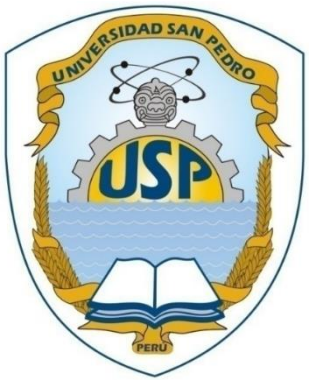
UNIVERSIDAD SAN PEDRO

VICERRECTORADO ACADÉMICO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS



Auditoría de seguridad física de la Empresa AGROKASA Supe

Tesis para obtener el título profesional de ingeniero en informática y de sistemas

Autor:

Nilo Franklin, Salinas Vega

Asesor:

Ing. Lara Carreño, Marco

Huacho - Perú

2017

ÍNDICE

TÍTULO

AUDITORÍA DE SEGURIDAD FÍSICA DE LA EMPRESA AGROKASA SUPE

PALABRAS CLAVE:

Tema	Auditoría de Seguridad Informática
Especialidad	Gestión

KEYWORDS:

Theme	Computer Security Audit
Specialty	TIC

Línea de Investigación.

Área	**Sub-área**	**Disciplina**
2. Ingeniería y Tecnología	2.2 Ingeniería Eléctrica, Electrónica e Informática	Ingeniería de Sistemas y Comunicaciones

RESUMEN

El objetivo de este proyecto de investigación fue desarrollar una auditoria de seguridad física al a empresa Agrokasa Supe – Barranca.

Con el fin de revisar su administración y estructura de la seguridad física de la organización, verificar su cumplimiento de las políticas de seguridad según la norma y determinar en qué medida cumplen con la implementación de requerimientos de seguridad física en el área de informática, atreves de un análisis de brechas(GAP análisis) y se decidió por aplicar la Metodología EDPAA (Asociación de Auditores en Procesamiento de Datos Electrónicos) para el desarrollo de auditoría física y en base a los controles de la norma de gestión de la seguridad de la información ISO 27002, con el fin de emitir un informe de hallazgos, que muestre las falencias existentes en dichas tecnologías de información y plantear las recomendaciones y políticas de seguridad.

Se logró aplicar la auditoria, teniendo como resultado en porcentaje del cumplimiento para el dominio de seguridad física y ambiental del ISO 27002, y dio que el Subdominio 9.1 Áreas Seguras cumple un 2% y el subdominio 9.2 Seguridad de los Equipos cumple un 13.4%, teniendo un nivel total de cumplimiento del dominio en un 10.3%.

ABSTRACT

The objective of this research project was to develop a physical security audit for the company Agrokasa Supe - Barranca.

In order to review its management and structure of the physical security of the organization, verify its compliance with the security policies according to the standard and determine to what extent they comply with the implementation of physical security requirements in the area of information technology, through a gap analysis (GAP analysis) and decided to apply the EDPAA Methodology (Association of Auditors in Electronic Data Processing) for the development of physical audit and based on the controls of the ISO information security management standard 27002, in order to issue a report of findings, which shows the shortcomings in these information technologies and raise the recommendations and security policies.

The audit was applied, resulting in percentage of compliance for the physical and environmental security domain of ISO 27002, and gave Subdomain 9.1 Safe Areas meets 2% and subdomain 9.2 Security of Equipment meets 13.4%, having a total level of domain compliance of 10.3%.

INTRODUCCIÓN

1.1 ANTECEDENTES Y FUNDAMENTACIÓN CIENTÍFICA.

Cadme y Duque (2012), en la tesis de grado de título "Auditoría de seguridad informática ISO 27001 para la empresa de alimentos Italimento Cia. Ltda" se realizó este estudio objetivo de abarcar hasta qué punto puede ayudar este tipo de estándar en la organización que se va auditar con la norma ISO 27001, así realizar con políticas claramente establecidas creando el aumento de productividad, mejora las relaciones laborales, motivación y ambiente de trabajo entre el personal, compromiso con la misión de la compañía, gestionar los activos de la empresa que son de suma importancia para la producción de la compañía, y deja en claro las recomendaciones de los objetivos señalados de acuerdo a la medida establecida en la norma.

León y Manotoa (2005), en la tesis de grado de título "Desarrollo de una Auditoría Informática mediante la aplicación de la Metodología COBIT en la Universidad Técnica de Cotopaxi" se hizo el estudio con el fin de mejorar la eficiencia del servicio informático, disminuir costos, mejorar la relación servicio-usuario y en general mejorar el control del servicio informático en la Universidad y aplicar la Guía en la realización de una auditoría informática a través del uso de la metodología COBIT, contar con la documentación necesaria para garantizar el uso adecuado de todos los recursos informáticos, conocer y difundir las normas de control interno de la Contraloría para optimizar el uso de la tecnología en cuanto a recursos informáticos se refiere y proporcionar información a las personas inmersas que trabajan en el proceso informático de la universidad, con el interés de establecer normatividad clara a fin de prevenir:

- Destrucción de Información,
- Fraudes Informáticos,
- Funcionamiento incorrecto de Sistemas,
- Discontinuidad Operativa o falla total de los Servicios Informáticos,
- Pérdida, destrucción, deterioro de los recursos,

Dejando en claro las conclusiones y recomendaciones para cada área establecidas de acuerdo a los objetivos planteados para su modificación.

Xiloj C. (2008), en la tesis de grado de licenciado "Auditoría externa en un ambiente de sistemas de información computarizado en el área de ingresos de una empresa comercializadora de vehículos" hizo el estudio con el fin de expresar una opinión sobre los estados financieros, garantizar información financiera confiable y oportuna, verificar la salvaguarda de los activos, promover la eficiencia operativa de la entidad, verificar el cumplimiento de objetivos, políticas, planes, procedimientos, leyes y reglamentos y que el auditor deberá cumplir con el "Código de Ética para los contadores profesionales" emitido por la Federación Internacional de Contadores, así como con el vigente localmente. Los principios éticos que gobiernan las responsabilidades profesionales del Auditor son: independencia, integridad, objetividad, competencia profesional y debido cuidado, confidencialidad, conducta profesional y normas técnicas que fue enfocado en la norma ISO-9000, luego de realizar la pruebas con determinadas técnicas se deja el informe de la auditoria.

Huamán M. (2014), en la Tesis de grado de título "Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano" hizo el estudios con el fin de establecer un procedimiento de auditoría de cumplimiento para la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 en las instituciones del Estado Peruano basado en el marco COBIT 5.0, como parte del proceso de implantación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 y mejorar la gestión de la seguridad de la información, también identificar los activos de información involucrados, elaborar el mapeo del marco COBIT 5.0 frente a la NTP 17799 y también Elaborar la guía metodológica para la ejecución de la auditoría de cada control contemplado en la norma NTP 17799, teniendo una lista de resultados según los objetivos planteados, dejando en claro las conclusiones y recomendaciones.

Nogueira S. (2013), en la Tesis de grado de título "Procedimientos para la auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar

internacional TIER" hicieron el estudio con el fin de diseñar un procedimiento de auditoría física y medio ambiental para centros de datos (Data Center) basado en la clasificación y estándar internacional TIER y de verificar las condiciones de seguridad de información con las que cuentan dichas instalaciones y también identificar los activos de información involucrados en la seguridad física y medio ambiental del Data Center e investigar las características más importantes relacionadas a seguridad física y ambiental expuestas por la clasificación y estándar internacional TIER para Data Center y ver las vulnerabilidades, riesgos y amenazas comunes en seguridad física y medio ambiental con la ayuda de la elaboración de una guía metodológica para conducir una auditoría ordenada, sistemática, repetible, eficiente e integral, enumerando los resultados obtenidos de acuerdo a los objetivos planteados, y dejando las conclusiones y recomendaciones del caso.

Barrantes y Hugo (2012), en la tesis de grado de título "Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos" realizaron el estudios con el fin de reducir y mitigar los riesgos de los activos de información de los procesos que se encuentran bajo la gerencia de tecnología de Card Perú S.A. que ponen en peligros los recursos, servicios y continuidad de los procesos tecnológicos e implementar una política de seguridad de información que sea desplegada de todos los colaboradores, proveedores y terceros, también gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de la información, para reducirlos en un 80%, desplegar la medidas de seguridad para gestionar los riesgos y ejecutar controles de tratamiento de riesgos, también la formalización y concientización al 100% de los colaboradores involucrados en los procesos de tecnología, en temas de seguridad de información, cumplimiento de las legislación vigente sobre la información personal, propiedad y gestionar y controlar el 100% de los documento de SGSI, que después de las pruebas dando una lista de resultados y beneficios obtenidos.

Cáceres y García (2014), en su tesis de grado de título "Implementación de una Auditoria Informática para la Oficina de Servicios Informáticos de la UNJFSC Aplicando el Marco de Referencia COBIT", se hizo con el fin la finalidad de realizar

una evaluación de la Gestión de la Información en la Oficina de Servicios Informáticos de la Universidad Nacional José Faustino Sánchez Carrión, con dicha investigación se logra encontrar aspectos que no permiten la optimización y la buena gestión de la Información en dicha oficina la cual fueron observadas para la evaluación correspondiente, usando la metodología de trabajo Cobit se llegará a medir el grado de madurez en la que se encuentra.

Díaz y Ugarte (2013), en la tesis de grado de título "Auditoria informática aplicada a la Municipalidad Provincial Huaura - Huacho", cuyo objetivo fue realizar una auditoría que permita evaluar el cumplimiento de los objetivos institucionales con respecto a la seguridad de la información emitiendo recomendaciones que contribuyen a mejorar su nivel de cumplimiento.

León R. (2012), en la monografía de grado de título "Auditoria informática en la empresa de servicios públicos Emapa Huacho s.a. 2012" hicieron una revisión y evaluación del desempeño de los diferentes equipos de cómputo, sistemas con que cuenta la empresa EPS EMAPA HUACHO; su utilización, eficiencia y seguridad, con la finalidad de que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones, y según la evaluación realizada se concluyó que se pudo constatar que el área de informática no cumplía con los requerimientos que establecen las Normas de Control Interno y las Normas del INEI, dejando las recomendaciones específicas para cada observación.

1.2 JUSTIFICACIÓN.

Desde el punto de vista social es importante por el impacto que se evidenciara con la auditoría a la empresa Sociedad Agrícola Drokasa S. A., en el que se evaluó la eficiencia del manejo de sus tecnologías de información, ya que es muy imprescindible y de vital importancia para el desempeño de los sistemas información como factor crítico de éxito para las organizaciones, y por lo tanto se debe tener mucho énfasis en la aplicación para llevar acabo la inspección y verificación del estado e instalación de los equipos, por medio de estrategias y el planteamiento de medidas correctivas y recomendaciones necesarias a las observaciones; y que de una manera indirecta se

permitirá brindar un mejor servicios a los usuarios internos y externos a la organización.

Desde el punto de vista de conocimiento, permitir aplicar metodologías existentes que manejan estándares internacionales, para validar y permitir una mejor evaluación e identificando las vulnerabilidades, fallas y riesgos, también le permitirá comprobar su calidad y capacidad en cuanto a los requerimientos de los sistemas informáticos.

1.3 PROBLEMA.

DESCRIPCIÓN DEL PROBLEMA

La investigación surge a raíz que en todo ámbito organizacional se requiere información oportuna y confiable para la toma de decisiones, realidad que ha permitido el desarrollo de sistemas de información.

La empresa AGROKASA no siendo la excepción, que para el desarrollo de sus actividades comerciales y financieras utiliza TI, sin embargo, no es ajena a los diversos problemas en cuanto a seguridad informática, se ha podido observar que no existe preocupación por establecer una cultura de seguridad informática a nivel de toda la empresa.

