones

Los hallazgos encontrados en la auditoria fueron revisados para determinar las conformidades y no conformidades

Tabla 13 Hallazgos de la auditoria

Objetivo de control	No Conformidad	Hallazgos de la auditoría
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1.1. Seguridad de la Información	• Dentro de la florícola, no se encuentran definidos roles de seguridad de la información • El área de sistemas solo cuenta con una persona que realizar las actividades.
	A.6.1.2. Separación de deberes.	• Dentro de la florícola, no se encuentran definidos roles de seguridad de la información • El área de sistemas solo cuenta con una

		persona que realizar las actividades.
	A.6.1.4. Contacto con grupos de interés especial.	• El departamento no cuenta con contactos de grupos de interés y tampoco se encuentra en foros de soporte técnico
	A.6.1.5. Seguridad de la información en Gestión de Proyectos.	• Los proyectos no cuentan con la seguridad de la información, es decir, no se pone en consideración los bloqueos de puertos, accesos libres, etc.
	A.6.2.2. Teletrabajo.	• No cuenta con políticas de confidenciales para realizar teletrabajo. • La conexión mantiene no restringe el acceso de la información ya que usan el programa Any Desk para una conexión remota.
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1.1. Selección.	• El área de sistemas no interviene en la selección del personal, es decir, no es un filtro en la seguridad en cuento a revisión de antecedentes penales, pruebas de polígrafo entre otras.
A.8. GESTIÓN DE ACTIVOS.	A.8.1.1. Inventario de Activos.	• No mantienen un inventario de activos de software, siendo este el mas importante en la

		seguridad de la información
	A.8.1.3. Uso Aceptable de los Activos.	• Activos sin documentación e identificación para el uso del personal.
	A.8.2.2. Etiquetado de la Información.	• No cuentan con un formato interno de etiquetado de la información.
	A.8.3.1. Gestión de medios de Soporte Removibles.	• Los medios de soporte removibles no son trasladados de manera segura con actas de salida. • No existe restricciones para acceder a estos medios
	A.8.3.3. Transferencia de medios de soporte físicos.	• Se encuentra al alcance del personal, no tiene restricciones. • No cuentan con políticas de uso para los medios de soporte físico
A.9. CONTROL DE ACCESO.	A.9.1.2. Acceso a redes y a servicios en red.	• El lugar físico no cuenta con un área restringida • Los equipos se encuentran expuestos a la manipulación del personal
	A.9.2.4. Gestión de información de autenticación secreta de usuarios.	• No existe un sustento formal donde especifique la confidencialidad del usuario con las contraseñas asignadas.
	A.9.3.1.Uso de información secreta.	• No cuenta con un proceso de gestión formal de la contraseña de seguridad, teniendo

		en cuenta que mantienen una caja fuerte.
	A.9.4.2. Procedimiento de Conexión Segura.	• No mantienen una política de conexión segura y tampoco se realiza revisiones de urls mediante herramientas de inspección
	A.9.4.3. Sistema de Gestión de Contraseñas.	• La generación de contraseñas se realiza de manera manual, es decir, es generada a conveniencia por el área de sistemas. • Las contraseñas de ingreso de dos usuarios son iguales. • El sistema integrado acepta contraseñas débiles
	A.9.4.4. Uso de programas utilitarios privilegiados	• No existe supervisión por parte del área de sistemas de los programas que los usuarios instalan.
A.10. CRIPTOGRAFÍA	A.10.1.1. Política sobre el uso de controles Criptográficos.	• No cuentan con una política interna para el uso de claves criptográficas.
	A.10.1.2. Gestión de Claves.	• No cuentan con una política interna para el uso de claves criptográficas.
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1.4. Protección contra amenazas externas y ambientales.	• El plan de contingencia se encuentra desactualizado desde el 2017 • Los UPS se encuentran deteriorados

		• La copia de seguridad de la información se encuentra dentro de la oficina
	A.11.2.1. Ubicación y protección de los equipos.	• El área de sistemas se encuentra dentro del financiero, por ende, los equipos tecnológicos se encuentran al alcance de todo el personal.
	A.11.2.3. Seguridad del cableado.	• El cableado se encuentra a la intemperie sin ninguna protección, existe cables de red cristalizados. • Los equipos de red se encuentran expuestos a la manipulación del personal.
	A.11.2.6. Seguridad de equipos y activos fuera del predio.	• Los equipos que trabajan fuera del predio no cuentan con actas de salida, actas de responsabilidad.
	A.11.2.9. Política de escritorio limpio y pantalla limpia.	• No cuentan con una política de escritorio limpio, es decir, los archivos no se encontraban organizados
A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1.2. Gestión de Cambios.	• Los cambios que se realizan dentro de la florícola a nivel operativo no consideran la seguridad de la información.
	A.12.2.1. Controles contra códigos maliciosos.	• Los equipos no cuentan con controles contra códigos maliciosos, por ejemplo, no cuentan con

		antivirus, bloqueos de pop-up en los navegadores.
	A.12.4.1. Registro de eventos.	• No cuentan con una bitácora de eventos para su posterior revisión.
	A.12.4.2. Protección de la información de registro.	• No existe un control del personal en las oficinas.
	A.12.5.1. Instalación de software en sistemas operativos.	• No mantienen un control de instalación de software, los usuarios pueden instalar programas sin supervisión.
	A.12.6.2. Restricciones sobre la instalación de Software.	• No mantienen un control de instalación de software, los usuarios pueden instalar programas sin supervisión.
	A.12.7.1. Controles sobre auditorías de Sistemas de Información.	• No mantienen un control sobre auditorias de sistemas de información, las auditorias registrados son sobre el medio ambiente
A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.1.1. Controles de redes.	• No mantiene una administración de la red, debido a que usan equipos que no son administrables.
	A.13.1.2. Seguridad de los servicios de red.	• No mantienen mecanismos de seguridad en la red, no existe firewall

	A.13.1.3. Separación en las redes.	• La topología de la red actual se encuentra en cascada, y no mantienen separaciones de la red por VLAN
	A.13.2.1. Políticas y procedimientos de transferencia de información.	• No existe políticas de transferencia de la información mediante la red, debido a que los equipos no soportan ese tipo de comunicación
	A.13.2.2. Acuerdos sobre transferencia de información.	• No existen políticas ni acuerdos para el intercambio de información con proveedores.
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	• En el desarrollo o compra de software a terceros, entre las cláusulas la información no cuenta con la debida seguridad, es decir, trabajan mediante puertos públicos y no privados.
A.15. RELACIONES CON LOS PROVEEDORES.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores.	• No existe una política para la seguridad de la información con los proveedores, es decir, cuando los proveedores realizan visitas a la finca, la misma no mantiene un control de las áreas en donde puede ingresar.
	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores.	• No mantiene acuerdos de seguridad de la información en

		ningún contrato con proveedores,
	A.15.1.3. Cadena de suministro de tecnología de información y comunicación.	• Las proformas presentadas por los proveedores aseguran el funcionamiento operativo de los equipos de hardware y de software, sin embargo, la seguridad de la información no es considerada.
	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores.	• La florícola no realiza un seguimiento a los proveedores tecnológicos, una vez concluido el contrato con el proveedor es archivado hasta la próxima compra.
	A.15.2.2. Gestión de cambios a los servicios de los proveedores.	• Al no mantener un seguimiento con los proveedores, tampoco tienen una gestión de cambios en cuanto a la seguridad de la información.
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1.1. Responsabilidades y procedimientos.	• Al ser solo una persona encargada del área de sistemas, no existen roles de responsabilidades para evitar los incidentes de la seguridad de la información
	A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	• No existe un registro de los eventos de la seguridad de la información, por

		ende, no existe una clasificación de riesgos.
	A.16.1.5. Respuesta a incidentes de seguridad de la información.	• El área de sistemas da respuesta a los incidentes de seguridad, sin embargo, no son documentados.
	A.16.1.7. Recolección de evidencia.	• No existen procedimientos para identificar, recolectar y preservar evidencia en cuanto a la seguridad de la información
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	A.17.1.1. Planificación de la continuidad de la seguridad de la información.	• El área de sistemas no cuanta con un plan de continuidad para la seguridad de la información.
	A.17.1.2.Implementación de la continuidad de la seguridad de la información.	• Al no contar con un plan de continuidad de la seguridad de la información, la florícola no ha realizado ninguna implementación
	A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	• Al no contar con un plan de continuidad de la seguridad de la información, la florícola no ha realizado ninguna implementación
	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información.	• Las instalaciones de la florícola en cuento al área de sistemas no son redundantes para cumplir con los requisitos de disponibilidad.
A.18. CUMPLIMIENTO	A.18.1.2. Derechos de Propiedad Intelectual.	• La florícola en cuanto al Sistema Operativo Windows 10 y el

		paquete de Office 2016 se encuentran activados con parches KMSPICO
	A.18.1.5. Reglamentación de Controles Criptográficos.	• La florícola no usa controles criptográficos.

Finalizada la selección se procedió a verificar los objetivos y controles que representan un riesgo en la seguridad de la información dentro de la florícola, los cuales se encuentran expuestos en la siguiente matriz.

		GRAVEDAD (IMPACTO)				
		MUY BAJO **1**	BAJO **2**	MEDIO **3**	ALTO **4**	MUY ALTO **5**
PROBABILIDAD	MUY ALTA **5**	5	10	15	20	25
	ALTA **4**	4	8	12	16	20
	MEDIA **3**	3	6	9	12	15
	BAJA **2**	2	4	6	8	12
	MUY BAJA **1**	1	2	3	4	5

Figura 14 Valoración de riesgo

En base a la clasificación que se muestra en la "Tabla 14" se procedió a realizar la matriz de riesgo en donde se enlista las no conformidades que fueron encontradas en el proceso de auditoría.

Objetivo de control	Riesgo	Probabilidad (Ocurrencia)	Gravedad (Impacto)	Valor de riesgo	Nivel de riesgo
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1.1. Personal no capacitado y con acceso a información critica	3	3	9	Importante

	A.6.1.2. Todo el personal tiene acceso a toda la información.	3	4	12	Importante
	A.6.1.4. La florícola no se encuentra a la vanguardia en cuanto a programas de producción	3	3	9	Importante
	A.6.1.5. Fuga de información.	4	5	20	Muy grave
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1.1. El personal ingresa sin la verificación previa de antecedentes.	2	3	6	Apreciable
A.8. GESTIÓN DE ACTIVOS.	A.8.1.1.Problemas de seguridad de propiedad intelectual y el incumplimiento de licencias.	5	5	25	Muy grave
	A.8.1.3.Problemas de seguridad de propiedad intelectual y el incumplimiento de licencias.	5	5	25	Muy grave
	A.8.2.2. Pérdida de información en las diferentes áreas.	4	5	20	Muy grave

	A.8.3.1. Perdida de los total o parcial Backups de la florícola	3	4	12	Importante
	A.8.3.3. Perdida de los equipos de soporte físico con información	3	5	15	Muy grave
A.9. CONTROL DE ACCESO.	A.9.1.2. Daños en el sistema de red	5	5	25	Muy grave
	A.9.2.4. Pérdida total o parcial de la información de autenticación secreta	3	4	12	Importante
	A.9.3.1 Robo o mal uso de la información confidencial de la florícola	4	5	20	Muy grave
	A.9.4.2. Descargas de virus que afecten el funcionamiento del equipo	4	4	16	Muy grave
	A.9.4.3. Contraseñas con bajos niveles de seguridad	4	4	16	Muy grave
	A.9.4.4.Programas que afecten las funcionalidades del equipo	4	4	16	Muy grave
A.10. CRIPTOGRAFÍA	A.10.1.1. La información crítica es de fácil acceso para el personal no autorizado.	3	3	9	Importante