Descuido general con sus equipos tanto como su ubicación, debido a ello toda la información que se procesa en las diversas áreas de la empresa son vulnerables a riesgos como pérdida total o parcial de la información porque se observó que el cuarto de CPD no hay aviso de zona restringida.

El mantenimiento que realizan es correctivo y en plena producción causaría grandes problemas, como pérdidas económicas por parada de máquina, molestias en el ambiente de trabajo del personal y puede traer como consecuencia demasiados gastos en el área de TI ya que no cuenta con una programación de mantenimiento preventivo.

La empresa cuenta con diferentes áreas administrativas, la cual en cada área cuenta con varios equipos de cómputo e impresoras y por el tamaño del ambiente y la cantidad de personas dentro del área no tiene una buena condición ambiental y tanto pasa lo

mismo en el CPD, que esto pone en riesgo el funcionamiento de los sistemas y en general requiere un control ambiental, con respecto al calor que generan los equipos

La empresa hasta la fecha no ha realizado ninguna auditoría referente al tema de uso de la tecnología y a la gestión de la seguridad de la información, ni tampoco al análisis de riesgos informáticos.

Ante estos problemas nace el presente trabajo de investigación que permitirá mejorar el Área de Sistemas de la empresa AGROKASA - Supe.

FORMULACIÓN DE LA INTERROGATIVA DEL PROBLEMA

¿Cómo desarrollar una auditoria de seguridad física aplicando la norma ISO 27002 a la empresa AGROKASA Supe - 2016?

1.4 MARCO REFERENCIAL

Seguridad Informática

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Fundamentos:

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos (ISO, 2012)**.**

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades.

La información adopta diversas formas. Puede estar impresa o escrita en papel almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar La continuidad del negocio, minimizar los daños a la organización y maximizar el retomo de las inversiones y las oportunidades de negocios.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización. (NORMA TÉCNICA PERUANA, 2007)

Seguridad Física

La seguridad física cubre todo lo referido a los equipos informáticos: ordenadores de propósito general, servidores especializados y equipamiento de red. La seguridad lógica se refiere a las distintas aplicaciones que ejecutan en cada uno de estos equipos.

Las amenazas contra la seguridad física son:

- **Desastres naturales** (incendios, inundaciones, hundimientos, terremotos). Los tenemos en cuenta a la hora de ubicar el emplazamiento del centro de proceso de datos (CPD), donde alojamos los principales servidores de la empresa; pero, aunque tengamos el mejor sistema de extinción de incendios o la sala esté perfectamente sellada, siempre deberíamos tener un segundo CPD para que la actividad no pare.
- **Robos.** Nuestros equipos, y sobre todo la información que contienen, resultan valiosos para otros individuos u organizaciones. Debemos proteger el acceso a la sala del CPD mediante múltiples medidas de seguridad: vigilantes, tarjetas de acceso, identificación mediante usuario y contraseña, etc.
- **Fallos de suministro.** Los ordenadores utilizan corriente eléctrica para funcionar y necesitan redes externas para comunicar con otras empresas y con los clientes. Estos servicios los contrataremos con determinados suministradores, pero debemos estar preparados para las ocasiones en que no puedan proporcionarlo: unas baterías o un grupo electrógeno por si falla la corriente, una segunda conexión a Internet como línea de backup, incluso podemos optar por una solución inalámbrica— para estar protegidos ante un corte en la calle.

Por otro lado, podemos hablar de seguridad activa y seguridad pasiva.

La seguridad pasiva son todos los mecanismos que, cuando sufrimos un ataque, nos permiten recuperarnos razonablemente bien. Por ejemplo, las baterías ante una caída de tensión o la copia de seguridad cuando se ha estropeado la información de un disco.

La seguridad activa intenta protegernos de los ataques mediante la adopción de medidas que protejan los activos de la empresa, como vimos en el epígrafe anterior: equipos, aplicaciones, datos y comunicaciones. (Buendía, 2013)

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control para protección de las amenazas a los recursos (redUSERS, 2011)

Podemos definir la **Seguridad Informática** como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan con llevar daños sobre la información, comprometer su

confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (Vieites, 2014)

Auditoría

Conceptualmente la auditoria, toda y cualquier auditoria, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

TABLA 1 CONCEPTO DE LOS ELEMENTOS FUNDAMENTALES

1. contenido:	una **opinión**
2. contenido:	**profesional**
3. justificación:	Sustentada en determinados **procedimientos**
4. objetivo:	Una determinada información obtenida en un cierto soporte
5. finalidad:	Determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su **finalidad.**

Fuente: Auditoría informática un enfoque práctico.

En todo caso es una función que se acomete a posterior, en relación era actividades ya realizadas, sobre las que hay que emitir una opinión.

Clases de Auditoría

Los elementos 4 y 5 distinguen de qué clase o tipo de auditoria se trata. El objeto sometido a estudio, sea cual sea su soporte, por una parte, y la finalidad con que se realiza el estudio, definen el tipo de auditoría de que se trata. A título ilustrativo podríamos enumerar entre otras:

TABLA 2 CLASES DE AUDITORÍA

Clase	Contenido	Objetivo	Finalidad
Financiera	Opinión	Cuentas anuales	Presentan realidad
Informática	Opinión	Sistemas de aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas.
Gestión	Opinión	Dirección	Eficiencia, eficiencia, economicidad.
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas.

Fuente: Auditoría Informática un enfoque práctico

Auditoría Informática

Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momento del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnica mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, porque te deberá emplear software de auditoría y otras técnicas asistidas por computador.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por un auditor informático:

• Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases análogas de realización de cambios importantes.

• Revisar y juzgar los controles implantados en los sistemas informativos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.

• Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

La Auditoría Física

Lo físico en Informática, hasta ahora, ha tenido una importancia relativa: no en vano se ha visto siempre como algo que soporta lo que, en realidad, es la Informática, y que ocupa un lugar en la mesa.

La UCP (enorme), la pantalla, el teclado, la impresora, cables... y. además, el ratón con su alfombrilla que impiden extender libros y papeles sobre un espacio que, incomprensiblemente, por grande que sea, no existe.

Pero lo físico en Informática no se reduce únicamente a lo expuesto, esto es: dar un soporte tangible, un continente o vehículo a lo etéreo del software, verdadera esencia informática. Todo cuanto rodea o se incluye en el computado, también este mismo, son lo físico como tal, así como otros conceptos o virtualidades que, de una u otra forma, influyen o toman su razón de ser en el Entorno Físico del computador como generalidad o en el del CPD como Unidad Física Informática.

La Auditoría es el medio que va a proporcionar la evidencia o no de la Seguridad física en el ámbito en el que se va a desarrollar la labor profesional. Es por tanto, necesario asumir que la Auditoría Física no se debe limitar a comprobar la existencia de los medios físicos, sino también su funcionalidad, racionalidad y seguridad.

La Seguridad Física

No están muy claras las fronteras que delimitan, si es que lo hacen, los dominios y responsabilidades de los tres tipos de seguridad que a los usuarios de la Informática deben interesar: seguridad lógica, seguridad física y seguridad de las Comunicaciones.

Quizá fuera más práctico aunarlas y obtener una seguridad integral, aunque hay que reconocer las diferencias que, evidentemente, existen entre soft. hard. hard-soft, hard que soporta al soft y soft que mueve al hard.

La **seguridad física** garantiza la integridad de los activos humanos, lógicos y materiales de un CPD. (Piattini & Del Peso, 2001).

Auditoría: Con frecuencia la palabra auditoría se ha empleado incorrectamente y se le ha considerado como una evaluación cuyo único fin se detecta errores y señalar fallas. Por eso se ha llegado a usar la frase "tiene auditorias" como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría.

La palabra auditoría viene del latín *auditorius*, y de ésta proviene "auditor", el que tiene la virtud de oír; el diccionario lo define como "revisor de cuentas colegiado".

La auditoría no es una virtud meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguirse y estimar los resultados obtenidos. (Echenique García, 2001).

1.5 HIPÓTESIS

En vista de que la investigación tiene un alcance de carácter descriptivo y consiste en realizar una auditoría física a las TI utilizando la norma ISO 27002 en la empresa AGROKASA, la cual no es posible plantear una hipótesis debido a que no se intenta correlacionar o explicar causalidad de variables, debido a ello es que la hipótesis es Implícita.

1.6 OBJETIVOS

1.6.1 Objetivo General:

- Desarrollar una Auditoria de Seguridad Física de la Empresa AGROKASA-Supe, mediante los controles de la norma ISO 27002.

1.6.2 Objetivos Específicos:

- Revisar la organización su administración y estructura de la seguridad física.
- Verificar el cumplimiento de las políticas y otras medidas de seguridad informática establecidas por la norma.
- Aplicar la auditoria y determinar en qué medida se cumple con la implementación de requerimientos de seguridad física, en el área de informática de la empresa AGROKASA.

METODOLOGÍA DEL TRABAJO

2.1. TIPO Y DISEÑO DE INVESTIGACIÓN

2.1.1. TIPO DE LA INVESTIGACIÓN

- Según el propósito de la investigación:
  El presente trabajo de investigación es de tipo APLICADA; Se caracteriza porque busca la aplicación de conocimientos adquiridos durante el proceso de investigación.
- Según el nivel de conocimientos que se adquieren:
  Es DESCRIPTIVO, ya que permite obtener datos mediante instrumentos y técnicas de recolección de datos para luego describir la situación en que se encuentra una realidad.

2.1.2. DISEÑO DE LA INVESTIGACIÓN

- No experimental porque no pretende demostrar los resultados y transversal debido a que el estudio se realiza en un determinado momento.

2.2. TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN.

Usaremos las siguiente Técnicas:

- Entrevistas.

- Cuestionarios (Listas de verificación).

Usaremos los siguientes Instrumentos:

- Guía de Entrevistas.

- Cuestionario de preguntas.

2.3. METODOLOGIA

FASES DE LA AUDITORÍA FÍSICA

Siguiendo la Metodología resumida de EDPAA (Asociación de Auditores en Procesamiento de Datos Electrónicos), y sin perjuicio de alguna pequeña diferencia, más que nada en el orden o el ámbito de las fases, el Ciclo de Vida quedaría:

- Alcance de la Auditoría.

- Adquisición de Información General.

- Administración y Planificación.

- Ejecución de auditoria.

- Resultado.

ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2005

ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013.

El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995. En el año 2000 la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional publicaron el estándar ISO/IEC 17799:2000, con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento modificado ISO/IEC 17799:2005.

Con la aprobación de la norma ISO/IEZAC 27001 en octubre de 2005 y la reserva de la numeración 27.000 para la Seguridad de la Información, el estándar IGFSO/DIEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en el año 2007.

En Perú la ISO/IEC 17799:2000 es de uso obligatorio en todas las instituciones públicas desde agosto del 2004, estandarizando de esta forma los diversos proyectos y metodologías en este campo, respondiendo a la necesidad de seguridad por el uso intensivo de Internet y redes de datos institucionales, la supervisión de su cumplimiento está a cargo de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI (www.ongei.gob.pe).

Estructura General de la Norma

Este estándar contiene 11 cláusulas o dominios de control de seguridad conteniendo colectivamente un total de 39 categorías de objetivos de seguridad principal, 133 controles y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

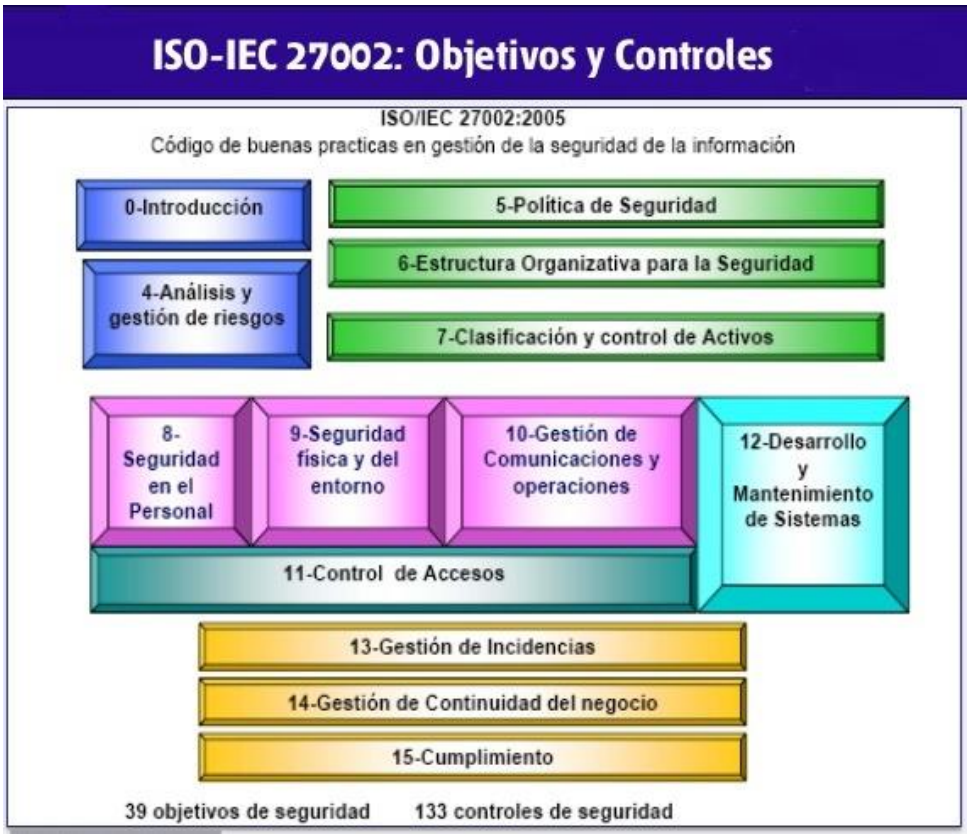


Figura 01: Estructura del ISO 27002.

Fuente: Manuel Fernández "Normas ISO Relativas a TICs" Pagina 29.

I. Evaluación y tratamiento del riesgo

a. Evaluación de los riesgos de seguridad

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

Tratamiento de los riesgos de seguridad

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es efectivo en costo para la organización. Estas decisiones debieran ser registradas.

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

a) aplicar los controles apropiados para reducir los riesgos;

b) aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;

c) evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;

d) transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo. Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

a) los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales:

b) objetivos organizacionales;

c) requerimientos y restricciones operacionales;

d) costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;

e) la necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas de la organización. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o medio ambiente, y podría no ser practicable en todas las organizaciones. Como ejemplo, 10.1.3 describe cómo se pueden segregar las tareas para evitar el fraude y el error. En las organizaciones más pequeñas puede no ser posible segregar todas las tareas y pueden ser necesarias otras maneras para lograr el mismo objetivo de control. En otro ejemplo, 10.10 describe cómo se debiera monitorear el uso del sistema y recolectar la evidencia. Los controles descritos; por ejemplo, bitácora de eventos; podrían entrar en conflicto con la

legislación aplicable, como la protección de la privacidad para los clientes o en el centro de trabajo.

Descripción De Los Dominios

1. **Políticas de Seguridad.**
2. **Organización de la Seguridad de Información.**
3. **Gestión de Activos.**
4. **Seguridad ligada a los Recursos Humanos.**
5. **Seguridad Física y del Entorno.** (es el dominio 9 en la norma)

- También se menciona los controles que contiene este dominio

5.1. Áreas seguras

- Objetivo:

Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.

- Principios:

Los servicios de procesamiento de información sensible deberían ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias.

La protección suministrada debería estar acorde con los riesgos identificados.

5.1.1. Perímetro de seguridad física.

Control: Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.

5.1.2. Controles físicos de entrada.

Control: Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.

5.1.3. Seguridad de oficinas, despachos y recursos.

Control: Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.

5.1.4. Protección contra amenazas externas y del entorno.

Control: Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.

5.1.5. El trabajo en áreas seguras.

Control: Se debería diseñar y aplicar protección física y pautas para trabajar en las áreas seguras.

5.1.6. Áreas aisladas de carga y descarga.

Control: Se deberían controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados y, si es posible, aislarlas de los recursos para el tratamiento de la información.

5.2. Seguridad de los equipos.

- Objetivo:

Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.

- Principios:

Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

Así mismo, se debería considerar la ubicación y eliminación de los equipos.

Se podrían requerir controles especiales para la protección contra amenazas físicas y para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.

5.2.1. Instalación y protección de equipos.

Control: El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.

5.2.2. Suministro eléctrico.

Control: Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.

5.2.3. Seguridad del cableado.

Control: Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.

5.2.4. Mantenimiento de equipos.

Control: Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.

5.2.5. Seguridad de equipos fuera de los locales de la Organización.

Control: Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos.

5.2.6. Seguridad en la reutilización o eliminación de equipos.

Control: Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación.

5.2.7. Traslado de activos.

Control: No deberían sacarse equipos, información o software fuera del local sin una autorización.

6. **Gestión de Comunicaciones y Operaciones.**
7. **Control de Accesos.**
8. **Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.**
9. **Gestión de Incidentes de Seguridad de la Información.**
10. **Gestión de Continuidad del Negocio.**
11. **Conformidad. (MarcadorDePosición1)**

ANÁLISIS DE BRECHAS (Gap Analysis)

Es un análisis que mide cómo una organización está llevando a cabo su desempeño con respecto a una serie de criterios establecidos en base a normas o procedimientos internos, controles seleccionados, las mejores prácticas de competencia, etc.

El objetivo principal de este análisis es conocer el diferencial en el desempeño de una organización respecto a las mejores prácticas, estándares, regulaciones legales; evaluar la desviación y establecer los planes para dirigir la organización hacia el cumplimiento de las mismas. Esta diferencia entre el estándar y la realidad del cliente es lo que conocemos como Gap Análisis o brecha. El análisis responde dos interrogantes: ¿dónde estamos? y ¿dónde deberíamos estar?

En otras palabras, un GAP Análisis compara lo que existe actualmente en una organización contra lo que es requerido en seguridad de la información. Los requerimientos se derivan de los estándares, leyes y regulaciones que gobiernan una empresa o industria en particular.

Esto le permite a la empresa identificar aquellas áreas en las cuales existe un espacio para mejorar.

Beneficios:

- Fundamentos para establecer la estrategia y cerrar la brecha de seguridad (Security GAP) existente.
- Cumplir con los estándares, leyes y regulaciones exigidos.
- Proteger los activos de información
- Mejorar los procesos de gestión de tecnología de información.

RESULTADOS

APLICACIÓN DE LA METODOLOGÍA

Desarrollo De La Auditoría Física

Alcance de la Auditoría

Se auditarán las áreas de la empresa tales como almacén, recursos humanos, bienestar social, logística, calidad, producción, mantenimiento e informática, en las cuales se verificará la vulnerabilidad de los equipos y la información.

Para la evaluación se utilizará como herramienta la norma ISO 27002:2005, tomando el dominio 9 (9.1 – 9.2) establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en la organización, que define claramente el punto en evaluación, que a los objetivos plasmados concretos a la auditoria en cuantos a la seguridad física y del entorno en cuanto a la Tecnología de la información, que debe centrarse en el análisis de la evaluación de los riesgos del tipo y la planificación de las actividades preventivas y de la organización de los recursos necesarios para realizarlas y el cual evaluara al área de Informática, el proceso de seguridad de equipos que trabajan con herramientas computacionales, que se divide en dos departamentos Jefatura y mantenimiento, que realizan los backup de los datos de cada área de la empresa, mantenimiento de los equipos, ver la conectividad vía wifi en producción, etc.

Por lo tanto, la auditoría no tiene como objetivo la seguridad del perímetro, seguridad de la oficina y contra amenazas externas (materiales peligrosos, estándares de salud).

Información General de la Empresa

Datos Del Cliente:

Destinado al área de Informática

Descripción De La Organización:

Sociedad Agrícola Drokasa. S.A. – AGROKASA - Surge en 1996 como respuesta de un importante grupo empresarial familiar peruano Corporación Drokasa S.A., fundado

en 1951. Líder en los mercados de fabricación y distribución de productos farmacéuticos y bienes de consumo, a partir del fenómeno de la Globalización el grupo ingreso al negocio de la agricultura.

Laboratorios Farmindustria y Pharmalab, empresas farmacéuticas del grupo, representan, unidas, el más grande fabricante/distribuidor de productos farmacéuticos del Perú. Durante más de 50 años nos hemos desenvuelto exitosamente en un mercado en el que la calidad era y es, el mayor atributo de éxito.

Al emprender el negocio agrícola, entendimos desde el principio las necesidades de calidad certificada, excelencia logística, exigencias de cumplimiento en las ofertas y sobre todo confiabilidad en las relaciones con nuestros socios comerciales.

En tan sólo 8 años desde nuestra fundación, nos hemos convertido en el exportador número uno de espárrago fresco y uva de mesa en el Perú.

Logotipo De La Organización

Figura 02: Logotipo de la empresa.
Fuente: www.agrokasa.com

Razón social de la organización

Sociedad Agrícola Drokasa S.A

Ubicación

Av. Panamericana norte km. 184.5 supe puerto - barranca

RUC 20325117835

Teléfono 012365454

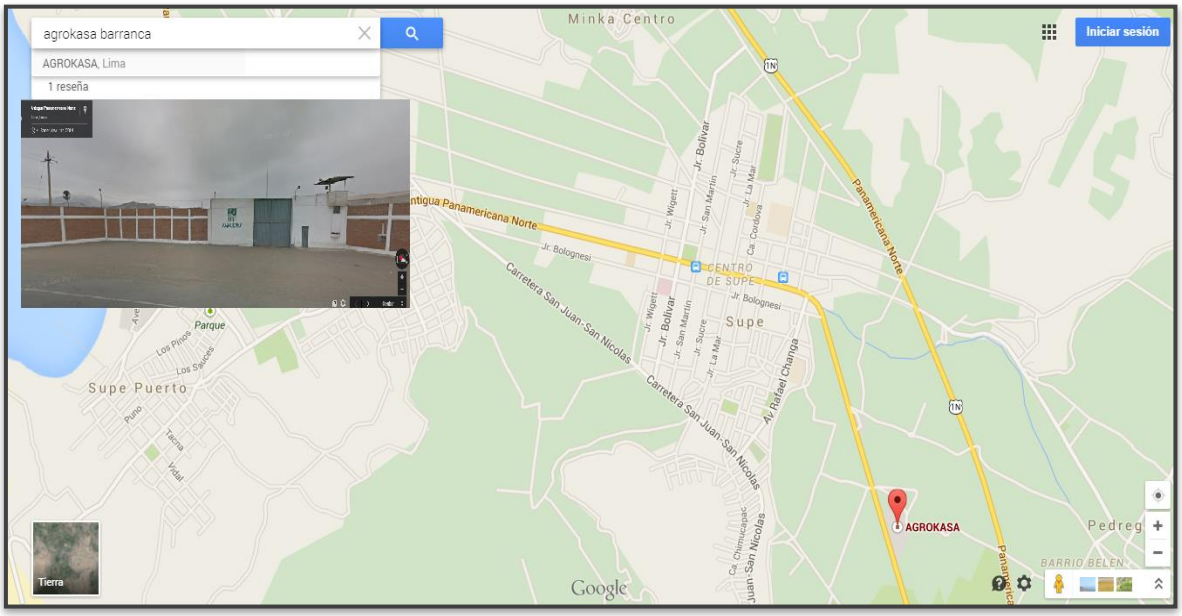


Figura 03: Ubicación de la empresa.

Fuente: Google Earth.

Misión:

AGROKASA produce, empaca y comercializa espárragos, paltas y uvas de mesa, en la condición de frescos, cumpliendo con las necesidades de nuestros clientes y llevando a cabo sus actividades en base a las siguientes premisas.