	A.10.1.2. La información no se encuentra protegida	3	4	12	Importante
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1.4. Pérdida total o parcial de la información y equipos	4	5	20	Muy grave
	A.11.2.1. Fallas totales en el sistema de la florícola	5	5	25	Muy grave
	A.11.2.3. El proceso operativo fallaría totalmente	5	5	25	Muy grave
	A.11.2.6. Pérdida de información de los clientes de la florícola	4	5	20	Muy grave
	A.11.2.9. Daños en el equipo, fuga de información mediante los puertos USB	4	5	20	Muy grave
A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1.2. Pérdida total o parcial de la información	4	4	16	Muy grave
	A.12.2.1. Daños en los archivos, y equipos de computo	4	4	16	Muy grave
	A.12.4.1. Riesgos recurrentes sin solución	4	3	12	Importante

	A.12.4.2. Personal no autorizado puede manipular los equipos de administración	4	5	20	Muy grave
	A.12.5.1. Infección de los equipos de computo	4	4	16	Muy grave
	A.12.6.2. Los usuarios instalan programas que pueden ser perjudiciales para la finca	4	5	20	Muy grave
	A.12.7.1. La florícola no mantiene auditorias de seguridad de la información	4	5	20	Muy grave
A.13. SEGURIDAD DE LAS COMUNICACIONES	A.13.1.1. Vulnerables ante ataques cibernéticos	4	5	20	Muy grave
	A.13.1.2. Fuga de información	4	5	20	Muy grave
	A.13.1.3. Generación de cuellos de botella en la red	5	5	25	Muy grave
	A.13.2.1. Información vulnerable ante robos	4	5	20	Muy grave
	A.13.2.2. Robo de información total o parcial	4	5	20	Muy grave

A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1.1. Información expuesta a robo total o parcial. Ataques cibernéticos	4	5	20	Muy grave
A.15. RELACIONES CON LOS PROVEEDORES.	A.15.1.1. Libre acceso de la información a los proveedores	3	5	15	Muy grave
	A.15.1.2. Modificación de la información interna y critica de la florícola	4	5	20	Muy grave
	A.15.1.3. Los equipos pueden presentar fallas de seguridad, sin antivirus.	4	5	20	Muy grave
	A.15.2.1. Los proveedores oferten productos descontinuados.	3	5	15	Muy grave
	A.15.2.2. Los equipos no tendrían la garantía, las políticas de procedimientos podrían afectar la seguridad de la información	5	5	25	Muy grave

A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1.1. No se brinda respuesta a los incidentes de seguridad de la información	3	4	12	Importante
	A.16.1.4. Cualquier evento es considerado como incidentes de seguridad de la información.	3	4	12	Importante
	A.16.1.5. No se evalúa los eventos frecuentes de seguridad	4	5	20	Muy grave
	A.16.1.7. Aplicación de sanciones al personal equivocado.	4	4	16	Muy grave
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	A.17.1.1. Durante una crisis o desastres no tendrían información para mantenerse operativos	3	4	12	Importante
	A.17.1.2. La información no se encuentra disponible	3	4	12	Importante
	A.17.1.3. El sistema de seguridad de la información no ayudaría al área operativa de la florícola	3	4	12	Importante
	A.17.2.1. No garantiza la disponibilidad de las instalaciones del procesamiento de la información	4	4	16	Muy grave

A.18. CUMPLIMIENTO	A.18.1.2. Demandas de propiedad intelectual	4	5	20	Muy grave
	A.18.1.5. Llamados de atención de las autoridades pertinentes	4	5	20	Muy grave

Figura 15 Matriz de riesgo

Finalización de la auditoría

Una vez finalizado la verificación de los controles y objetivos de la normativa se obtiene el siguiente informe final de auditoría y plan de mitigación:

Informe final de auditoria

19 de julio de 2022

Auditoria de seguridad informática en la florícola Galápagos Flores S.A

Institución auditada

Galápagos Flores S.A

El proceso de auditoría de seguridad informática se llevó a cabo bajo la normativa ISO 27001:2013, en donde se evaluó los controles de seguridad en el área de sistemas de la florícola Galápagos Flores S.A, que tuvo inicio en febrero de 2022 y finalizo en julio de 2022.

La auditoría de seguridad informática fue desarrollada por Heidy Quishpe, egresada de la Carrera de Ingeniería en Ciencias de Computación de la Universidad Politécnica Estatal del Carchi, bajo el asesoramiento del Ing. Marco Yandún Msc, docente de la misma Carrera.

El proyecto de investigación se realizó con el apoyo de los interlocutores, Ing. José Antonio Sosa, Gerente Financiero y el Ing. José Barreiro, encargado del Área de Sistemas.

Para realizar la presente auditoria se solicitó la siguiente información al área involucrada en el proceso:

- Sistema de gestión de seguridad informática
- Inventario de activos informáticos
- Matriz de riesgo de Seguridad Informática
- Planes de mejoramiento de seguridad informática
- Procedimiento de asignación de credenciales a los usuarios
- Procedimiento de ingreso del personal a la empresa
- Procedimiento de generación de contraseñas
- Procedimiento de generación de Backups
- Procedimiento de manejo de discos extraíbles
- Procedimiento de control de acceso a internet
- Cronograma de mantenimiento de activos informáticos
- Reporte de mantenimiento de activos informáticos
- Hojas de vida de activos informáticos
- Compromiso de confidencialidad firmado por los funcionarios
- Actas de capacitación a los usuarios internos en Seguridad Informática

Capacidad del proceso de auditoria

Los procesos para evaluar fueron determinados con base en el estudio inicial de la auditoria. De 114 controles de la norma ISO 27001:2013, 106 fueron aplicados en el área de sistemas de florícola Galápagos Flores S.A. Se agruparon por cada objetivo y se estableció la capacidad del control.

De un total de 106 controles aplicables a la florícola al finalizar el proceso de auditoría se obtuvo los siguientes resultados: 48 conformidades, 51 no conformidades y 8 observaciones, las cuales se enlistan a continuación

Conformidades

- A.5.1.1. Políticas para la Seguridad de la Información. La florícola mantiene conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.
- A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información son revisadas y renovadas anualmente.
- A.6.1.3. Contacto con las autoridades. El personal mantiene un contacto ameno con los superiores.
- A.6.2.1. Política para dispositivos móviles. La empresa tiene una política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
- A.7.1.2. Términos y condiciones del empleo. La florícola mantiene las cláusulas en los contratos en donde especifica el uso correcto de la información.
- A.7.2.1. Responsabilidades de la Dirección. La Gerencia de la florícola exige a sus trabajadores cumplir con las cláusulas de los contratos, caso contrario serán sancionados con multas.
- A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Mantienen un cronograma de capacitaciones en donde es socializado las políticas de seguridad de la información, el cual es firmado por todo el personal y el encargado de impartir la capacitación.
- A.7.2.3. Proceso disciplinario. Se emplea una sanción monetaria y a su vez un memo a su hoja de vida el cual es firmado por el trabajador.
- A.7.3.1. Terminación o cambio de responsabilidades de empleo. Al momento de que el personal es cambiado de área o finalizado su contrato, la florícola realiza el proceso formal de salida en donde el usuario entrega formalmente las credenciales de acceso al equipo, sistema, correo electrónico.
- A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario son propios de la florícola.
- A.8.1.4. Devolución de Activos. Los empleados y usuarios de partes externas entregan los activos que se encuentran a su cargo, esto es registrado en actas de entrega.

- A.8.2.1. Clasificación de la Información. La florícola mantiene una clasificación de la información.
- A.8.2.3. Manejo de Activos. De acuerdo con la organización interna de la empresa, el personal maneja los activos de su área correspondiente.
- A.8.3.2. Disposición de los medios de soporte. Los medios de soporte físico para ser utilizados son entregados con actas y una vez finalizado su uso es devuelto con un acta formal.
- A.9.1.1. Política de Control de Acceso. La florícola documenta y revisa la política de control de acceso con base en los requisitos del negocio
- A.9.2.1. Registro y cancelación del registro de usuarios. Para agregar o dar de baja a un usuario, es realizado mediante un proceso formal en donde firma el usuario y el área de sistemas.
- A.9.2.2. Suministro de acceso de usuarios. La empresa mantiene un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
- A.9.2.3. Gestión de derechos de acceso privilegiado. Mediante actas restringe y controlar la asignación y uso de derechos de acceso privilegiado.
- A.9.2.5. Revisión de los derechos de acceso de usuarios. Los usuarios revisan los derechos de acceso en intervalos de dos meses.
- A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información se cancelan al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios, todo esto queda documentado en las actas de usuario.
- A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones es restringido de acuerdo con la política de control de acceso.
- A.11.1.1. Perímetro de Seguridad Física. Se encuentra definido el perímetro de seguridad, en las áreas que contienen información confidencial.
- A.11.1.2. Controles Físicos de entrada. Las áreas de ingreso se encuentran protegidas con cámaras de seguridad.
- A.11.1.3. Seguridad de oficinas, salones e instalaciones. La florícola aplica la seguridad física a oficinas, salones e instalaciones esto mediante las cámaras que se encuentran en el área de sistemas, las cuales son revisadas diariamente.

- A.11.1.5. Trabajo en áreas seguras. Mantienen procedimientos para trabajo en áreas seguras, como, por ejemplo, el personal externo siempre debe trabajar bajo la supervisión de un encargado de la florícola.
- A.11.1.6. Áreas de despacho y carga. Controlan los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas.
- A.11.2.4. Mantenimiento de equipos. Los equipos reciben mantenimiento técnico según la planificación presentada por el área de sistemas, la cual es aprobada por gerencia antes de ser ejecutado el cronograma.
- A.11.2.5. Retiro de Activos. Los equipos, información o software no son retirados de su sitio sin autorización previa, para realizar algún cambio se debe realizar una solicitud y si la misma es aprobada se realizan las modificaciones.
- A.11.2.7. Disposición segura o reutilización de equipos. Mediante el soporte técnico que es realizado según la planificación, de igual manera se revisa la viabilidad de las piezas de los equipos y verificación en general del equipo.
- A.12.1.3. Gestión de Capacidad. Se realiza un seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
- A.12.3.1. Copias de respaldo de la información. Se realiza copias de respaldo de la información, software e imágenes de los sistemas.
- A.12.4.3. Registros del administrador y del operador. Las actividades del área de sistemas son registradas y revisadas con regularidad.
- A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información se encuentran sincronizados con una única fuente de referencia de tiempo.
- A.12.6.1. Gestión de las vulnerabilidades técnicas. Obtienen oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información mediante reportes enviados por cada área.
- A.13.2.3. Mensajes electrónicos. Mantienen una configuración de bloqueo de spam en los mensajes electrónicos.
- A.13.2.4. Acuerdos de confidencialidad o de no divulgación. La florícola, revisa regularmente y documentar los requisitos para los acuerdos de confidencialidad o no

divulgación que reflejen las necesidades de la organización para la protección de la información.