• Invirtiendo en el desarrollo humano y tecnológico de nuestros colaboradores, asegurándonos de contar con equipos y procesos de vanguardia y promoviendo la mejora continua en todas las fases del negocio.

• Respetando el Medio Ambiente, velando por la Salud Ocupacional de nuestros colaboradores y manteniendo una relación de apoyo con las Comunidades en las que desarrollamos nuestras actividades.

• Alineando los intereses de nuestros Clientes y los del Entorno Local con los de nuestros Colaboradores y Accionistas.

Visión:

AGROKASA será reconocida por sus clientes, por la calidad superior de sus productos, y servicios de atención logística y comercial que les brindamos.

AGROKASA mantendrá su posición de liderazgo nacional en la exportación de productos frescos, con la participación de espárragos, uvas de mesa, y paltas.

AGROKASA sustentará su éxito en la oportuna adecuación al cambio, mediante la permanente promoción de la innovación como medio generador de valor para la empresa.

AGROKASA será una empresa en la que será un orgullo trabajar por el nivel de exigencia profesional, por las relaciones con la comunidad, por el compromiso con la seguridad y salud ocupacional, así como por el respeto del medio ambiente.

Organigrama

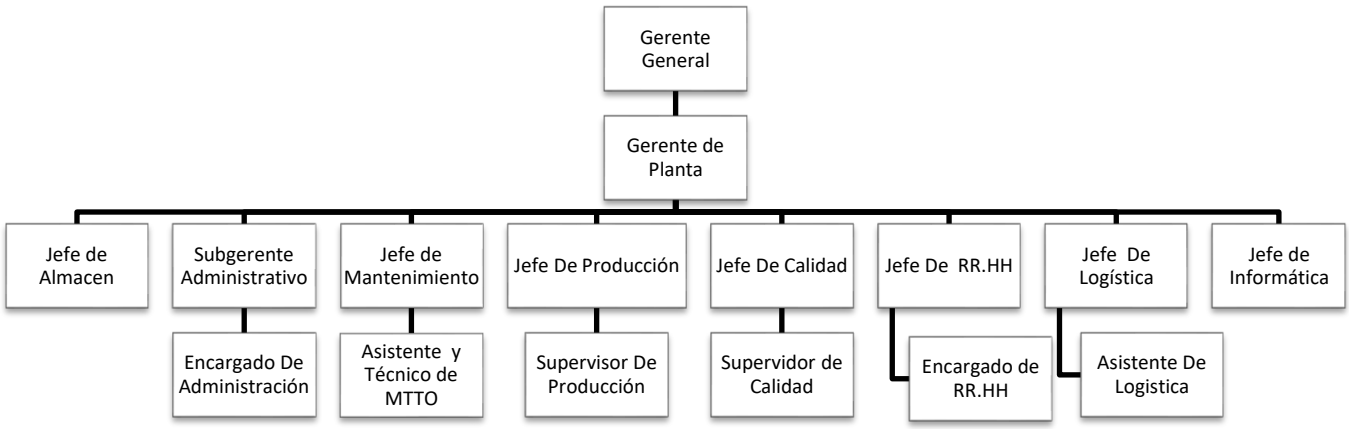


Figura 04: Organigrama de la empresa

Fuente: Elaboración propia.

Planificación, Desarrollo y Ejecución de la Auditoria

Este estudio se limita a considerar la seguridad de los Sistemas de Información, entendidos como sus mecanismos de soporte y tratamiento automatizables y no

naturales, incluyendo de entrada por ejemplo bases de datos, discos o disquetes, pero no incluyendo por ejemplo las películas o las conversaciones.

Estudio inicial

El objetivo es realizar un diagnóstico primario, rápido y no invasivo, para brindar al directorio, al Gerente General o a quién corresponda tomar la decisión, un primer enfoque de la problemática.

En este estudio el alcance de la evaluación del riesgo de seguridad comprende el área de informática, por ser el centro que soporta las operaciones administrativas de suma importancia para la empresa AGROKASA.

Para la evaluación de la seguridad física del Área de Informática se llevarán a cabo las siguientes actividades:

- Definición del alcance y objetivos.
- Estudio y evaluación del control interno.

Gestión Administrativa:

- Conocer y analizar las operaciones a las cuales se dedica el negocio y la forma en que está estructurado tanto desde el punto de vista organizacional y administrativo, así como el organigrama, número y distribución de empleados, sistema interno de autorizaciones, firmas, formularios utilizados, secuencia de operaciones y otros aspectos similares.
- Verificar si se ha diseñado un manual de organización y funciones a ser aplicado a los y por los usuarios del área de informática.
- Verificar si las contrataciones del personal del área de informática se han realizado con base a los criterios establecidos en el manual de funciones y cumplen el perfil del puesto.
- Verificar si la administración promueve la capacitación y adiestramiento constante del personal del área de informática.

- Verificar que las instalaciones donde labora el personal del área de informática estén adecuadas a las necesidades y no representen peligro para los empleados.

Gestión Informática:

Examinar la información preliminar correspondiente al área de informática, la cual puede ser:

Interna: conocer los procesos que se realizan dentro de la empresa para los cuales es utilizado el equipo informático. Se verificará si se lleva un control de las operaciones realizadas y si queda un registro de los usuarios del área de informática y los horarios en los cuales, han utilizado el equipo del centro.

Externa: Conocimiento e identificación de los usuarios del área de informática, así como de los proveedores de materiales y accesorios y otros.

- Conocimiento de las instalaciones físicas del negocio, materiales, mobiliario, inmuebles, equipos, inventarios y otros que tienen relación al área de informática.
- Solicitar las políticas, medidas de seguridad para la protección y control de ingreso al área, restricciones y autorizaciones, programas de prevención contra desastres.
- Solicitar documentación, políticas de seguridad, controles especiales para la protección de equipos, planes de mantenimiento de quipos, etc.
- Solicitar manuales técnicos, de operación del usuario y comprobar su actualización.
- Verificar si todo el equipo o hardware se encuentra debidamente inventariado y se ha elaborado la respectiva tarjeta de depreciación del mismo, a fin de que en el momento en que se vuelvan obsoletos se puedan dar de baja.
- Verificación documental y física de las adquisiciones de bienes del área de informática.
- Verificar si cuentan con áreas seguras, protegidos por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados que protejan la información y los medios de procesamiento de información. Comprobar los controles físicos de ingreso a la dependencia.

- Elaborar los cuestionarios para entrevistar al personal del área de Informática.

Para conocer el funcionamiento del departamento de informática dentro de la entidad, se diseñará un cuestionario en el cual se harán en su mayoría preguntas cerradas, con el propósito de conocer las actividades dentro del área, con el fin de detectar posibles fallas y con base en ello, detectar la clase de riesgo que presenten cada una de las operaciones y procedimientos. Dichos datos servirán en su conjunto para la realización del GAP análisis.

- Realizar las entrevistas a los principales responsables del Centro de Informática utilizar como herramienta los cuestionarios previamente elaborados.
- Procesamiento de la información obtenida para conocer el diferencial en el desempeño de la organización con respecto a las mejores prácticas establecidas en la Normativa utilizada para nuestro estudio, GAP análisis.
- Documentación adecuada de hallazgos.
- Recomendaciones.

Métodos aplicables para su documentación:

Descriptivo: La documentación utilizada, será en primer lugar de tipo descriptiva o sea basada en la narración verbal de los procedimientos.

Cuestionario: En segundo lugar, los procedimientos se documentarán a través de la pre-elaboración de preguntas, contestadas personalmente por los líderes de la empresa o por el personal encargado de los sistemas informáticos y por algunos usuarios dentro de la empresa que tenga relación con el mismo.

- Se presentará más adelante el cuestionario de requerimientos de la norma ISO 27002.

Análisis de brecha

El diagnóstico de la seguridad física hallada en el área de informática de la empresa AGROKASA, se basa en el cuestionario de verificación de requerimientos de la norma ISO 27002 presentado más adelante, para fines de este estudio se contempla los siguientes aspectos:

Seguridad física y del entorno

- ✓ Áreas Seguras
- ✓ Seguridad de los equipos

La **tabla 2** contiene análisis de brechas que muestra el grado de cumplimiento de los aspectos relacionados a la adecuación del plan de seguridad y requerimientos ISO 27002, se describe a continuación el contenido:

- **Mejores prácticas*:***

Muestra un resumen de aquellas actividades críticas que deberán alinearse con los requerimientos definidos por el estándar ISO 27002.

- **Análisis de brecha:**

Muestra de manera gráfica la brecha existente entre la situación actual encontrada en la empresa AGROKASA y los requerimientos del estándar.

TABLA 3 DESCRIPCIÓN DE GRÁFICOS

	Razonablemente cubierto	Los requerimientos ISO 27002 están razonablemente cubiertos.
	Sustancialmente cubierto	Falta realizar algunas actividades para cubrir razonablemente los requerimientos ISO 27002.
	Parcialmente cubierto	Se han realizado actividades que cubren parcialmente los requerimientos ISO 27002.
	Limitadamente cubierto	Se han realizado algunas actividades para cubrir los requerimientos ISO 27002.
	No cubierto	No se ha realizado ninguna actividad relacionada con los requerimientos ISO 27002.

Fuente: Elaboración Propia

TABLA 4 MATRIZ ANÁLISIS DE BRECHA

MEJORES PRÁCTICAS ISO 27002				ANÁLISIS DE BRECHA
9. SEGURIDAD FÍSICA Y AMBIENTAL				
9.1. Áreas Seguras				
Descripción del control	**Recomendado por la norma**	**Situación del Área de Informática**	**Sugerencias**	**Estado**
9.1.1 Perímetro de Seguridad Física	Los perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.	No cubierto	• Definir claramente los perímetros de seguridad y la ubicación y la fortaleza de cada perímetro deberían depender de los requisitos de seguridad de los activos dentro del perímetro. • Los perímetros de seguridad deben estar rodeados de paredes sólidas y las puertas y ventanas deben estar debidamente protegidas con alarma, cerraduras y cámaras de video • Se debe establecer un área de recepción con personal u otro medio par a controlar el acceso físico al perímetro de seguridad. • Evitar tener ventanas que colinden con el exterior dentro de los perímetros de seguridad. • Disponer de cámaras de video en el interior y exterior (puertas de ingreso y puertas de escape, ventanas) de los perímetros de seguridad.	

9.1.2 Controles físicos de entrada	Las áreas seguras deben ser protegidas con apropiados controles de ingreso que garanticen que solo se permite el acceso a personas autorizadas.	No cubierto	• Se debe registrar la fecha y la hora de entrada y salida del visitante, quien tiene que estar debidamente autorizado. La autorización de ingreso debe ser para un propósito específico y el visitante debe ser informado de los requerimientos de seguridad del área. • Utilizar controles de autenticación; por ejemplo, tarjetas electrónicas de identificación; para autorizar y validar todos los accesos; se debiera mantener un rastro de auditoría de todos los accesos a áreas donde se procesa o almacena información sensible. • Todos los usuarios empleados y terceras personas y todos los visitantes deben usar alguna forma de identificación visible. El personal de seguridad debe verificar que esta condición se cumpla. • Los derechos de acceso a áreas seguras debieran ser revisados y actualizados regularmente, y revocados cuando sea necesario	
9.1.3 Aseguramiento de oficinas, salas de servidores e instalaciones	La seguridad física debe ser diseñada y aplicada a las oficinas, recintos e instalaciones.	No cubierto	• Se debieran considerar los siguientes lineamientos para asegurar las oficinas, habitaciones y medios: ▪ El recinto donde se encuentra almacenada la información confidencial no debe ser de conocimiento y acceso público. Las puertas y las ventanas deberán permanecer cerradas cuando estén desatendidas	
9.1.4 Protección contra amenazas externas y ambientales	Se recomienda diseñar y aplicar medios de protección contra daños potenciales causados por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o causado por el hombre.	Limitadamente cubierto	▪ Los materiales peligrosos o combustibles debieran ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no debieran almacenarse en el área asegurada; ▪ El equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal; se debiera proporcionar equipo contra-incendios ubicado adecuadamente.	

9.1.5 Trabajo en áreas restringidas	Se recomienda que se diseñe y aplique protección física y las directrices para el trabajo en áreas protegidas.	No cubierto	▪ El personal solo tendrá conocimiento de la existencia o realización de actividades en un área segura en caso que necesite conocerlo. ▪ El trabajo no supervisado en las áreas seguras deberá evitarse no solo por razones de seguridad sino para evitar oportunidades de actividades malintencionadas. ▪ Las áreas seguras vacías deberán estar físicamente cerradas y ser inspeccionadas periódicamente. ▪ El personal de servicios de apoyo ajeno deberá tener acceso restringido a las áreas seguras o facilidades para el procesamiento de información sensible solo cuando sea imprescindible. Dicho acceso deberá estar supervisado y ser monitoreado. ▪ Podrían necesitarse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad dentro del perímetro de seguridad. ▪ No se debe permitir equipamiento fotográfico, de video, de audio u otro, a menos que se autorice expresamente.	
9.1.6 Acceso público, envíos y áreas de carga	Se recomienda que se controles los puntos de acceso, como las áreas de entrega y carga y otros puntos donde personas sin autorización pueden llegar a entrar a las instalaciones y de ser posible, se aíslen de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.	No cubierto	▪ El acceso a un área de carga y descarga desde fuera del edificio deberá estar limitado al personal identificado y autorizado. ▪ El área de carga y descarga deberá estar diseñada para que el personal asociado haga su trabajo sin tener acceso a otras partes del edificio. ▪ Las puertas externas de un área de carga y descarga deberán asegurarse cuando se abra la puerta interna. ▪ El material que se reciba deberá ser inspeccionado en busca de peligros potenciales antes de que se traslade del área de descarga al punto de uso. ▪ El material que se reciba deberá ser registrado a su entrada a la instalación en caso que sea necesario.	

9.2. Seguridad de los equipos				
9.2.1 Ubicación y protección de equipos tecnológicos	Los equipos deben ser ubicados o protegidos para reducir los riesgos de amenazas y peligros ambientales y protegerse de accesos no autorizados.	Limitadamente cubierto	▪ El equipo debe estar ubicado de manera que se minimice el acceso innecesario a las áreas de trabajo; ▪ Los medios de procesamiento de la información que manejan data confidencial deben ubicarse de tal manera que se reduzca el riesgo de que alguien pueda tener acceso visual a ellas durante su uso. ▪ Se deberán adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo. ▪ Establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información; ▪ Monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información; ▪ Deberá tenerse en cuenta el impacto de desastres que tengan lugar en instalaciones cercanas, por ejemplo, un incendio en un edificio vecino, fuga de agua desde el techo o en pisos por debajo del nivel del suelo, o una explosión en la calle.	
9.2.2 Seguridad en el suministro de electricidad y servicios	Los equipos deben ser protegidos frente a fallas o interrupciones de energía (fluido eléctrico), causadas por fallas de las utilidades de soporte (UPS, ventilación, suministro de agua, aire acondicionado)	Limitadamente cubierto	Las opciones para alcanzar una continuidad del suministro eléctrico incluyen: ▪ Cables de suministro múltiples para evitar que haya solo un punto de fallo en la alimentación; ▪ Fuentes de alimentación ininterrumpida (UPS); ▪ Generador de apoyo.	

9.2.3 Seguridad en el cableado	El cableado eléctrico y de datos debe ser protegido frente a daños e interceptaciones.	Limitadamente cubierto	▪ Las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información deben ser subterráneas donde sea posible, o estar sujetas a una alternativa de protección adecuada; ▪ El cableado de la red debe estar protegido contra intercepciones no autorizadas o daños, por ejemplo, mediante el uso de canales de protección o evitando las rutas a través de áreas públicas; ▪ Los cables de energía deben estar separados de los cables de comunicaciones para evitar la interferencia; ▪ Se debieran utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados;	
9.2.4 Mantenimiento de equipos	Se recomienda que el equipamiento reciba el correcto mantenimiento para asegurar su disponibilidad e integridad continuas.	Parcialmente cubierto	▪ El equipamiento deberá recibir el mantenimiento de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante. ▪ Solo el personal de mantenimiento autorizado deberá llevar a cabo las reparaciones y el servicio a los equipos. ▪ Se deberán llevar registros de todas las fallas reales y del mantenimiento preventivo y correctivo. ▪ Se deberán controlar los envíos de equipamiento fuera de las instalaciones para que reciban mantenimiento. Esto deberá hacerse de conformidad con todos los requerimientos impuestos por las pólizas de seguro.	
9.2.5 Seguridad de equipos fuera de las áreas seguras	Se recomienda que se aplique la seguridad al equipamiento que este fuera del ámbito de la organización considerando los diferentes riesgos a los que están expuestos.	No cubierto	▪ El equipamiento y los medios que se saquen de las instalaciones no se deberán dejar desatendidos en lugares públicos. Las computadoras portátiles deberán llevarse como equipaje de mano y disfrazadas como sea posible cuando se viaje. Deberán observarse en todo momento las instrucciones de los fabricantes para equipamiento de protección, por ejemplo, la protección contra la exposición a fuertes campos electromagnéticos. ▪ Los controles para el trabajo en la casa deberán estar determinados por una evaluación de riesgos y controles adecuados aplicados según corresponda, por ejemplo, archiveros bajo llave, política de escritorio despejado y controles de acceso para computadoras. ▪ Deberán ponerse en vigor las pólizas de seguro adecuadas para proteger el equipamiento fuera de las instalaciones.	

9.2.6 Destrucción y reutilización de equipos	Todos los componentes de los equipos que contienen medios de almacenamiento deben ser chequeados para asegurar que datos reservados o confidenciales o software licenciado sean removidos antes de que estén disponibles a otras personas.	No cubierto	▪ Los dispositivos que contienen información confidencial debieran ser físicamente destruidos o se debieran destruir, borrar o sobre-escribir la información utilizando técnicas que hagan imposible recuperar la información original, en lugar de simplemente utilizar la función estándar de borrar o formatear. ▪ Los dispositivos que contienen data confidencial pueden requerir una evaluación del riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar	
9.2.7 Autorización de sacar equipos	Se recomienda que el equipamiento, la información o el software no se retiren de las instalaciones sin previa autorización.	No cubierto	▪ El equipamiento, la información o el software no deberán sacarse del local de trabajo sin autorización. ▪ Donde sea necesario y apropiado, el equipamiento deberá registrarse a la salida y a la entrada al devolverse. ▪ Se debieran establecer límites de tiempo para el retiro del equipo y se debieran realizar un chequeo de la devolución; ▪ Los usuarios empleados, contratistas y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera del local debieran estar claramente identificados; ▪ Se deberán realizar inspecciones al azar para detectar las extracciones no autorizadas. Las personas deberán tener conocimiento de que se realizarán dichas inspecciones	

Fuente: Elaboración Propia

ANÁLISIS

Tras haber realizado la recolección general de información según lo descrito en los anteriores apartados, se procedió al análisis de toda la información recogida y situaciones existentes, estudiando las posibles carencias en seguridad de la información tomando como punto de referencia las buenas prácticas de la norma ISO 27002. Se observó lo siguiente:

- El Plan de Seguridad de Información (PSI) no ha sido desarrollado. Si bien cuentan con procedimientos y controles que cubren algunos aspectos de la seguridad de la información y las tecnologías, se carece en general de una metodología, guía o marco de trabajo que ayude a la identificación de riesgos y determinación de controles para mitigar los mismos.
- Dentro de los distintos aspectos a considerar en la seguridad de la Información, se ha podido observar el incumplimiento de Políticas de seguridad de la Información y de una Clasificación de Seguridad de los activos de Información de la empresa.
- No han implementado controles con respecto a la seguridad física y de personal. Tampoco están claramente identificados los roles y funciones del personal con respecto a la seguridad informática.
- Se ha observado la existencia de controles, en el caso de la Seguridad Lógica, sobre los accesos a los sistemas de información así como procedimientos establecidos para el otorgamiento de dichos accesos.
- Sin embargo, estos controles no obedecen a una definición previa de una Política de Seguridad ni de una evaluación de riesgos de seguridad de la información a nivel de toda la empresa.
- Los controles establecidos a la fecha son producto de evaluaciones particulares efectuadas por las áreas involucradas o bajo cuyo ámbito de responsabilidad recae cierto aspecto de la seguridad.
- Además en muchos casos las directivas ya establecidas con respecto a la seguridad informática se cumplen en forma parcial, o no se cumplen. En el Anexo 1 se muestran los activos de la organización, las amenazas que los afectan directamente y las consecuencias que puede acarrear la materialización de estas amenazas. Se

describen también las salvaguardas o información referida a las medidas de seguridad existentes en la empresa AGROKASA - Supe.

TABLA 5 ANÁLISIS DE RESULTADOS

% DE CUMPLIMIENTO PARA EL DOMINIO DE SEGURIDAD FÍSICA Y AMBIENTAL ISO 27002:2005		
COD.	**DESCRIPCIÓN**	**%**
9.1	**Áreas Seguras**	**2**
9.1.1	Perímetro de Seguridad Física	0
9.1.2	Controles físicos de entrada	0
9.1.3	Aseguramiento de oficinas, salas de servidores e instalaciones	0
9.1.4	Protección contra amenazas externas y ambientales	12
9.1.5	Trabajo en áreas restringidas	0
9.1.6	Acceso público, envíos y áreas de carga	0
9.2	**Seguridad de los equipos**	**13.4**
9.2.1	Ubicación y protección de equipos tecnológicos	8
9.2.2	Seguridad en el suministro de electricidad y servicios	13
9.2.3	Seguridad en el cableado	5
9.2.4	Mantenimiento de equipos	26
9.2.5	Seguridad de equipos fuera de las áreas seguras	0
9.2.6	Destrucción y reutilización de equipos	0
9.2.7	Autorización de sacar equipos	-
	NIVEL TOTAL DE CUMPLIMIENTO DEL DOMINIO	**10.3**

Fuente: Elaboración Propia

De acuerdo con los resultados obtenidos se observa que el área de informática de la empresa AGROKASA - Supe ha implementado en mayor medida los lineamientos de la norma orientados a la Seguridad de los Equipos con un de cumplimiento de 13.4%, aunque no se puede afirmar que el resultado sea favorable, por el contrario aún es insuficiente. Con respecto a Áreas de seguridad el total cubierto es solo el 2%.

En consecuencia el nivel de cumplimiento de los requerimientos de la norma, con respecto al Dominio de Seguridad Física y Ambiental es de 10.33%. Este resultado no es nada alentador, es por eso que se recomienda definir una estrategia para cerrar el gap, en función de un análisis más extenso que profundice los hallazgos obtenidos en este estudio.

El diagnóstico de la seguridad física existente en la empresa AGROKASA- Supe constituye un análisis inicial de los riesgos asociados a las Tecnologías de la Información. Es importante que una vez emitidas las Políticas de Seguridad y consolidada la estructura organizacional responsable de la seguridad de la información, se afinen los puntos considerados de acuerdo con los objetivos de seguridad de la empresa AGROKASA.

Como mencionamos anteriormente y sumado al análisis de brecha presentado, se realizarán una serie de recomendaciones tanto metodológicas como de producto de forma de poder atacar las diferentes fallas de seguridad que surjan del estudio de situación. En el Anexo se proponen políticas para la seguridad de la Información.