- A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes es protegida de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
- A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones es protegida mediante el control del servidor al momento de recibir la información.
- A.14.2.7. Desarrollo contratado externamente. La florícola supervisa y realiza un seguimiento de la actividad de desarrollo de sistemas contratado.
- A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo la florícola lleva a cabo ensayos de funcionalidad de la seguridad.
- A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones realiza un cronograma para programas de ensayo y criterios relacionados.
- A.14.3.1. Protección de datos de ensayo. Los datos de ensayo son seleccionados cuidadosamente para no sufrir perdidas de información.
- A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información son informados mediante actas.
- A.16.1.3. Informe de debilidades de seguridad de la información. Se mantiene una bitácora de quejas o errores que presenta el equipo, la red o el sistema, el cual es revisado mensualmente por el área.
- A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. Mediante la revisión de la bitácora el área se encuentra en desarrollo de planes de solución para que los mismo ya no sean recurrentes.
- A.18.1.3. Protección de registros. Los registros se encuentran protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, mediante respaldos en la nube y backup en discos externos.
- A.18.2.1. Revisión independiente de la seguridad de la información. Cuando la finca presenta un cambio significativo, se realiza una inspección general, en donde se verifica si la información se encuentra segura.

- A.18.2.3. Revisión del Cumplimiento Técnico. Los sistemas informáticos cumplen un procedimiento de revisión con gerencia para determinar si son óptimos para la florícola.

No conformidades

- A.6.1.1. Seguridad de la Información Roles y Responsabilidades. La florícola no cuenta con la definición de roles y responsabilidades para la seguridad de la información.
- A.6.1.2. Separación de deberes. La empresa no realiza la separación de deberes por área, es decir, el personal de talento humano puede realizar actividades de contabilidad.
- A.6.1.4. Contacto con grupos de interés especial. El área de sistemas de florícola no mantiene relación con los equipos de soporte técnico de las empresas que se encuentran en el cantón, además el encargado del área de sistemas no ha realizado cursos de actualizaciones tecnológicas.
- A.6.1.5. Seguridad de la información en Gestión de Proyectos. En el proceso para gestión de proyectos, no se toma en cuenta la seguridad de la información en cuanto a verificación de puertos, servidores.
- A.7.1.1. Selección. El área de sistemas no es un filtro para la selección del personal en cuento a revisión de antecedentes.
- A.8.1.1. Inventario de Activos. No cuentan con un inventario de activos de la información.
- A.8.1.3. Uso Aceptable de los Activos. No determinan reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
- A.8.2.2. Etiquetado de la Información. No cuentan con un proceso formal de etiquetado de la información.
- A.8.3.1. Gestión de medios de Soporte Removibles. El área de sistemas no mantiene un proceso formal para el traslado de medios de soporte removibles, es decir, cualquier usuario puede tener acceso.
- A.8.3.3. Transferencia de medios de soporte físicos. El área de sistemas no mantiene un proceso formal para el traslado de medios de soporte removibles, es decir, cualquier usuario puede tener acceso.

- A.9.1.2. Acceso a redes y a servicios en red. No cuentan con restricción de usuarios, es decir, el personal puede ingresar y manipular los equipos de red.
- A.9.2.4. Gestión de información de autenticación secreta de usuarios. La información crítica de la florícola no es controlada mediante un proceso formal, todos los usuarios tienen acceso.
- A.9.3.1.Uso de información secreta. No cuentan con prácticas para el manejo de información secreta.
- A.9.4.2. Procedimiento de Conexión Segura. No cuentan con políticas de conexión segura. De igual manera, no mantienen controles de verificación de conexión.
- A.9.4.3. Sistema de Gestión de Contraseñas. La generación de contraseñas es realizada de manera empírica, no utilizan ningún sistema para la generación.
- A.9.4.4. Uso de programas utilitarios privilegiados. No existen restricciones del uso de programas privilegiados, todos los usuarios tienen acceso.
- A.9.4.5. Control de Acceso a Códigos Fuente de Programas. La florícola no mantiene controles de verificación de ingreso a códigos fuente.
- A.10.1.1. Política sobre el uso de controles Criptográficos. No cuentan con controles criptográficos.
- A.10.1.2. Gestión de Claves. No cuentan con controles criptográficos.
- A.11.2.1. Ubicación y protección de los equipos. Los equipos no se encuentran ubicados los lugares seguros para su funcionamiento, se encuentran expuestos a manipulación de cualquier usuario.
- A.11.2.3. Seguridad del cableado. El cableado de potencia no se encuentra separado del cableado de datos, además, los cables se encuentran expuestos a manipulación ya que se encuentran sin protección.
- A.11.2.6. Seguridad de equipos y activos fuera del predio. No mantienen controles de seguridad para los equipos que salen de la florícola
- A.11.2.9. Política de escritorio limpio y pantalla limpia. No cuentan con una política de escritorio limpio para los papeles y medios de almacenamiento removibles
- A.12.1.2. Gestión de Cambios. No existe un control de cambios en los sistemas de procesamiento de información que afectan la seguridad de la información.
- A.12.2.1. Controles contra códigos maliciosos. Los antivirus se encuentran con licencias caducadas en todos los equipos.

- A.12.4.1. Registro de eventos. No existe un registro de eventos dentro del área de sistemas.
- A.12.4.2. Protección de la información de registro. No existe restricciones a los usuarios no autorizados.
- A.12.5.1. Instalación de software en sistemas operativos. No existen procedimientos para controlar la instalación de software en sistemas operativos.
- A.12.6.2. Restricciones sobre la instalación de Software. No existe un reglamento de instalación de software por parte de los usuarios.
- A.12.7.1. Controles sobre auditorías de Sistemas de Información. La florícola no ha mantenido auditorías de los sistemas de la información.
- A.13.1.1. Controles de redes. No cuentan con un control de la red, no son administrables debido a que tienen equipos obsoletos.
- A.13.1.2. Seguridad de los servicios de red. No cuentan con mecanismos de seguridad, no tienen firewall, es decir, toda la información se encuentra expuesta.
- A.13.1.3. Separación en las redes. No cuenta con una segmentación de las redes por áreas de trabajo.
- A.13.2.1. Políticas y procedimientos de transferencia de información. No cuentas con políticas, procedimientos y controles de transferencia para proteger la transferencia de información, debido a que no cuentan con firewall y segmentación de la red.
- A.13.2.2. Acuerdos sobre transferencia de información. No cuentan con acuerdos para la transferencia segura de información entre la florícola y las partes externas.
- A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. No incluyen los requerimientos de seguridad en las nuevas compras de equipos tecnológicos.
- A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. No cuentan con una política de seguridad de la información con proveedores para mitigar los riesgos de pérdida de información.
- A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. No tienen establecidos requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
- A.15.1.3. Cadena de suministro de tecnología de información y comunicación. No existe acuerdos con proveedores donde incluyan los requisitos para tratar los riesgos

de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

- A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. La florícola no realiza seguimientos a la prestación de servicios de los proveedores.
- A.15.2.2. Gestión de cambios a los servicios de los proveedores. La empresa no gestiona los cambios en el suministro de servicios por parte de los proveedores donde incluya el mantenimiento y controles de seguridad de la información.
- A.16.1.1. Responsabilidades y procedimientos. No se encuentran establecidas las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
- A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información no se evalúan.
- A.16.1.5. Respuesta a incidentes de seguridad de la información. El departamento de sistemas no da respuesta s a los incidentes de seguridad, debido a que los mismos no se encuentran documentados.
- A.16.1.7. Recolección de evidencia. El área de sistemas no define procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
- A.17.1.1. Planificación de la continuidad de la seguridad de la información. El área no determina los requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información.
- A.17.1.2. Implementación de la continuidad de la seguridad de la información. No procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación de riesgo.
- A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. No cuentan con controles de continuidad de la seguridad de la información.
- A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. El área de sistemas no cuenta con un área específica para la adquisición de nuevos equipos que mejoren el funcionamientos de los procesos.
- A.18.1.2. Derechos de Propiedad Intelectual. No mantiene procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de

reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.

- A.18.1.5. Reglamentación de Controles Criptográficos. No cuentan con controles criptográficos

Observaciones

- A.6.2.2. Teletrabajo. Implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

  La política cumple parcialmente debido a que mantienen restricciones con dispositivos móviles, pero en cuanto al procesamiento de la información mediante teletrabajo no se registran políticas
- A.11.1.4. Protección contra amenazas externas y ambientales. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

  Al no contar con un firewall la florícola se encuentra expuesta al robo de información.
- A.11.2.2. Servicios Públicos de soporte. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.

  No todos los equipos de la florícola cuentan con UPS de respaldo.
- A.11.2.8. Equipos sin supervisión de los usuarios. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.

El encargado de cada equipo mantiene su contraseña, sin embargo, en la pantalla muestra el inicio de su contraseña.

- A.12.1.1. Procedimientos de operación documentadas. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.

  Los procesos realizados por el área de sistemas son realizados, sin embargo, los que no se encuentran dentro de la planificación no se encuentran documentados, por ejemplo, cambio de disco al equipo de contabilidad, no se encuentra un registro del mismo.

- A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

  La florícola mantiene la política de privacidad y protección de información personal pero el personal no tiene conocimiento de esta.
- A.18.2.2. Cumplimiento con las políticas y normas de seguridad. . Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.

  Los jefes de cada departamento no revisan o diseñan las políticas, el jefe de seguridad es quien determina las políticas generales de seguridad.

Recomendaciones a los hallazgos

Para concluir con el proceso de auditoría, se recomienda lo siguiente:

- A.6.1.1. Se recomienda definir las responsabilidades de la seguridad de la información.
- A.6.1.2. Se sugiere separar las tareas y áreas de responsabilidad en conflicto para reducir las posibilidades de modificación no autorizada o no intencional el uso indebido de los activos de la organización.
- A.6.1.4. Se recomienda mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
- A.6.1.5. Se sugiere tratar en la gestión de proyectos la seguridad de la información independiente del tipo de proyecto.
- A.7.1.1. Se recomienda incorporar al área de sistemas como un filtro en la contratación del personal, para la revisión de antecedentes y de ser posible las pruebas de polígrafo.
- A.8.1.1. Se recomienda identificar los activos asociados con información e instalaciones de procesamiento de información y elaborar un inventario de estos activos.

- A.8.1.3. Se recomienda identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
- A.8.2.2. Se sugiere desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
- A.8.3.1. Se sugiere implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
- A.8.3.3. Los medios que contienen información se sugieren proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
- A.9.1.2. Se recomienda permitir el acceso a la red y a los servicios de red solo a los usuarios autorizados.
- A.9.2.4. La asignación de información de autenticación secreta se recomienda controlar por medio de un procedimiento de gestión formal.
- A.9.3.1. Se debe recomienda a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
- A.9.4.2. Se recomienda mantener un proceso de conexión segura cuando se realice el ingreso a sistemas y aplicaciones.
- A.9.4.3.Para los sistemas de gestión de contraseñas se recomienda que sean interactivos y deben asegurar contraseñas de calidad.
- A.9.4.4. Se recomienda restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
- A.9.4.5. Se sugiere restringir el acceso a códigos fuente de programas.
- A.10.1.1. Se recomienda desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.
- A.10.1.2. Se sugiere desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.
- A.11.2.1. Se recomienda mantener a los equipos ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.

- A.11.2.3. El cableado de potencia y de telecomunicaciones se recomienda proteger contra interceptaciones, interferencia o daño.
- A.11.2.6. Se sugiere aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización.
- A.11.2.9. Se recomienda adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.
- A.12.1.2. Se sugiere controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
- A.12.2.1. Se recomienda implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
- A.12.4.1. Se recomienda elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.
- A.12.4.2. Se recomienda proteger las instalaciones y la información de registro contra alteración y acceso no autorizado.
- A.12.5.1. Se recomienda implementar procedimientos para controlar la instalación de software en sistemas operativos.
- A.12.6.2. Se sugiere establecer e implementar el reglamento de instalación de software por parte de los usuarios.
- A.12.7.1. Se recomienda gestionar procesos de auditoría de seguridad de la información para mantener los controles más eficientes
- A.13.1.1. Se recomienda gestionar y controlar las redes para proteger la información en sistemas y aplicaciones.
- A.13.1.2. Se sugiere identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios.
- A.13.1.3. Se recomienda separar en las redes por grupos de servicios de información, usuarios y sistemas de información.