CUESTIONARIO DE VERIFICACIÓN DE REQUERIMIENTOS DE LA NORMA ISO 27002

Se evalúa de la situación encontrada en la empresa AGROKASA - Supe, de acuerdo a la información obtenida durante las entrevistas y de los documentos relevantes entregados por el personal del área de informática. Este cuestionario sirve de base para el análisis de brecha, también ayudará a determinar la situación actual de riesgos de información y de tecnologías de información de la empresa AGROKASA-Supe.

En los siguientes cuadros se muestra el cuestionario de diagnóstico basado en la norma ISO 27002.

A partir de la evidencia encontrada y la información obtenida en primera instancia se estableció el criterio de asignación del porcentaje de cumplimiento que indica el nivel de implementación y/o cumplimiento de los controles de la ISO 27002 Se detalla en la siguiente tabla:

TABLA 6 DESCRIPCIÓN CON PORCENTAJES DE LOS GRÁFICOS.

Estado %	Representación de la brecha	Situación actual	Descripción
76 a 100		Razonablemente cubierto	Los requerimientos ISO 27002 están razonablemente cubiertos.
51 a 75		Sustancialmente cubierto	Falta realizar algunas actividades para cubrir razonablemente los requerimientos ISO 27002.
26 a 50		Parcialmente cubierto	Se han realizado actividades que cubren parcialmente los requerimientos ISO 27002.
1 a 25		Limitadamente cubierto	Se han realizado algunas actividades para cubrir los requerimientos ISO 27002.
0		No cubierto	No se ha realizado ninguna actividad relacionada con los requerimientos ISO 27002.

Fuente: Elaboración Propia

TABLA 7 EVALUACIÓN DE LA NORMA

EVALUACIÓN NORMA ISO 27002			
Dominio: Seguridad Física y Ambiental			
Objetivo de Control: Áreas Seguras			
Título: Cuestionario de Control Interno – Aéreas seguras			**Año:** 2016
SEGURIDAD FÍSICA Y DEL ENTORNO			
Áreas Seguras	**SI/ NO**	**Observaciones**	**% de cumplimiento**
¿Existen mecanismos de control de acceso implementados con respecto al acceso a los sitios de procesamiento de información? Algunos ejemplos son controles biométricos, tarjetas de acceso, control de visitantes, etc.	NO	No cubierto	0
¿Existen controles de acceso de tal modo a que solo las personas autorizadas puedan ingresar a las distintas áreas de la organización?	NO	No cubierto	0
¿Las salas de servidores u otros equipos de procesamiento (routers, switches, etc.), están apropiadamente resguardados bajo llave o en cabinas con llave?	NO	No cubierto	0
¿Se tienen implementadas protecciones o resguardos contra fuego, inundaciones, temblores, explosiones, manifestaciones y otras formas de desastres naturales o provocadas por el hombre?	SI	Cuentan con medidas de protección contra incendios, extintores.	12
¿Se tienen procedimientos designados e implementados sobre cómo trabajar en las áreas seguras?	NO	No cubierto	0
¿Con respecto a las zonas de acceso público, entrega, descarga donde personas no autorizadas pueden acceder, las zonas de procesamiento de información y equipos delicados son aislados y asegurados para prevenir el acceso no autorizado?	NO	No cubierto	0
		Total, cubierto	2%

Dominio: Seguridad Física y Ambiental			
Objetivo de Control: Equipo de seguridad			
Título: Cuestionario de Control Interno – Equipo de seguridad			**Año:** 2016
SEGURIDAD FÍSICA Y DEL ENTORNO			
Equipo de seguridad	**SI/ NO**	**Observaciones**	**% de cumplimiento**
¿Los equipos son protegidos para reducir los riesgos de daños ambientales y oportunidades de acceso no autorizado?	SI	Control de la temperatura, aire acondicionado	8
¿Los equipos son protegidos contra fallas eléctricas y otras fallas que pudieran tener (redundancia)?	SI	Limitadamente cubierto	2
¿Mecanismos de protección eléctrica son utilizados como Alimentación múltiple, UPS, generador de backup, etc.?	SI	Dispositivos de suministro de energía ininterrumpido (UPS)	24
¿Los cables de suministro eléctrico y comunicaciones son debidamente protegidos contra intercepción y/o daños?	SI	Protección limitada del cableado de la energía y datos	10
¿Existen controles adicionales de seguridad con respecto al transporte de información crítica? Por ej. Encriptado en las comunicaciones.	NO	No cubierto	0
¿Se realiza mantenimiento periódico de los equipos de modo a asegurar la continua disponibilidad e integridad?	SI	Plan de mantenimiento preventivo y correctivo;	30
¿En la realización de mantenimientos, son respetados los intervalos y recomendaciones de los fabricantes?	SI	Limitadamente cubierto	10
¿Los mantenimientos son realizados únicamente por personal capacitado y autorizado?	SI	sólo el personal de mantenimiento	90
¿Los logos de alertas de los equipos, son revisados periódicamente para detectar y corregir posibles fallas en los mismos? (principalmente fallas en discos)	NO	No cubierto	0

¿Se aplican los controles adecuados cuando se envían los equipos fuera de la organización?	NA	No aplicable	-
¿Todos los equipos están cubiertos por pólizas de seguro y los requerimientos de la Compañía de Seguros están apropiadamente realizados?	NO	No cubierto	0
¿Existen mecanismos de control y mitigación de riesgos implementados con relación a equipos utilizados fuera de la organización? (inscripción de discos de las notebooks, seguro, etc.)	NA	No aplicable	-
¿En caso de utilización de equipos fuera de la organización, estos cuentan con la autorización respectiva de las gerencias?	NA	No aplicable	-
¿Cuándo se disponga la reutilización de equipos o cuando sean dados de baja, son verificados los medios de almacenamiento con respecto a datos y software licenciado y luego destruidos totalmente antes de su entrega?	NO	No cubierto	0
¿Existen controles implementados con respecto a que ningún equipo, información y software sea sacado de la organización sin la autorización respectiva?	NO	No cubierto	0
Fuente: Elaboración Propia		Total cubierto	13.4%

- De acuerdo con los resultados según orientación y cumplimiento:
  - Seguridad de los Equipos: 13.4%,
  - Áreas de seguridad: 2%.

ANÁLISIS Y DISCUSIÓN

El propósito de la investigación fue recopilar información respecto a las medidas de seguridad física implementadas en la empresa AGROKASA para garantizar la seguridad informática considerando los objetivos de control establecidos en la norma ISO27002 y su grado de cumplimiento. El gobierno de TI es responsabilidad de los ejecutivos y del consejo de directores el cual consta de estructuras y procesos organizacionales.

Luego de aplicar los instrumentos de recolección de datos (encuestas, entrevistas y observación), podemos decir que el control que lleva la Oficina de Sistemas e Informática con respecto a la seguridad y administración de los procesos no es tan favorable.

La dirección debe optimizar el uso de los recursos de TI disponibles, los cuales incluyen aplicaciones, información, infraestructura y personas, todo esto con el fin de poder garantizar la calidad y seguridad de su información, así como de todos sus activos.

En síntesis, para proporcionar la información que la organización necesita para el logro de sus objetivos, los recursos de TI deberán ser administrados por un conjunto de procesos que interactúen y se integren de forma natural.

Los resultados obtenidos evidencian que la mayor debilidad de la Oficina de Sistemas e Informática se encuentra en la el trabajo de gestión y difusión de la información sobre las políticas preventivas y mejores prácticas que se deben de realizar para garantizar la seguridad de la información, según Cadme y Duque (2012) en su investigación presenta recomendaciones por cada aspecto de seguridad auditada y cuáles son sus objetivos, beneficios y responsabilidades, ya que encuentra observaciones en todos los enfoques que toma dentro de la empresa, apoyándose en la norma ISO 27001 para mejorar la seguridad de la información en la empresa, mientras que Barrantes y Hugo (2012) en su investigación de diseño e implementación de un sistema de gestión de seguridad, con la metodología magerit y analizado con análisis de brechas con sus indicadores, que dio como resultado que solo un 34% de cumplimiento, tiendo un gran

espacio que no estaba cumpliendo, para minimizar la brecha se propuso un plan para el mantenimiento del sistema de seguridad y planteando mejor la política de seguridad.

Puedo decir entonces que este último proyecto fue de apoyo para mi investigación, en cuanto al uso dela análisis de brechas con sus controles, para encontrar las falencias de la empresa

Asimismo, en lo que respecta a atención oportuna y solución de problemas relacionados a TI, el personal se muestra conforme en su mayoría con el servicio brindado por la Oficina de Sistemas e Informática, es algo preocupante el poco conocimiento por parte del personal administrativo sobre seguridad informática y políticas preventivas, pero se cree que se puede mejorar realizando distintas actividades informativas como lo argumenta el trabajo de investigación, también mencionar que Cáceres y García (2014) donde se indica cuáles son los aspectos que se deben mejorar de forma inmediata a fin de lograr una optimización y buena gestión de la información a nivel organizacional.

Todo esto nos lleva a concluir que los instrumentos de recolección de datos utilizados nos ayudaron a identificar hallazgos, los cuales nos permitieron ver la situación actual de la organización, en especial de la Oficina de Sistemas e Informática y el servicio que brinda.

CONCLUSIONES

El desarrollo de la presente investigación ha llevado a las siguientes conclusiones:

- Al revisar la situación actual se determinó que la mayor falla es la falta de seguridad de información de la empresa AGROKASA.

El personal de la empresa AGROKASA no tiene conocimiento de las amenazas que pueden afectar al proceso de negocio, amenazas que van desde fallos técnicos y accidentes no intencionados, pero no menos peligrosos hasta acciones intencionadas, más o menos lucrativas, de curiosidad, espionaje, sabotaje, vandalismo, chantaje o fraude.

- Se verifico que sus políticas de seguridad están empíricamente desarrolladas y no fundamentadas bajo ninguna norma, y no cumplen con su ejecución.

Se debe tomar en cuenta que el análisis de brechas nos permite comparar los procesos de seguridad existentes con los lineamientos de la norma y establecer en qué áreas o procesos se debe priorizar y enfocar esfuerzos para incrementar la seguridad.

El objeto o propósito de implementar controles para la seguridad consiste sobre todo en mantener la continuidad de los procesos organizacionales.

La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo, y también debieran estar sujetas a las regulaciones y legislación nacionales e internacionales relevantes.

- Se observó después de la evaluación con la auditoria que es muy bajo el cumplimiento con respecto a los requerimientos de seguridad física en la empresa.

Se concluye que cada uno de los elementos del Área de Informática es de suma importancia para la empresa AGROKASA, por lo que se sugiere la aplicación de controles establecidos en la norma ISO 27002.

RECOMENDACIONES

- Elabora el Manual de funciones y responsabilidades, asignándole a cada área sus responsabilidades.

El encargado del área informática sea la persona que oriente en la adquisición de software, seguridad de la información, una adecuada ambientación de los equipos y coordine con las demás áreas en lo referente al uso de las TICS en la empresa.

- La empresa debe de estar preparado para cualquier riesgo que ocurra dentro de ella y debe de realizar un plan estratégico y de esta forma mejorar sus procesos y actividades diarias, ya que después de haber aplicado la norma ISO 27002.

El personal que trabaja en la empresa debe tomar conciencia de lo importante que es adoptar controles para la seguridad informática.

Se recomienda realizar una Evaluación de los riesgos con el fin de identificar y valorar los riesgos a los cuales los sistemas de información y sus activos están expuestos, para identificar y seleccionar los controles adecuados que minimicen los riesgos identificados.

- Es recomendable que la organización adopte el plan de mejoras como una buena práctica aplicadas a las TI, para la planificación, seguridad, control, prevención y corrección para mejorar su situación actual.

Una vez que se han tomado las decisiones para el tratamiento de los riesgos, se deberían seleccionar los controles adecuados y se deberían implementar para asegurar que los riesgos se reduzcan a un nivel aceptable.

Se debe considerar el desarrollo y cumplimiento de políticas de seguridad informática como una pauta para que la Institución este acorde con las regulaciones legales y técnicas del entorno.