- A.13.2.1. Se recomienda contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.
- A.13.2.2. Se recomienda realizar acuerdos de transferencia segura de información del negocio entre la organización y las partes externas.
- A.14.1.1. Los requisitos relacionados con seguridad de la información se sugieren incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
- A.15.1.1. Se recomienda acordar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización.
- A.15.1.2. Se sugiere establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
- A.15.1.3. Se recomienda incluir en los acuerdos con los proveedores requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
- A.15.2.1. Se recomienda al florícola hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
- A.15.2.2. Se sugiere gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.
- A.16.1.1. Se recomienda establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
- A.16.1.4. Se recomienda evaluar los eventos de seguridad de la información y decidir si se van a clasificar como incidentes de seguridad de la información.
- A.16.1.5. Se sugiere dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

- A.16.1.7. Se recomienda a la empresa definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
- A.17.1.1. Se sugiere a la empresa determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas.
- A.17.1.2. Se sugiere a la florícola establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
- A.17.1.3. Se recomienda a la empresa verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.
- A.17.2.1. Las instalaciones de procesamiento de información se sugieren implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
- A.18.1.2. Se recomienda implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.
- A.18.1.5. Se sugiere usar controles criptográficos, en cumplimiento de todos los acuerdos

Plan de mitigación

PLAN DE MITIGACIÓN

Objetivo.

Mitigar los riesgos identificados en el proceso de auditoria basada en la norma ISO 27001:2013 con la finalidad de disminuir el impacto provocado por los incidentes del área de sistemas en la florícola Galápagos Flores S.A.

Periodo auditoría. Marzo 2021 - Julio 2022

Equipo auditor.

Auditor Heidy Selena Quishpe Pillajo

Asesor Ing. Marco Antonio Yandún Velasteguí, MSc.

Con la valoración generada por la matriz, se procede a listar los riesgos desde los más altos hasta los más bajos. Se realiza con el fin de emitir las estrategias de mitigación:

VALORACIÓN DE RIESGO

		GRAVEDAD (IMPACTO)				
		MUY BAJO **1**	BAJO **2**	MEDIO **3**	ALTO **4**	MUY ALTO **5**
PROBABILIDAD	MUY ALTA **5**	5	10	15	20	25
	ALTA **4**	4	8	12	16	20
	MEDIA **3**	3	6	9	12	15
	BAJA **2**	2	4	6	8	12
	MUY BAJA **1**	1	2	3	4	5

Figura 16 Valoración de riesgos

Situación de riesgo	Riesgo	Estrategias de mitigación
A.6.1.1. Personal no capacitado y con acceso a información critica	Importante	• Definir responsabilidades a cada empleado o puesto de trabajo en relación con la seguridad de la información • Contratación de personal capacitado para la designación de roles de seguridad de la información
A.6.1.2. Todo el personal tiene acceso a toda la información.	Importante	• Determinar los procesos y responsabilidades de cada área de trabajo según la organización estructural interna • Separar las funciones de petición y concesión de permisos administrativos de acceso a sistemas evitando que la misma persona se conceda las autorizaciones
A.6.1.4. La florícola no se encuentra a la vanguardia en cuanto a programas de producción	Importante	• Ingreso a foros gratuitos de interés tecnológico. • Comunicación con la red del personal de sistemas del cantón Pedro Moncayo. • Comunicación con los proveedores de equipos, para mantenerse a la vanguardia en tecnología
A.6.1.5. Fuga de información.	Muy grave	• Establecer una política de seguridad de la información en la gestión de proyectos. • Mejorar la evaluación de costes de proyectos considerando los riesgos que no fueron evaluados.
A.7.1.1. El personal ingresa sin la verificación previa de antecedentes.	Apreciable	• Establecer al departamento de sistemas como un filtro en el proceso de ingreso al personal. • Verificación de antecedentes penales, pruebas de polígrafo.
A.8.1.1.Problemas de seguridad de propiedad intelectual	Muy grave	• Realizar la clasificación de activos que permita identificar el tipo de activo al que corresponde. Ejemplo, Activo de soporte técnico, Activo de software, etc • Determinar en la clasificación de activos la información detallada de cómo realizar un inventario de activos,

y el incumplimiento de licencias.		
A.8.1.3.Problemas de seguridad de propiedad intelectual y el incumplimiento de licencias.	Muy grave	• Documentar el uso apropiado de la información describiendo los requisitos de seguridad • Comunicar al personal las medidas a tomar por difamación, acoso, suplantación de identidad y compras no autorizadas.
A.8.2.2. Pérdida de información en las diferentes áreas.	Muy grave	• Determinar un sistema de etiquetado de la información según su organización estructural interna, por ejemplo, en el área de contabilidad AC-CONT-001 • El etiquetado puede realizarse de manera física o por medio de metadatos
A.8.3.1. Pérdida de los total o parcial Backups de la florícola	Importante	• Mantener un registro de los soportes extraíbles en la entrada y salida de finca • Renovación de los dispositivos mediante un periodo determinado para evitar la duplicidad de los datos Documentar los procedimientos para los cuales son usados los soportes extraíbles
A.8.3.3. Pérdida de los equipos de soporte físico con información	Muy grave	• Al trasladar un medio de soporte físico debe ser llevado con actas de responsabilidad en donde se registre la hora de salida y llegada, persona a carga y el tipo de información que se encontraba en el dispositivo.
A.9.1.2. Daños en el sistema de red	Muy grave	• Disponer de guardianía en el acceso al área administrativa para realizar los controles de ingreso al personal. • Restringir el acceso físico en horas no laborables. • Contratación del personal capacitado en seguridad del personal (Guardias)

A.9.2.4. Pérdida total o parcial de la información de autenticación secreta	Importante	• Incluir cláusulas en contratos y condiciones de puesto de trabajo sobre el mantenimiento del secreto de las contraseñas o información de autenticación • Identificar al usuario antes de entregar las contraseñas y obtener acuse de recibo • Uso de contraseñas seguras, no compartidas • Cambiar contraseñas a personal externo después de que han realizado sus trabajos
A.9.3.1 Robo o mal uso de la información confidencial de la florícola	Muy grave	• Evitar el uso de registros de contraseñas (papel, archivos etc.) • Políticas para cambiar las contraseñas ante amenazas • Políticas para la calidad de las contraseñas • Evitar el almacenamiento de contraseña
A.9.4.2. Descargas de virus que afecten el funcionamiento del equipo	Muy grave	• El procedimiento de inicio de sesión no debe mostrar los identificadores del sistema o de la aplicación hasta que el inicio de sesión haya tenido éxito. • Las sesiones inactivas deben ser dependientes del tiempo, cerradas después de un cierto tiempo o un cierto tiempo inactivo. • Determinar políticas de conexión segura
A.9.4.3. Contraseñas con bajos niveles de seguridad	Muy grave	• Determinar que el sistema interno de la florícola rechace contraseñas débiles. • Establecer cambios de contraseñas de forma periódica, además de registrar todas las contraseñas y rechazar contraseñas similares utilizadas anteriormente. • Se recomienda el uso de generadores de contraseñas seguras open source como KeeperSecurity, LastPass
A.9.4.4.Programas que afecten las funcionalidades del equipo	Muy grave	• Los programas con funciones privilegiadas deberían requerir autenticación por separado y estar segregados de las aplicaciones del sistema. • Todas las actividades deben registrarse. Se debe considerar nuevamente la segregación de funciones cuando sea posible.

A.10.1.1. La información crítica es de fácil acceso para el personal no autorizado.	Importante	• Determinar una política de implementación y administración de claves de cifrado de datos. • Identificar a un responsable de la política para su implementación y administración.
A.10.1.2. La información no se encuentra protegida	Importante	• Los medios de cifrado implican mantener una gestión de claves criptográficas utilizadas por los medios de cifrado. • La gestión de claves implica tener en cuenta políticas que tengan en cuenta el ciclo de vida completo: generación, uso y protección, distribución y finalmente la renovación o destrucción
A.11.1.4. Pérdida total o parcial de la información y equipos	Muy grave	• Se debe considerar, diseñar y aplicar la protección física contra factores externos. • Desarrollo de “Planes de Continuidad del Negocio” y de “Recuperación ante desastres”
A.11.2.1. Fallas totales en el sistema de la florícola	Muy grave	• Controles para proteger los equipos de daños ambientales y accesos no autorizados • Medidas de protección contra daños eléctricos (fuentes de alimentación reguladas, líneas de alimentación separadas y respaldadas etc.) • Control medioambiental para cumplir con las especificaciones del fabricante en cuanto a condiciones de humedad, temperatura protección contra polvo o materiales que puedan dañar los equipos
A.11.2.3. El proceso operativo fallaría totalmente	Muy grave	• Los cables deben estar bajo tierra hasta el punto de acceso dentro de la instalación • Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencias. • Los puntos de acceso del cableado a los equipos o a las salas deben asegurarse según corresponda y los cables deben estar protegidos. El cableado alrededor de las salas de servidores y centros de datos debería estar aislado de forma segura para evitar la conexión de dispositivos no autorizados.

A.11.2.6. Pérdida de información de los clientes de la florícola	Muy grave	• Mantener un registro de la custodia de los activos que abandonan la organización y realice evaluaciones de riesgo para instalaciones donde serán utilizados
A.11.2.9. Daños en el equipo, fuga de información mediante los puertos USB	Muy grave	• Las pantallas no deben mostrar información cuando el equipo no esté en uso y los escritorios deben estar libres de papeles cuando no estén en uso o desatendidos. • Dependiendo de la clasificación de los documentos en papel y la cultura de la organización, el papel y los medios extraíbles deben asegurarse según la política cuando no estén en uso.
A.12.1.2. Pérdida total o parcial de la información	Muy grave	• Establecer una planificación para los cambios a realizar en equipos, sistemas software etc. Acompañado de pruebas realizadas y comunicaciones a todos los involucrados. • Mantener un registro que contenga al menos la información de: Quien autoriza los cambios, Quien realiza los cambios, Fecha, Descripción de las tareas, Validación del cambio.
A.12.2.1. Daños en los archivos, y equipos de computo	Muy grave	• Disponer de sistemas de detección de código malicioso en los servidores y en los puestos de trabajo. • Establecer un procedimiento de seguridad dirigido a los usuarios para que conozcan sus obligaciones respecto a la seguridad de la información y evitar que abran archivos adjuntos sin asegurarse de que no sean maliciosos • Poner en la lista negra sitios conocidos o restringir el uso de internet en los puestos de trabajo si no es necesario para el desempeño de sus funciones.
A.12.4.1. Riesgos recurrentes sin solución	Importante	• Mantener un registro de los eventos donde se determine qué estaba sucediendo mediante los datos de la hora, la fecha del incidente, etc., las personas involucradas, el origen y las causas, etc. • Revisar los registros de forma periódica, independientemente de si hay un incidente o no puede ayudar a analizar tendencias, detectar potenciales actividades fraudulentas, o detectar el origen de fallos de funcionamiento, antes de que ocurran incidentes importantes.
A.12.4.2. Personal no autorizado puede manipular los equipos de administración	Muy grave	• Los registros de eventos deben tener el nivel de protección apropiado para evitar pérdidas, corrupción o cambios no autorizados. • El administrador del sistema no debe tener permiso para borrar o desactivar el registro de sus propias actividades.