Es importante que los principios de la Política de Seguridad y la implementación de un Plan de Seguridad Informática sean parte de la cultura Organizacional.

AGRADECIMIENTOS

Le agradezco a Dios por haberme acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

A mi amada esposa y amiga Caterin, quien fue el ingrediente perfecto para poder lograr alcanzar esta dichosa y muy merecida victoria en la vida, por su paciencia comprensión, por tantas ayudas y tantos aportes, no solo para el desarrollo de mi tesis sino también por su apoyo y ánimo que me brinda día con día para alcanzar nuevas metas, tanto profesionales como personales en mi vida; que es mi inspiración y mi motivación, sin su apoyo este trabajo nunca se habría escrito y por eso, este trabajo es también el suyo.

A mis padres Glicerio y Rosa por haberme brindado la oportunidad de estudiar la carrera en la Universidad San Pedro Huacho, por su esfuerzo, dedicación y entera confianza.

Papá, gracias por iluminar mi camino y darme la pauta para poder realizarme en mis estudios y mi vida. Agradezco los consejos sabios que en el momento exacto has sabido darme para no dejarme caer y enfrentar los momentos difíciles.

Mami, tu eres la persona que siempre me ha levantado los ánimos tanto en los momentos difíciles de mi vida estudiantil como personal. Gracias por tu paciencia y esas palabras sabias que siempre tienes para mis enojos, mis tristezas y mis momentos felices, por ser mi amiga y ayudarme a cumplir mis sueños, te quiero mucho.

A mis hermanos que quienes a lo largo de mi vida me han apoyado en mi bienestar y educación en todo momento.

El agradecimiento al Ing. Eddy Iván Quispe Soto que mediante sus conocimientos a respaldado la realización del presente trabajo, también mis sinceros agradecimientos al Ing. Luis Descailleaux Donayre, quién ha contribuido en el asesoramiento de manera desinteresada en la culminación de la presente tesis.

"Más gracias sean dadas a Dios, que nos da la victoria por medio de nuestro Señor Jesucristo… sabiendo que vuestro trabajo en el Señor no es en vano."
1 Corintios 15:57-58

REFERENCIAS BIBLIOGRÁFICAS

Barrantes Porras, C., & Hugo Herrera, J. (2012). *Diseño e implementación deun sistema de gestión de seguridad de información en procesos tecnológicos.* Lima-Perú: http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/609/3/barrantes_ce.pdf.

Buendía, J. F. (2013). *Seguridad Informática.* Madrid: McGraw-Hill.

Cadme Ruiz, C. M., & Duque Pozo, D. F. (2012). *Auditoría de seguridad informática ISO 27001 para la empresa de alimentos "Italimento Cia. Ltda".* Cuenca - Ecuador: http://dspace.ups.edu.ec/bitstream/123456789/2644/16/UPS-CT002441.pdf.

Díaz, M., & Ugarte, Y. (2013). *Auditoria informática aplicada a la.* Huacho-Perú: Escuela académico profesional de ingeniería informática y de sistemas - Universidad San Pedro. Huacho.

Echenique García, J. A. (2001). *Aiditoría en Informática* (Segunda ed.). México: Mc Graw Hill.

Huaman Monzón, F. (2014). *Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano.* Lima - Perú: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5582/HUAMAN_ FERNANDO_AUDITORIA_NORMA_TECNICA_INSTITUCIONES.pdf?sequence=1.

ISO. (2012). *ISO2007*. Recuperado el 7 de Enero de 2017, de ISO 2007.ES: http://www.iso27000.es/sgsi.html

Nogueira Solis, J. (2013). *Procedimientos para la auditoría física y medio.* Lima-Perú: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4978/NOGUEIRA_JOCE.

NORMA TÉCNICA PERUANA. (2007). *Tecnología de la información NTP-ISO/IEC 17799.* Lima, Lima, Perú. Recuperado el 15 de Noviembre de 2016

Piattini, M. G., & Del Peso, E. (2001). *Auditoría Informática un enfoque práctico* (Segunda ed.). Madrid, España: RA-MA.

redUSERS. (2011). *Hacking.* Buenos Aires: Fox Andina.

Vieites, Á. G. (2014). *Enciclopedia de la Seguridad Informática* (Segunda ed.). México: Ra-Ma.

Xiloj Charuc, F. (2008). *Auditoría externa en un ambiente de sistemas de información computarizado en el área de ingresos de una empresa comercializadora de vehículos.* Guatemala -Guatemala: http://biblioteca.usac.edu.gt/tesis/03/03_3202.pdf.

ANEXOS Y APÉNDICES

ANEXO 1

DESCRIPCIÓN DE CONSECUENCIAS Y SALVAGUARDAS

A continuación, se muestran los principales activos de la organización, las amenazas que los afectan directamente y las consecuencias que puede acarrear la materialización de estas amenazas. Se describen también las salvaguardas o información referida a las medidas que ha tomado la empresa AGROKASA-Supe para mitigar estas consecuencias. Por último, se han evaluado estas medidas, indicando si son Deficientes, Mejorables o Eficientes.

D = Deficientes

M = Mejorables

E = Eficientes.

ACTIVO VITAL	AMENAZA	CONSECUENCIAS	¿SE PROTEGE?	MEDIDAS DE PROTECCIÓN	¿ES EFECTIVA?
Infraestructura: Centro de Cómputo	025 Incendios	Daños en el área	SI	Uso de extintores	E
	013 Entrada sin autorizaciones	Pérdida de equipos / Pérdida de información	NO		D
	010 Deshonestidad y sabotaje	Paralización de los sistemas(Falta de sistemas) / Robo, modificación de información	NO		D
	023 Falta de registros de auditoria.	Imposibilidad del seguimiento de uso de la información y generación de reportes	NO		D
	009 Desastres Naturales (rayos, lluvias, inundaciones)	Destrucción de equipos /Pérdida de información	NO		M
	028 Interrupción del servicio de energía	Paralización de los sistemas/Paralización de actividades	SI	Energía estabilizada conectada a un UPS.	E

	034 Mala evaluación de datos de auditoria.	No se advierten las faltas relacionadas a seguridad.	NO		D
Dispositivos de conectividad y soporte en comunicaciones (Cableado, antenas, switch, hubs, módems.)	009 Desastres Naturales (rayos, lluvias, inundaciones)	Destrucción de los equipos	NO		M
	046 Servicio de mantenimiento inadecuado	Fallas generales en el sistema y/o en la red /Deterioro en el funcionamiento del sistema / Aumento de Vulnerabilidades e inestabilidad del sistema	NO		M
	003 Administración inadecuada	Lentitud en el procesamiento de la información / Pérdida de tiempo en horas hombre / Inconsistencia de datos, mala configuración, fraude	SI	Administración por personal capacitado	M
	015 Errores de configuración y operación	Fallas generales en el sistema y/o en la red	SI	Configuración por personal capacitado	M

ACTIVO VITAL	AMENAZA	CONSECUENCIAS	¿SE PROTEGE?	MEDIDAS DE PROTECCIÓN	¿ES EFECTIVA?
Servidores centrales	009 Desastres Naturales (rayos, lluvias, inundaciones)	Destrucción de los equipos	NO		M
	025 Incendios	Destrucción de los equipos	SI	Uso de extintores	E
	001 Accesos no autorizados	Entorpecimiento del Funcionamiento de los Procesos.	SI	Administración por personal capacitado	E
	019 Fallas físicas de los equipos (averías)	Pérdida de tiempo por necesidades de reemplazo / Deterioro en el funcionamiento del sistema	NO		M

	026 Infección de virus	Pérdida de información. Falla en el sistema	SI	Antivirus instalado en cada estación / Escaneo semanal de virus	D
	043 Robo de equipos	Paralización de los sistemas/ Pérdida de información	NO		M
	035 Mantenimiento inadecuado	Fallas generales en el sistema y/o en la red /Deterioro en el funcionamiento del sistema / Aumento de Vulnerabilidades e inestabilidad del sistema	SI	Administración por personal capacitado	E
	028 Interrupción del servicio de energía	Daños en equipos / Pérdida de información	SI	Energía estabilizada conectada a un UPS.	E
PC de escritorio	009 Desastres Naturales (rayos, lluvias, inundaciones)	Destrucción de los equipos	NO		M
	025 Incendios	Destrucción de los equipos	SI	Uso de extintores	E
	001 Accesos no autorizados	Entorpecimiento del Funcionamiento de los Procesos.	SI	Administración por personal capacitado	M
	019 Fallas físicas de los equipos (averías)	Pérdida de tiempo por necesidades de reemplazo / Deterioro en el funcionamiento del sistema	NO		M
	026 Infección de virus	Pérdida de información. Falla en el sistema	SI	Antivirus instalado en cada estación / Escaneo semanal de virus	D
	043 Robo de equipos	Paralización de los sistemas/ Pérdida de información	NO		M

	048 Soporte técnico de equipos inadecuado	Fallas generales en el sistema y/o en la red /Deterioro en el funcionamiento del sistema / Aumento de Vulnerabilidades e inestabilidad del sistema	SI	Administración por personal capacitado	M
	035 Mantenimiento inadecuado	Fallas generales en el sistema /Aumento de Vulnerabilidades e inestabilidad del sistema	SI	Administración por personal capacitado	M
	051 Uso descontrolado de recursos	Entorpecimiento del Funcionamiento de los Procesos / Pérdida de tiempo en horas hombre	NO		M
	053 Vandalismo	Destrucción de los equipos	NO		M
	028 Interrupción del servicio de energía	Daños en equipos / Pérdida de información	SI	Energía estabilizada conectada a un UPS.	E
Sistema de alimentación Ininterrumpida (UPS)	009 Desastres Naturales (rayos, lluvias, inundaciones)	Destrucción de los equipos	NO		M
	035 Mantenimiento inadecuado	Fallas generales en el sistema /Aumento de Vulnerabilidades e inestabilidad del sistema	SI	Administración por personal capacitado	E
	019 Fallas físicas de los equipos (averías)	Pérdida de tiempo por necesidades de reemplazo / Deterioro en el funcionamiento del sistema	NO		E

ACTIVO VITAL	AMENAZA	CONSECUENCIAS	¿SE PROTEGE?	MEDIDAS DE PROTECCIÓN	¿ES EFECTIVA?
Sistema operativo	003 Administración inadecuada	Lentitud en el procesamiento de la información / Pérdida de tiempo en horas hombre/ inconsistencia de datos, mala configuración, fraude	SI	Administración por personal capacitado	M
	005 Aplicaciones sin licencia	Aumento de vulnerabilidades e inestabilidad del sistema	NO		D
	026 Infección de virus	Pérdida de Información. Falla en el sistema	SI	Antivirus instalado en cada sistema	D
	042 Robo de claves	Robo, modificación de información	NO		M
Sistemas para la Gestión Interna	003 Administración inadecuada	Lentitud en el procesamiento de la información / Pérdida de tiempo en horas hombre/ Inconsistencia de datos, mala configuración, fraude	SI	Administración por personal capacitado	E
	039 Procesamiento de información inadecuado	Lentitud en el procesamiento de la información / Pérdida de tiempo en horas hombre / consistencia de datos, mala configuración, fraude	SI	Administración por personal capacitado	E
	054 Vulnerabilidad de la Plataforma tecnológica de tablas libres	Robo, modificación o eliminación de información	NO		M
	028 Interrupción del servicio de energía	Pérdida de información	SI	Energía estabilizada conectada a un UPS.	E
	026 Infección de virus	Pérdida de Información. Falla en el sistema	SI	Antivirus instalado en cada sistema	D