A.12.5.1. Infección de los equipos de computo	Muy grave	• Probar las nuevas aplicaciones o software en entornos aislados especialmente preparados para prueba • Comprobar las necesidades de instalación (compatibilidad del entorno) antes de su instalación • Establecer procedimientos o herramientas de monitoreo del software para detectar cambios no autorizados
A.12.6.2. Los usuarios instalan programas que pueden ser perjudiciales para la finca	Muy grave	. • La instalación de software debe realizarse por personal autorizado y con la capacitación adecuada • Definir reglas concisas para limitar la capacidad de los usuarios finales, como, por ejemplo: Qué tipos de instalaciones de software son las permitidas a los usuarios finales (por ejemplo, actualizaciones y parches de seguridad al software existente), Qué tipos de instalaciones se encuentran prohibidas (por ejemplo, software que es sólo para uso personal y software cuyo origen pueda ser potencialmente dañino etc.
A.12.7.1. La florícola no mantiene auditorias de seguridad de la información	Muy grave	• Asignar responsabilidades dentro del equipo de gestión y que se siguen una serie de procedimientos establecido. • Los principales elementos para gestionar dentro de una red son los elementos físicos que dan soporte a la red y sobre todo los que nos interconectan con el exterior (routers, switch, etc.). • Considerar controles adicionales para mantener las conexiones (disponibilidad) y la privacidad (confidencialidad) y la integridad de los datos.
A.13.1.1. Vulnerables ante ataques cibernéticos	Muy grave	• Los principales elementos para gestionar dentro de una red son los elementos físicos que dan soporte a la red y sobre todo los que nos interconectan con el exterior (routers, switch, etc.). • Implementación del firewall con reglas de seguridad y bloqueos de puertos.
A.13.1.2. Fuga de información	Muy grave	• Aplicarlos criterios de cómo están siendo monitoreados los activos de información, cuál es su evaluación de riesgos y los controles que deberemos aplicar para abordar nuestras vulnerabilidades técnicas. • Realizar separaciones de red mediante VLAN en donde cada departamento se encuentre separado, de esta manera no existirá una mezcla de información en los departamentos.
A.13.1.3. Generación de cuellos de botella en la red	Muy grave	• Definir procedimientos y políticas para proteger la información que se va a transmitir donde se tenga en cuenta los aspectos como: los medios de transmisión, las redes, los soportes informáticos, los soportes documentales, Etc.

		• Las medidas de seguridad deberán definirse en función de la naturaleza del remitente, el destinatario y los soportes utilizados. • Las políticas y los procedimientos deben incluir requisitos para la protección contra intercepción, copia, modificación, dirección incorrecta o destrucción.
A.13.2.1. Información vulnerable ante robos	Muy grave	• Deben existir acuerdos entre las partes de intercambio de información para garantizar tanto el uso que se le va a dar a la información como los niveles de protección. • Los acuerdos deben tratar puntos como: La responsabilidad de las partes en el uso y protección y custodia de la información, la trazabilidad de los datos, el cumplimiento de las normas técnicas y legales, los requisitos de cifrado
A.13.2.2. Robo de información total o parcial	Muy grave	• Incluir requisitos para la seguridad de la información en la fase de especificación de condiciones para sistemas de información. • Prever requisitos de seguridad en las fases tempranas de un desarrollo es el ahorro de costes ya que un rediseño puede ser mucho más costoso sin contar con los daños potenciales de los fallos no previstos en la seguridad • Controles de seguridad debemos considerar en una especificación: ¿Qué nivel de confianza requiere la aplicación?, ¿Qué funciones y responsabilidades requiere de los usuarios?, ¿Qué necesidades de protección tienen los activos involucrados?, ¿Qué requisitos de seguridad se derivan de los procesos del negocio? • A la hora de integrar un software en aplicaciones o sistemas propios considerar si es necesario configurar las aplicaciones, sistemas y Software a implantar en relación a la seguridad. Elabore procedimientos y asegúrese de que se implementan
A.14.1.1. Información expuesta a robo total o parcial. Ataques cibernéticos	Muy grave	• Las condiciones de seguridad deben ser acordadas con el proveedor antes de firmar los contratos y debe quedar documentada si es necesario en los anexos oportunos. • Subcontratar servicios de información tiene muchos beneficios hoy en día para la empresa como la reducción de costes la mayor flexibilidad etc.

A.15.1.1. Libre acceso de la información a los proveedores	Muy grave	• Las condiciones de seguridad de la información deben quedar reflejadas en los contratos de forma explícita y en un apartado específico para ello. • Los documentos sobre los acuerdos para la seguridad de la información deben estar firmados por ambas partes.
A.15.1.2. Modificación de la información interna y critica de la florícola	Muy grave	• Establecer los criterios de seguridad para cada servicio, producto o tecnología de comunicación a subcontratar. La evaluación de riesgos enfocada a un servicio o producto en concreto, nos puede ayudar a establecer los criterios a la hora de subcontratar este servicio y determinar qué características o nivel de seguridad requiere a la hora de elegir al contratista. • Establecer clausulas para el subcontratista en cuanto a que apliquen requisitos de seguridad a sus proveedores y a toda la cadena de suministro. • Establecer procesos para comprobar que los productos o servicios suministrados cumplen con los requisitos establecidos para la seguridad de la información al menos para los productos y servicios que se determine como fundamentales y que son adquiridos fuera de la organización.
A.15.1.3. Los equipos pueden presentar fallas de seguridad, sin antivirus.	Muy grave	• Establecer mecanismos de monitorización de los servicios proporcionados por terceros y además solicitar los informes al proveedor sobre el nivel de servicio prestado.
A.15.2.1. Los proveedores ofertan productos descontinuados.	Muy grave	• Aplicar un análisis de riesgos al nuevo escenario • Evaluar la necesidad de modificar o ampliar los acuerdos de prestación de servicios para cubrir las nuevas necesidades de seguridad si así se estima oportuno
A.15.2.2. Los equipos no tendrían la garantía, las políticas de procedimientos podrían afectar la seguridad de la información	Muy grave	• Tener implantado y documentado los procedimientos que nos dirijan en el proceso de gestión de incidentes de la seguridad de la información. • Definir un responsable para la gestión de incidentes quien deberá garantizar que se desarrollan los procedimientos adecuados para que se realicen todas las tareas o procesos necesarios para gestionar los incidentes • Determinar procedimientos para la detección, análisis y elaboración de informes de incidentes de la seguridad de la información

A.16.1.1. No se brinda respuesta a los incidentes de seguridad de la información	Importante	• Determinar un criterio de priorización de incidentes dependiendo del sistema o servicio afectado, del usuario etc. • Realizar una evaluación de incidentes, debe ser realizada tanto por el usuario como por el equipo de gestión que debe revisar la prioridad. • Llevar un registro de la evaluación de los incidentes para poder analizar los parámetros de calidad tanto en su resolución como de su clasificación.
A.16.1.4. Cualquier evento es considerado como incidentes de seguridad de la información.	Importante	• Controlar el proceso de resolución de incidentes en la seguridad de la información. • Evaluar si la organización tiene la capacidad para resolver el incidente por si misma o necesita ayuda de terceros. • Establecer el sistema de comunicaciones necesarias entre usuarios y el equipo de gestión de incidencias o quien deba estar informado de las actuaciones y situación del proceso de resolución de las incidencias
A.16.1.5. No se evalúa los eventos frecuentes de seguridad	Muy grave	• Los incidentes sobre la seguridad de la información pueden requerir acciones posteriores como sanciones o acciones legales. • Proveer de un mecanismo de recuperación de la información, como por ejemplo la certificar los sistemas de recolección de evidencia.
A.16.1.7. Aplicación de sanciones al personal equivocado.	Muy grave	• Implantar medidas de protección y de recuperación ante posibles desastres de esta naturaleza para minimizar los daños y facilitar el restablecimiento de las operaciones. • Mantener un plan de continuidad o recuperación ante incidentes.
A.17.1.1. Durante una crisis o desastres no tendrían información para mantenerse operativos	Importante	• Disponer de un plan con medidas concretas para restablecer la disponibilidad de la información en unos plazos identificados mediante unos planes de respuesta ante emergencias que tengan en cuenta la organización y sus recursos • **Establecer una Estructura de gestión** que defina responsabilidades en la continuidad y recuperación de los sistemas • **Designar a las personas** que van a desempeñar las distintas funciones dentro del plan de continuidad de la seguridad de la información y la recuperación ante desastres.

A.17.1.2. La información no se encuentra disponible	Importante	• Las cláusulas de revisión permiten que un sistema se mantenga vivo en el tiempo. Para ello se debe revisar periódicamente. La aplicabilidad de los controles, El alcance del plan de continuidad en el sentido en que no queden nuevos activos de información fuera del plan de continuidad, Revisar la implicación del personal en las tareas de recuperación verificando que todo el mundo esté al tanto de sus responsabilidades al respecto
A.17.1.3. El sistema de seguridad de la información no ayudaría al área operativa de la florícola	Importante	• Identificar que sistemas de información por su arquitectura no pueden garantizar la disponibilidad exigida por los procesos del negocio sin un sistema de respaldo • Analizar la viabilidad de sistemas redundantes • Realizar pruebas tanto de buen funcionamiento de los sistemas redundantes como de transición sin interrupciones de un sistema principal a un sistema redundante
A.17.2.1. No garantiza la disponibilidad de las instalaciones del procesamiento de la información	Muy grave	• Establezcan procedimientos que garanticen el uso del software de acuerdo a los términos previstos en la Ley de Propiedad Intelectual. • Disponemos de una política de uso legal de productos Software • Mantener la documentación que justifique o acredite la propiedad de las licencias (discos, manuales etc.)
A.18.1.2. Demandas de propiedad intelectual	Muy grave	• Para utilizar los mecanismos de cifrado deben tenerse en cuentas las normativas sobre uso de controles criptográficos vigentes.

Figura 17 Riesgos encontrados en la auditoría

4.2 DISCUSIÓN

Finalizada la auditoria con la norma ISO 27001:2013 donde de un total de 106 controles se obtuvo 51 no conformidades, 48 conformidades y 8 observaciones. Con este resultado se procedió a realizar un análisis de seguridad utilizando la Metodología OSSTMM en donde se obtuvo los siguientes resultados.

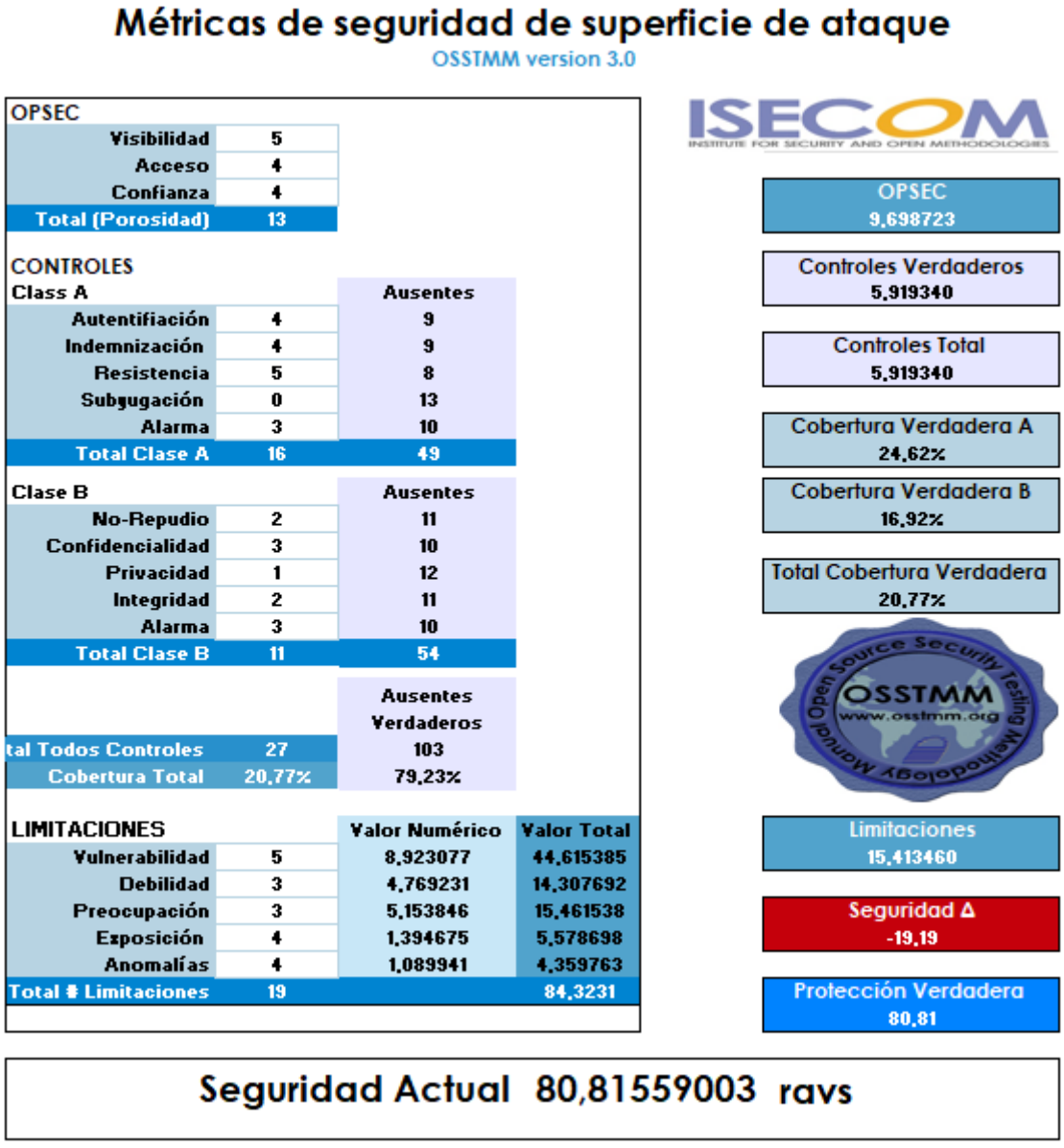


Figura 18. Resultado OSSTMM

Como se muestra en la “Figura 18” la florícola Galápagos Flores S.A con la Metodología abierta obtuvo un total de 80, 81 RAVS, es decir, cuenta con controles de seguridad, pero no están siendo efectivos.

Como se muestra en el apartado 4.1 Resultados, se aplicó el ciclo de Deming basado en la ISO 27001:2013 por ello el presente estudio tuvo como finalidad principal elaborar un informe y plan de mitigación de riesgos de la auditoria de seguridad informática en la florícola Galápagos Flores S.A tomando como base la norma ISO 27001:2013 desarrollada por la Organización Internacional de Normalización (ISO: “International Organization for Standardization”) y por la Comisión Electrotécnica Internacional (IEC: “International Electrotechincal Commission”). Aplicando las fases de planificar, hacer, revisar y actuar.

Por lo tanto, en el 4.1 muestra el informe de auditoría, matriz de riesgos encontrados y el plan de mitigación con las recomendaciones para cada riesgo.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Se alcanzó el cumplimiento del objetivo general referente a la auditoria de seguridad informática aplicando la norma ISO 27001:2013, desarrollando un informe final y la elaboración de un plan de mitigación de riesgos, el cual fue socializado a Subgerencia General, Gerencia Financiera y el encargado del Área de Sistemas.

La información fue recopilada mediante libros, revistas y medios virtuales incluyendo la norma ISO 27001:2013 y la Metodología Abierta de Testeo de Seguridad (OSSTMM) las cuales permitió ajustar los requerimientos de investigación con los objetivos de la florícola para poder establecer el proceso de auditoría y evaluar la situación actual de Galápagos Flores S.A.

El proceso de auditoría fue llevado a cabo mediante la norma ISO 10011-1:2018 la cual estableció los principios básicos, criterios y prácticas de una auditoría, además de proveer lineamientos para establecer, planificar, realizar y documentar la auditoría.

Aplicando la norma ISO 27001:2013 y la Metodología Abierta de Testeo de Seguridad (OSSTMM) a la florícola Galápagos Flores S.A se obtuvo como resultado que los controles de seguridad son mediamente cumplidos, es decir, la seguridad de la información necesita cumplir con más controles.

El estudio inicial se realizó mediante técnicas de verificación las cuales fueron: la entrevista dirigida al encargado del área de sistemas y la encuesta aplicada al personal que se encuentra en contacto con los equipos tecnológicos que fueron un total de 15 personas.

Finalmente se determinó 51 riesgos en base a los hallazgos de la auditoría, los mismo que fueron priorizados en la matriz de riesgo en base al impacto y probabilidad. Posterior mente se emitieron estrategias de mitigación los cuales fueron socializados al personal a cargo de la florícola Galápagos Flores S.A.

5.2. RECOMENDACIONES

Concluido el proceso de investigación , y contando con el conocimiento de estructura y funcionamiento de la florícola, se pone en consideración lo siguiente:

Se recomienda fortalecer el área de sistemas con personal capacitado para cumplir con las estrategias de mitigación socializadas y mejorar la seguridad de la información de la empresa.

Realizar las actualizaciones de los riesgos o amenazas para cada una de las planificaciones dispuestas en Galápagos Flores S.A ya que los mismo pueden aumentar o disminuir con el tiempo, teniendo en cuenta que la florícola se encuentra en una nueva administración.

Es recomendable que la florícola gestione las estrategias emitidas en el plan de mitigación de riesgos, para cumplir con los parámetros solicitados en las auditorías ambientales, de esta manera se consideran e indican que los controles han sido identificados y gestionados obteniendo una adecuada optimización de recursos.

Es importante que el área de sistemas cuente con un lugar adecuado de funcionamiento en donde los equipos mantengan la seguridad necesaria y no se encuentre al alcance de todo el personal, al igual que los servidores de datos cuenten con uno o más respaldos para más seguridad de la información.

Se recomienda realizar los respaldos de la información al menos 2 veces al mes y que los mismos sean guardados en un lugar diferente a la oficina de financiero. Además, priorizar la clasificación de la información y la asignación de las mismas a los usuarios.

IV. REFERENCIAS BIBLIOGRÁFICAS

BECERRA ARÉVALO, N. P. (2017). *AUDITORÍA INFORMÁTICA BASADA EN NORMA ISO 27004 PARA EL CONTROL DEL PARQUE TECNOLÓGICO DE UNIANDES PUYO*. [UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES "UNIANDES"].http://dspace.uniandes.edu.ec/bitstream/123456789/7415/1/PIUAMIE013-2017.pdf

Benavides, C. (2017). Como crear un plan de mitigación o un plan de contingencia de riesgos. https://calidadparapymes.com/plan-de-mitigacion-de-riesgos/

Bernal, J. (2013). *Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua : PDCA Home*. https://www.pdcahome.com/5202/ciclo-pdca/

Carrillo, D. (2018). *BII13. Seguridad física y lógica de un sistema de información. Riesgos, amenazas y vulnerabilidades. Medidas de protección y aseguramiento. Auditoría de seguridad física. – GSITIC*. https://gsitic.wordpress.com/2018/01/19/bii13-seguridad-fisica-y-logica-de-un-sistema-de-informacion-riesgos-amenazas-y-vulnerabilidades-medidas-de-proteccion-y-aseguramiento-auditoria-de-seguridad-fisica/

Cortes Robles, D. (2017). *El proceso de Auditoria Informática*. https://www.seguridadyfirewall.cl/2017/01/el-proceso-de-auditoria-informatica.html

Cuellar Triana, N., María, O., Castañeda, P., Triana, C., & Pinilla, &. (2015). *El papel del auditor frente a una auditoria sobre TIC El papel del auditor frente a una auditoria sobre TIC Citación recomendada Citación recomendada*. https://ciencia.lasalle.edu.co/contaduria_publicaM.

ESET. (2019). *ESET SECURITY REPORT Latinoamérica 2019*. Obtenido de ESET SECURITY REPORT Latinoamérica 2019: https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf

Gavino LLagas, A. R. (2018). *UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN*. UNIVERSIDAD NACIONAL JOSÉ FAUSTO SÁNCHEZ CARRIÓN.

Hernandez, E. (2015). *Auditoria de Informática (Un Enfoque Metodológico)*.

Hernández, R., Fernández, C., & Baptista, P. (2017). Metodología de la investigación. (Quinta Edición). México D.F, México:McGraw-Hill

Medina, F. L. C., Díaz, A. D. P. L., & Cardenas, C. R. (2017). Sistema de gestión ISO 9001-2015: técnicas y herramientas de ingeniería de calidad para su implementación. *Ingeniería Investigación y Desarrollo: I2+ D*, *17*(1), 59-69. Medina, F. L. C., Díaz, A. D. P. L., & Cardenas, C. R. (2017). Sistema de gestión ISO 9001-2015: técnicas y herramientas de ingeniería de calidad para su implementación. *Ingeniería Investigación y Desarrollo: I2+ D*, *17*(1), 59-69.

Ministerio de Finanzas Ecuador. (2017). Metodología para la gestión integral de riesgos. https://www.finanzas.gob.ec/wp- 195 content/uploads/downloads/2017/04/Metodolog%C3%ADa-para-la-Gesti%C3%B3nde-Riesgos-30-03-17.pdf

MINTIC. (2017). *Guía para la Gestión y Clasificación de Activos de Información.* https://www.mintic.gov.co. https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

P Herzog. «OSSTMM 3 - The open source security testing methodology manual». En: Institute for Security and Open Methodologies: ISECOM (2010).

ISACA. (2012). *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Madrid: El capítulo de Madrid ISACA®.

Olmedo, J. Y León, F.(2018). Análisis de los Ciberataques Realizados en América Latina. *INNOVA Research Journal, ISSN 2477-9024*

Palella Stracuzzi, S y Martins Pestana, F.(2012). *Metodología de la investigación Cuantitativa.* Universidad Pedagógica Experimental Libertador. https//es.calameo.com/read/000628576f51732890350

Pérez, A., & Rodríguez, A. (2017). Métodos científicos de indagación y de construcción del conocimiento. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-81602017000100179

Prieto, J.(2018). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales. Cuadernos de Contabilidad, 18(46). https;//doi.org/10.11144/javeriana.cc18-46-umdi

Romero, M. I., Grace, C., Figueroa, L., Denisse, M., Vera, S., José, N., Álava, E., Galo, C., Parrales, R., Christian, A., Álava, J., Ángel, M., Murillo Quimiz, L., Adriana, M., & Merino, C. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. Universidad Estatal del Sur de Manabí.

Sampieri, R. (2016). Metodología de la investigación.

Ulloa Barrera, J. G. (2017). *Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo Descentralizado Municipal de San Cristóbal de Patate.* [UNIVERSIDAD TÉCNICA AMBATO]. https://repositorio.uta.edu.ec/bitstream/123456789/27125/1/Tesis_ t1360si.pdf

Villardefrancos Alvarez, M. D. C., & Rivera, Z. (2006). *La auditoria como proceso de control: concepto y tipología* (Vol. 37, Issue 2).