Aplicaciones herramientas (ofimática , antivirus, navegador web, cliente de correo electrónico, Messenger)	003 Administración inadecuada	Lentitud en el procesamiento de la información / Pérdida de tiempo en horas hombre / Inconsistencia de datos, mala configuración, fraude	SI	Administración por personal capacitado	D
	028 Interrupción del servicio de energía	Pérdida de información	SI	Energía estabilizada conectada a un UPS.	E
	057 Errores de Mantenimiento/ Actualización de programas	Aumento de vulnerabilidades e inestabilidad del sistema	SI	Actualizaciones programadas	M

ACTIVO VITAL	AMENAZA	CONSECUENCIAS	¿SE PROTEGE?	MEDIDAS DE PROTECCIÓN	¿ES EFECTIVA?
Datos de gestión interna (financieros, contables, Archivos de normas, contratos, etc.)	011 Destrucción negligente de los datos	Robo, eliminación de información	NO		M
	036 Modificación no autorizada	Degradación /Pérdida de información	SI	Administración por personal capacitado	E
	014 Entrenamiento inadecuado de usuarios	Robo, modificación o eliminación de información	NO		M
	026 Infección de virus	Pérdida de información.	SI	Antivirus instalado en cada sistema	D
	021 Falta de cuidado en el manejo de información	Degradación /Pérdida de información	NO		M
Datos Vitales / confidenciales (Historias clínicas, datos de pacientes)	002 Accesos no autorizados a datos con modificación	Degradación /Pérdida de información	SI	Administración por personal capacitado	E
	011 Destrucción negligente de los datos	Pérdida de información.	SI	Administración por personal capacitado	M

	014 Entrenamiento inadecuado de usuarios	Robo, modificación o eliminación de información	NO		M
	017 Falla de backup	Degradación /Pérdida de información	SI	Administración por personal capacitado	E
	021 Falta de cuidado en el manejo de información	Degradación /Pérdida de información	NO		M
	026 Infección de virus	Pérdida de información.	SI	Antivirus instalado en cada sistema	D
	036 Modificación no autorizada	Degradación /Pérdida de información	SI	Administración por personal capacitado	D
	045 Saturación de información por espacio	Degradación /Pérdida de información	NO		M
	058 Introducción de información incorrecta	Lentitud en el procesamiento de la información	SI	Administración por personal capacitado	M
Documentación de programas, hardware, sistemas, procedimientos administrativos, manuales, etc.	011 Destrucción negligente de los datos	Pérdida de información.	NO		M
	026 Infección de virus	Pérdida de información.	SI	Antivirus instalado en cada sistema	D

ACTIVO VITAL	AMENAZA	CONSECUENCIAS	¿SE PROTEGE?	MEDIDAS DE PROTECCIÓN	¿ES EFECTIVA?
Personal del área(Operadores, Técnicos, etc.)	040 Retiro/ausencia intempestiva de personal	Aumento de vulnerabilidades e inestabilidad del Sistema / Incremento de riesgos en caída de servicios	NO		M
	010 Deshonestidad y sabotaje	Paralización de los sistemas(Falta de sistemas) / Robo, modificación de información	NO		M

	032 Mal uso de derechos de administración	Fallas generales en el sistema y/o en la red / Pérdida de tiempo en horas hombre/ inconsistencia de datos, mala configuración, fraude	NO		M
	048 Soporte técnico de equipos inadecuado	Fallas generales en el sistema y/o en la red /Deterioro en el funcionamiento del sistema / Aumento de Vulnerabilidades e inestabilidad del sistema	SI	Administración por personal capacitado, Ejecución del Plan Anual del Mantenimiento	M
	012 Documentación deficiente	Aumento de vulnerabilidades e inestabilidad del sistema / Incremento de riesgos en caída de servicios	NO		D
	014 Entrenamiento inadecuado de usuarios	Aumento de vulnerabilidades e inestabilidad del sistema	NO		D
	035 Mantenimiento inadecuado	Fallas generales en el sistema /Aumento de Vulnerabilidades e inestabilidad del sistema	SI	Administración por personal capacitado	M
Usuarios Internos	014 Entrenamiento inadecuado de usuarios	Aumento de vulnerabilidades e inestabilidad del sistema	NO		D
	059 Divulgación de Información	Imagen institucional	SI	Administración por personal capacitado	E
	011 Destrucción negligente de los datos	Pérdida de información.	NO		M

POLÍTICAS DE SEGURIDAD

Se plantean políticas de seguridad con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la empresa AGROKASA-Supe.

Las políticas de seguridad se escogieron para brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- **Generalidades**

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Organización. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la organización y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

- **Objetivo**

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política. Mantener la Política de Seguridad de la empresa actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos computacionales de la empresa y el uso adecuado de los mismos.

- **Alcance**

Esta Política se debe aplicarse en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

- **Organización de la Seguridad**

Generalidades

Es necesario tener bien definido un marco de gestión para efectuar diferentes tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades, para tener una eficiente administración de la seguridad de información.

Objetivo

Administrar la seguridad de la información dentro de la empresa y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

En este control es necesario definir un Comité de Seguridad que entre sus funciones deberá:

- Revisar y proponer a la máxima autoridad de la empresa para su aprobación, la Política y las funciones generales en materia de seguridad de la información.

- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

- Garantizar que la seguridad sea parte del proceso de planificación de la información.

- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

- Promover la difusión y apoyo a la seguridad de la información dentro la empresa.

- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la empresa frente a interrupciones imprevistas.

Una vez integrado el Comité, es necesario se definan las funciones de los miembros del mismo para poder para que este pueda desempeñar sus actividades y mejorar la seguridad en la empresa. En la implementación están especificados los miembros del Comité. El Comité de Seguridad de la Información debe proponer a la Gerencia para su aprobación la definición y asignación de las responsabilidades que surjan de sus funciones.

Es necesario definir el proceso para la autorización de nuevos recursos para el procesamiento de información, así como los requerimientos de Seguridad en contratos con Terceros, los principales puntos que se deben considerar lo siguiente:

a) Cumplimiento de la Política de seguridad de la información de la Organización.

b) Protección de los activos de la Organización, incluyendo:

- Procedimientos para proteger los bienes de la Organización, abarcando los activos físicos, la información y el software.

- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.

- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.

- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes del acuerdo y responsabilidades legales.

g) Definiciones relacionadas con la protección de datos.

h) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

i) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

j) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

k) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

l) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

- **Gestión de los Activos**

Generalidades

La organización debe tener conocimiento sobre los activos que posee como parte importante de la administración de riesgos.

Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Responsabilidad sobre los activos

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada.

El responsable de informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la Política.

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 4 meses. El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

- **Seguridad del Personal**

Generalidades

La seguridad de la información se basa en la capacidad para conservar la integridad, confidencialidad y disponibilidad de los activos.

Para lograr lo anterior es fundamental educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de

sus funciones y de las expectativas depositadas en ellos en materia de seguridad. Así mismo, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

Objetivo

Reducir los riesgos de error humano, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Indicar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Organización en el transcurso de sus tareas normales

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Seguridad en la definición del trabajo y los recursos

- Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

- Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

Términos y condiciones de la relación laboral

- Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

- Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la empresa y del horario normal de trabajo.

- Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de contrato.

Conocimiento, educación y entrenamiento en seguridad de la información

- Todos los empleados de la empresa y, cuando sea necesario, los usuarios externos y los terceros que desempeñen funciones en la empresa, deberán recibir una adecuada capacitación y actualización periódica en materia de la política de seguridad, normas y procedimientos para la seguridad.

- Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

- El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la Política.

- Cada 6 meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

- Además se otorgará una guía de usuario para que tengan un mejor conocimiento con respecto a las amenazas informáticas y sus posibles consecuencias dentro de la Corporación de tal manera que se llegue a concienciar y crear una cultura de seguridad de la información.

- **Seguridad Física y del Entorno**

Generalidades

La seguridad física y ambiental minimiza los riesgos de daños e interferencias a la información y a las operaciones de la Corporación. Además, trata de evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad. El control de los factores ambientales permite garantizar el correcto

funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

Previo a la implementación de un control de seguridad física y del entorno, es necesario que se realice un levantamiento de información de la situación actual de la Corporación en cuanto a su seguridad física para determinar las vulnerabilidades y posibles soluciones.

Áreas Seguras

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

- Definir y documentar claramente el perímetro de seguridad.

- Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción).

- Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

- Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán medios alternativos de control de acceso físico al área o edificio. El acceso a dichas áreas y edificios estará restringido exclusivamente al

personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

- Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.

- Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

El Responsable de Seguridad Informática llevará un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Edificio y Área.

b) Principales elementos a proteger.

c) Medidas de protección física.

Seguridad de Equipos

- Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

- Registrar el retiro de equipamiento de la sede del Organismo para su mantenimiento.

TÉRMINOS Y DEFINICIONES

Para propósitos de este documento, se aplican los siguientes términos y definiciones.

Activo

Cualquier cosa que tenga valor para la organización.

Control

Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

NOTA. El control también se utiliza como sinónimo de salvaguarda o contramedida.

Lineamiento

Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas.

Medios de procesamiento de la información

Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

Seguridad de la información

Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudiación y confiabilidad

Evento de seguridad de la información

Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de la información

Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

Política

Intención y dirección general expresada formalmente por la gerencia

Riesgo

Combinación de la probabilidad de un evento y su ocurrencia (ISO/IEC Guía 73:2002)

Análisis del riesgo

Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Proceso general del análisis del riesgo y la evaluación del riesgo.

Evaluación del riesgo

Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.

Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

NOTA. La gestión del riesgo normalmente incluye la evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

Tratamiento del riesgo

Proceso de selección e implementación de medidas para modificar el riesgo.

Tercera persona

Esa persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

Amenaza

Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.

Vulnerabilidad

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

MATRIZ DE CONSISTENCIA

TEMA: AUDITORÍA DE SEGURIDAD FÍSICA DE LA EMPRESA AGROKASA SUPE

PROBLEMA	HIPOTESIS	OBJETIVOS	VARIABLES
¿Cómo desarrollar una auditoria de seguridad física aplicando la norma ISO 27002 a la empresa AGROKASA Supe - 2016?	En vista de que la investigación tiene un alcance de carácter descriptivo, no es posible plantear una hipótesis debido a que no se intenta correlacionar o explicar causalidad de variables, debido a ello es que la hipótesis es Implícita. .	**General:** -Desarrollar una Auditoria de Seguridad Física de la Empresa AGROKASA-Supe, mediante los controles de la norma ISO 27002. **Específicos:** • Revisar la organización su administración y estructura de la seguridad física. • Verificar el cumplimiento de las políticas y otras medidas de seguridad informática establecidas por la norma. • Determinar en qué medida se cumple con la implementación de requerimientos de seguridad física, en el área de informática de la empresa AGROKASA	-Auditoria -Seguridad Física

Operacionalización y Definición de las Variables

VARIABLES	DEFINICIÓN CONCEPTUAL	OPERACIONALIZACIÓN DE VARIABLES		DISEÑO METODOLÓGICO
		INDICADORES	ÍNDICES / ESCALA	
Variable 1: **Auditoría**	**Auditoría:** Inspección o verificación de la contabilidad de una empresa o una entidad, realizada por un auditor con el fin de comprobar si sus cuentas reflejan el patrimonio, la situación financiera y los resultados obtenidos por dicha empresa o entidad en un determinado ejercicio.	**Auditoría:** - Cumplimiento - Evaluación - Eficiencia - Eficacia - Gestión	**Auditoría:** - Malo - Regular - Bueno - Muy Bueno	**1.Tipo y Nivel de Investigación:** Aplicada y Descriptiva **2. Diseño de Investigación:** No Experimental **3. Unidad de Análisis** Agroindustria AGROKASA SAC - SUPE **4. Población:** 12 personas independientemente responsables por área
Variable 2: **Seguridad Física**	**Seguridad Física**: Son todos aquellos mecanismos generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema.	**Seguridad Física**: - Acceso físico - Desastres naturales - Alteraciones del entorno	**Seguridad Física**: - Malo - Regular - Bueno - Muy Bueno	