V. ANEXOS

Anexo 1 Acta de sustentación de la predefensa

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE COMPUTACION

Educamos para transformar el mundo

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL TRABAJO DE INTEGRACIÓN CURRICULAR:

NOMBRE: HEIDY SELENA QUISHPE PILLAJO — **CÉDULA DE IDENTIDAD:** 1755068929
NIVEL/PARALELO: 0 — **PERIODO ACADÉMICO:** PAO 2022A

TEMA DEL TIC: Auditoria de seguridad informática en la floricola Galápagos Flores S.A.

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. CARLITOS ALBERTO GUANO CÁRDENAS
DOCENTE TUTOR: MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
DOCENTE: MSC. GEORGINA GUADALUPE ARCOS PONCE

De acuerdo al artículo 32: Una vez entregados los documentos; y, cumplidos los requisitos para la realización de la pre-defensa el Directorio de Carrera designará el Tribunal, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 4 **AULA:** 108
FECHA: lunes, 15 de agosto de 2022
HORA: 15H00
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 4,80
2) Trabajo escrito 2,20
Nota final de PRE DEFENSA **7,00**
Por lo tanto: **NO APRUEBA** ; debiendo acatar el siguiente artículo:

Art. 36.- De los estudiantes que aprueban el informe final del TIC con observaciones.- Los estudiantes tendrán el plazo de 10 días para proceder a corregir su informe final del TIC de conformidad a las observaciones y recomendaciones realizadas por los miembros del Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el lunes, 15 de agosto de 2022

MSC. CARLITOS ALBERTO GUANO CÁRDENAS
PRESIDENTE

MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
DOCENTE TUTOR

MSC. GEORGINA GUADALUPE ARCOS PONCE
DOCENTE

Adj.: Observaciones y recomendaciones

Anexo 2 Certificado antiplagio del informe de investigación

TESIS VERSION FINAL

por Heidy Quishpe

Fecha de entrega: 05-ago-2022 03:55p.m. (UTC-0500)
Identificador de la entrega: 1879251490
Nombre del archivo: TIC-QUISHPE_HEIDY.docx (2.83M)
Total de palabras: 21937
Total de caracteres: 125135

60	Samuel Israel Goyzueta Rivera, Danna Melina Torrico Ibarra. "Efectos del género en la decisión de compra en línea", Revista Compás Empresarial, 2022 Publicación	<1 %
61	repositorio.unjfsc.edu.pe Fuente de Internet	<1 %
62	www.borrmart.es Fuente de Internet	<1 %
63	www.um.es Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 15 words
Excluir bibliografía	Activo		

Anexo 3 Certificado del abstract por parte del Centro de Idiomas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Quishpe Pillajo Heidy Selena
DATE: 13 de septiembre de 2022

TOPIC: "Auditoria de seguridad informática en la floricola Galápagos Flores S.A"
MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ■	GOOD: 1Vera Játiva Edwin Andrés,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ■	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	TOTAL 9		

1

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Quishpe Pillajo Heidy Selena
Fecha de recepción del abstract: 13 de septiembre de 2022
Fecha de entrega del informe: 13 de septiembre de 2022

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:
Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9, por lo cual se validad dicho trabajo.

Atentamente

EDISON ROAMERGES PEÑAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

2

Anexo 4 Oficio aprobación de la realización del trabajo de titulación.

Educamos para transformar el mundo

Señor.

Ing. José Antonio Sosa

Gerente Financiero de la florícola Galápagos Flores S.A

Presente. -

De mis consideraciones

Yo, Quishpe Pillajo Heidy Selena con CC. 175506892-9, por medio del presente me dirijo a usted muy respetuosamente para solicitar autorización para el desarrollo del plan de investigación dentro de la florícola Galápagos Flores S.A, requisito para egresar de la carrera de computación de la Universidad Politécnica Estatal del Carchi, cuyo tema es: "*Auditoría de seguridad informática en la florícola Galápagos Flores S.A*".

Esperando que usted acepte mi solicitud, me comprometo a mandar una carta formal por parte de la universidad con la finalidad de cumplir con todos los reglamentos.

Por la atención que se digne a dar a la presente, anticipo mis debidos agradecimientos.

Atentamente

HEIDY QUISHPE

UNIVERSITARIA UPEC

Ingeniería en Ciencias de la Computación

José Sosa Romero
12/01/2021.

Anexo 5 Oficio aplicación de instrumentos de investigación

Tabacundo, 5 de octubre del 2021

Ing.

José Sosa

Gerente Financiero Galápagos Flores S.A

Presente.-

De mi consideración:

Reciba un atento y cordial saludo, a la vez desearle toda clase de éxito en las funciones que acertadamente desempeña.

El presente tiene como finalidad solicitar la autorización para realizar el levantamiento de información aplicando la técnica de la entrevista y encuesta a un total de quince personas que son las que mantienen un contacto directo con los equipos de cómputo, como parte del desarrollo del Proyecto de Integración Curricular denominado "Auditoria de seguridad informática en la floricola Galápagos Flores S.A", el contenido de la entrevista y encuestas busca identificar como el departamento de sistemas se encuentra involucrado en los procesos que realiza la empresa.

Esperando una favorable acogida a la presente, anticipo mis agradecimientos.

Atentamente

Heidy Selena Quishpe Pillajo

C.I 1755068929

Estudiante de la Carrera de Ingeniería en Ciencias de la Computación

Universidad Politécnica Estatal del Carchi

GALAPAGOS

Anexo 6 Oficio aplicación de entrevista y encuesta

Tabacundo, 21 de febrero del 2022

Ing.

José Sosa

Gerente Financiero Galápagos Flores S.A

Presente.-

De mi consideración:

Reciba un atento y cordial saludo, a la vez desearle toda clase de éxito en las funciones que acertadamente desempeña.

El presente tiene como finalidad solicitar la autorización para aplicar la entrevista y encuestas finales, como parte del Proyecto de Integración Curricular denominado "Auditoria de seguridad informática en la floricola Galápagos Flores S.A", el contenido de la entrevista y encuestas busca evaluar el nivel de seguridad informática que mantiene actualmente la empresa y con ello determinar el Plan de mitigación.

Adjunto la planificación y las hojas de trabajo a utilizar.

Esperando una favorable acogida a la presente, anticipo mis agradecimientos.

Atentamente

Heidy Selena Quishpe Pillajo

C.I 1755068929

Estudiante de la Carrera de Ingeniería en Ciencias de la Computación

Universidad Politécnica Estatal del Carchi

GALAPAGOS FLORES

Anexo 7 Aplicación encuesta

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Facultad de Industrias Agropecuarias y Ciencias Ambientales

Carrera de Computación

Proyecto de Integración Curricular

Tema: Auditoria de seguridad informática en la floricola Galápagos Flores S.A

Fecha: _____

Tema: Auditoria de seguridad informática en la floricola Galápagos Flores S.A

Objetivo: La presente encuesta está dirigida al personal de la finca Galápagos flores S.A, con la finalidad de conocer el nivel de conocimiento acerca de la seguridad informática dentro de la floricola.

1. ¿Con que frecuencia se mantiene un control de los procesos que realiza el computador?
   - Nunca ( )
   - Casi nunca ( )
   - Ocasionalmente ( )
   - Casi todos los días ( )
   - Todos los días ( )
2. ¿Con que frecuencia recibe capacitaciones por parte del departamento de sistemas?
   - Nunca ( )
   - Casi nunca ( )
   - Ocasionalmente ( )
   - Casi todos los días ( )
   - Todos los días ( )
3. ¿Para ingresar al sistema integrado FINANCONTRY requiere una contraseña?
   - Si ( )
   - No ( )
4. ¿Para iniciar sesión en su computador requiere ingresar una contraseña?
   - Si ( )
   - No ( )
5. ¿Los equipos de cómputo cumplen con las características para agilizar el proceso?
   - Cumple totalmente ( )

Quishpe, H. Número 2021

- Cumple ( )
- Cumple parcialmente ( )
- No cumple ( )

6. ¿Tiene conocimiento de los programas instalados en el equipo de cómputo?
   - Si ( )
   - No ( )
   - N
7. ¿Con frecuencia se realiza mantenimiento técnico al equipo de cómputo?
   - Una vez a la semana( )
   - Una vez al mes( )
   - Una vez cada dos meses ( )
   - Nunca ( )
8. ¿Tiene conocimiento de las políticas de privacidad de la información que maneja la florícola?
   - Si ( )
   - No ( )
9. ¿La administración esta monitoreando su computadora todo el tiempo?
   - Si ( )
   - No ( )
   - No sé ( )
10. ¿Qué tan difícil es para usted identificar un virus informático?
    - Muy difícil ( )
    - Difícil ( )
    - Neutral ( )
    - Fácil ( )
    - Muy fácil ( )

Anexo 8 Aplicación de la entrevista

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Facultad de Industrias Agropecuarias y Ciencias Ambientales

Carrera de Computación

Proyecto de Integración Curricular

Tema: Auditoria de seguridad informática en la floricola Galápagos Flores S.A

Nombre del entrevistado: José Barreiro

Objetivo: Conocer los procesos y procedimientos que se llevan a cabo en el área.

La entrevista contempla los siguientes puntos:

1. Se solicita al jefe del departamento de sistemas socializar cada uno de los procedimientos solicitados en información requerida.

DOCUMENTACIÓN REQUERIDA	SOCIALIZACIÓN
Sistema de gestión de seguridad informática	No existe documentación
Certificación de estudios del jefe del departamento de sistemas	Certifica sus estudios como ingeniero en sistemas
Inventario de activos informáticos	El inventario se encuentra desactualizado desde el 2018
Matriz de riesgo de Seguridad Informática	Se miden siete riesgos, los cuales se encuentran inmersos en la matriz de área
Planes de mejoramiento de seguridad informática	No existe
Plan de contingencia de la seguridad de la información	El plan de contingencia se enfoca en el respaldo de la información del sistema integrado, sin embargo, la información que se maneja diariamente. Cuenta con un plan de contingencia básico para la información que actualmente se maneja.
Procedimiento de asignación de credenciales a los usuarios	No existe, se realiza de manera empírica
Procedimiento de asignación de contraseñas a la red WIFI	No existe, se realiza de manera empírica
Procedimiento de generación de contraseñas	No existe, se realiza de manera empírica

Procedimiento de ejecución de Backups	No existe, se realiza empíricamente.
Procedimiento de Manejo de discos extraíbles	No existe, se realiza empíricamente.
Procedimiento de control de acceso a internet	No existe, se realiza empíricamente.
Cronograma de mantenimiento de activos informáticos	Se realiza mediante una planificación anual que es aprobada a principios del año en curso.
Hojas de vida de activos informáticos	No existe
Compromiso de confidencialidad firmado por el personal	Existe el documento de confidencialidad el cual es firmado al realizar el contrato, dicho documento se encuentra anexado en cada carpeta del trabajador
Actas de capacitación a los usuarios internos en Seguridad Informática	No existe

2. Se solicita al jefe del departamento de sistemas que explique la matriz de riesgos.

El Ing. José Barreiro, indica que los riesgos mostrados en la matriz para el área de sistemas se realizó conjunto con el mapa de riesgos de la empresa.

Se miden los siguientes riesgos

- ✓ No hay comunicación entre CLIENTE-SERVIDOR
- ✓ Interrupción del fluido eléctrico durante la ejecución de procesos
- ✓ Indisponibilidad de los servidores que contienen almacenados los datos
- ✓ Pérdida del servicio de internet
- ✓ Falla de un servidor
- ✓ Substracción, robo o fuga de información confidencial
- ✓ Desactualización hardware/software

3. Se solicita al jefe del departamento de sistemas que socialice los planes de mejoramiento de la seguridad de la información.

El Ing. José Barreiro menciona que la falta de recursos limita la realización de planes de mejoramiento, además afirma que con la pandemia COVID-19 la empresa

tubo que reducir su presupuesto dejando al departamento de sistemas como no prioritario.

4. Se solicita al jefe del departamento de sistemas la socialización de los inventarios de activos informáticos y su ubicación.

   El jefe del departamento de sistemas muestra una hoja impresa de Excel, la cual no ha sido actualizada desde el 2018, ante esto menciona que los equipos no han sido actualizados desde dicho año. Luego de un recorrido por la finca para la verificar la concordancia de la hoja con lo que actualmente mantienen, se puede evidenciar que dos equipos fueron dados de baja y reemplazos por un computador, lo cual no se evidencia en la matriz de activos.

5. Se solicita al jefe del departamento de sistemas que socialice el plan de mantenimiento.

El jefe del departamento de sistemas muestra el plan anual realizado a inicios del año en curso el cual es aprobado por Gerencia Técnica.

El cronograma de mantenimiento muestra la fecha, área, usuario a cargo y el procedimiento que se va a realizar. De igual manera, el cronograma se ajusta a las temporadas altas en donde menciona que los equipos deben estar en perfectas condiciones para no retrasar los procesos.

Se puede verificar que el cronograma se cumple parcialmente, esto mediante las hojas de control firmadas por los usuarios a los que se realizó soporte técnico a los equipos.

Anexo 9 Planificación para la auditoría

HEIDY QUISHPE PILLAJO

De:	sistemas@galapagosflores.com
Enviado el:	lunes, 31 de enero de 2022 11:30
Para:	HEIDY QUISHPE PILLAJO
Asunto:	Documentos Solicitados
Datos adjuntos:	1. Organigrama Estructural y Funcional.pdf; Manual de Seguridad 2020 (24-OCTUBRE-2020).doc

Estimada Srta. Selena Quishpe.

Adjunto los documentos solicitados para su trabajo de titulación.

- Organigrama empresarial
- Misión, visión, Objetivo general, Objetivos específicos.

Cabe aclarar que los documentos deben ser usados únicamente con fines educativos.

De igual manera me permito informarle que los cronogramas de ingreso a la empresa para realizar los proyectos de investigación han sido aprobados por el la Gerencia, aclarando que el mismo tomara validez a partir de la **segunda semana de febrero**, debido a que actualmente nos encontramos en temporada alta (Valentín).

Una vez aclarado esto su horario es el siguiente:

Srta. Selena Quishpe

- Miércoles y jueves de 08h00 a 16h30

En el horario estipulado puede acceder a las instalaciones en donde se realizará el respectivo registro en guardianía además de seguir con los protocolos de bioseguridad.

Sin mas que agregar a la presente, quedo atento a sus comentarios

Saludos Cordiales,

Ing. José Barreiro
Departamento de Sistemas
GALAPAGOS FLORES GALAFLOR S.A

1

Anexo 10 Planificación, alcance de la auditoria

Auditoria Galápagos Flores S.A

Mediante la presente se da a conocer el alcance, objetivo y justificación de la auditoria a llevarse a cabo en la floricola Galápagos Flores S.A. A demás, del cronograma en donde el equipo auditor realizará la visita a la finca.

Objetivo de auditoria. Desarrollar un análisis de seguridad informática de la floricola Galápagos Flores S.A, con el propósito de identificar los riesgos tecnológicos que afectan el logro de los objetivos de la floricola.

Alcance de la Auditoria informática.

La auditoria de seguridad informática en la floricola Galápagos Flores S.A se revisará las áreas de tecnología, ventas, financiero, recursos humanos en donde se realizará un diagnóstico a los controles de seguridad de la información con la finalidad de identificar los puntos críticos que afectan el cumplimiento de los objetivos institucionales.

Justificación. La auditoria de seguridad informática es un proceso de evaluación que permite detectar debilidades a nivel tecnológico y así contemplar mejoras en los servicios que brinda el área de sistemas.

Planificación de la auditoria

Fecha	Actividades de Auditoria	Áreas auditadas	Personal encargado
21 de febrero de 2022	Presentación del auditor y presentación del plan de auditoria	Área administrativa: Contabilidad, Recursos Humanos, Compras, Ventas, Postcosecha, Sistemas	Gerencia Financiera Encargado del área de sistemas
21 de febrero de 2022	Aplicación de la encuesta en el área funcional de postcosecha	Área funcional: Postcosecha	Auditora
21 de febrero de 2022	Aplicación de la entrevista al encargado del Área de sistemas	Área administrativa: Sistemas	Auditora
24 de febrero de 2022	Clasificación de los activos de la información	Área administrativa: Sistemas	Encargado del área de sistemas

			Auditora
24 de febrero de 2022	Aplicación de la lista de chequeo ISO 27001:2013	Área administrativa: Sistemas	Auditora
19 de julio de 2022	Socialización de los resultados obtenidos de la auditoria	Área administrativa: Contabilidad, Recursos Humanos, Compras, Ventas, Postcosecha, Sistemas	Auditora

Anexo 11 Aplicación de la auditoría

ISO 27001:2013 GALÁPAGOS FLORES S.A						
OBJETIVOS DE CONTROL Y CONTROLES			CUMPLE			
			SI	PARCIALMENTE	NO	OBSERVACIONES
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	X			
	Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	X			
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.			X	
	Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.			X	
		A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	X			
		A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.			X	
		A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,			X	
	A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	X			

	Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.		X		
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1. Antes de asumir el empleo.	A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.			X	
	Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	X			
	A.7.2. Durante la ejecución del empleo.	A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	X			
	Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	X			
		A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	X			
	A.7.3. Terminación y cambio de empleo.	A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	X			
	Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.					

A.11. SEGURIDAD FÍSICA Y AMBIENTAL.		A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	X			
		A.11.1.4. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.		X		
		A.11.1.5. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	X			
		A.11.1.6. Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	X			
	A.11.2. Equipos.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.			X	
	Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.		X		
		A.11.2.3. Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.			X	
		A.11.2.4. Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X			
		A.11.2.5. Retiro de Activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	X			
		A.11.2.6. Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentren fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.			X	

A.8. GESTIÓN DE ACTIVOS.	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.			X	
	Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.	X			
		A.8.1.3. Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.			X	
		A.8.1.4. Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	X			
	A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	X			
	Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.			X	
		A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	X			
	A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.			X	
	Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	X			

A.12. SEGURIDAD DE LAS OPERACIONES.	Objetivo. Registrar eventos y generar evidencia.	A.12.4.2. Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.			X	
		A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	X			
		A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	X			
	A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.			X	
	Objetivo. Asegurarse de la integridad de los sistemas operacionales.					
	A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X			
	Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.			X	
	A.12.7.1 Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.			X	
	Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.					
	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.			X	

		A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.			X	
A.9. CONTROL DE ACCESO.	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	X			
	Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.			X	
	A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	X			
	Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	X			
		A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	X			
		A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.			X	
		A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	X			
		A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	X			
	A.9.3. Responsabilidades de los usuarios.	A.9.3.1. Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.			X	

	Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.					
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	X			
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.			X	
		A.9.4.3. Sistema de Gestión de Contraseñas. Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.			X	
		A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.			X	
		A.9.4.5. Control de Acceso a Códigos Fuente de Programas. Se debe restringir el acceso a códigos fuente de programas.				No Aplica
A.10. CRIPTOGRAFÍA	A.10.1. Controles Criptográficos.	A.10.1.1. Política sobre el uso de controles Criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.			X	
	Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A.10.1.2. Gestión de Claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.			X	
	A.11.1. Áreas Seguras.	A.11.1.1. Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	X			
	Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	X			

A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	A.17.1. Continuidad de seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.			X	
	Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	A.17.1.2. Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.			X	
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.			X	
	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.			X	
	Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.					
A.18. CUMPLIMIENTO.	A.18.1. Cumplimiento de requisitos legales y contractuales.	A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.		X		
	Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2. Derechos de Propiedad Intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.			X	
		A.18.1.3. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	X			

A.13. SEGURIDAD DE LAS COMUNICACIONES	Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.			X	
		A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.			X	
	A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.			X	
	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.			X	
		A.13.2.3. Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	X			
		A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	X			
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.			X	
	Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	X			

		A.11.2.7. Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reusó.	X			
		A.11.2.8. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.		X		
		A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.			X	
	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.		X		
	Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.			X	
		A.12.1.3. Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	X			
	A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.			X	
	Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.					
	A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X			
	Objetivo. Proteger contra la pérdida de datos.					
	A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.			X	

		A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.	X			
		A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.	X			
		A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.	X			
		A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.	X			
	A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	X			
	Objetivo. Asegurar la protección de los datos usados para ensayos.					
A.15. RELACIONES CON LOS PROVEEDORES.	A.15.1. Seguridad de la información en las relaciones con los proveedores.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.			X	
	Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.			X	
		A.15.1.3. Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.			X	
	A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.			X	

	Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	A.15.2.2. Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.			X	
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.			X	
	Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	X			
		A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	X			
		A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.			X	
		A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.			X	
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	X			
		A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.			X	

		A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.		X		
		A.18.1.5. Reglamentación de Controles Criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos			X	
	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	X			
	Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	A.18.2.2. Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.		X		
		A.18.2.3. Revisión del Cumplimiento Técnico. Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	X			

Anexo 12 Socialización del Informe de Auditoría

Tabacundo, 19 de julio de 2022

Ingeniero

José Antonio Sosa

Gerente Financiero de Galápagos Flores S.A

Presente.-

De mi consideración:

Reciba un atento saludo, a la vez desearle toda clase de éxitos en las funciones que acertadamente desempeña.

El presente tiene como finalidad realizar la socialización formal del **PLAN DE MITIGACIÓN,** resultados propuestos para el Proyecto de Titulación denominado "Auditoria de seguridad informática en la floricola Galápagos Flores S.A"

Los documentos que serán socializados son:

- Informe de resultados de Auditoría Informática
- Plan de mitigación

Atentamente

Realizado por:

Heidy Selena Quishpe Pillajo
Egresada de la Carrera de Ingeniería en Ciencias de la Computación
Universidad Politécnica Estatal del Carchi

Recibido por:

Ing. José Antonio Sosa
Gerente Financiero
Galápagos Flores S.A

GALAPAGOS FLORES

Anexo 13 Certificado de cumplimiento

GALAPAGOS

CERTIFICO

Que la Señorita Heidy Selena Quishpe Pillajo con cédula de identidad N° 1755068929 egresada de la carrera de Ingeniería en Ciencias de la Computación de la Universidad Politécnica Estatal del Carchi, trabajó en esta empresa florícola en el desarrollo del proyecto "**Auditoria de seguridad informática en la floricola Galápagos Flores S.A**" en donde la florícola ha brindado las facilidades para llevar a cabo la finalización del mismo.

La propuesta del proyecto que constituye el informe de resultados de la Auditoria Informática y el Plan de mitigación el cual ha sido socializado con el personal administrativo el mismo contribuye alcanzar las metas propuestas dentro de la empresa y a su vez mejorar en la seguridad de la información, por lo cual extendemos nuestro agradecimiento a la institución por los resultados obtenidos.

Es todo cuanto puedo certificar en honor a la verdad, facultando a la interesada hacer el uso del presente que estima conveniente.

Dado y firmado en el cantón Pedro Moncayo a los veinte y dos días del mes de Julio del año dos mil veinte y dos

Atentamente

GALAPAGOS

Ing. José Antonio Sosa

Gerente Financiero Galápagos Flores S.A