UNIVERSIDAD SANTO TOMAS SECCIONAL TUNJA

FACULTAD DE CONTADURÍA PÚBLICA

ESPECIALIZACIÓN EN AUDITORIA Y ASEGURAMIENTO DE LA INFORMACIÓN

ESTUDIO DE IMPLEMENTACIÓN DE LA ISO 27001 EN ALGUNAS EMPRESAS TUNJANAS

Elaborado por: Ana Milena Prieto López

Presentado a:

Comité Curricular.

Asesor:

Andrea Cruz Yomayusa

Tunja -Boyacá

2021

Título: Estudio de Implementación de la ISO 27001 en Algunas Empresas Tunjanas

Autor: Ana M. Prieto López, Universidad Santo Tomas Seccional de Tunja
Título Académico: Tecnóloga en Contabilidad y Finanzas (SENA), Contadora Pública., Especialista en Auditoria y Aseguramiento de la información (En curso).
Correo: ana.prietol@usantoto.edu.co
Institución: Universidad Santo Tomas – Seccional Tunja

Resumen

El estudio de la norma en una organización se realiza con el fin de mejorar las prácticas y optimizar los procesos de seguridad de la empresa, puesto que es el centro que conecta los diferentes sistemas para dar respuesta a los principios de la seguridad de la información como son la integridad, la confidencialidad y la disponibilidad.

Este articulo pretende identificar la problemática que se presenta por la falta de conocimiento de la ISO 27001 del Sistema de Gestión de la Seguridad de la información realizando un estudio a algunas personas que trabajan en diferentes empresas de la ciudad de Tunja, teniendo en cuenta los riesgos y vulnerabilidades a los que se encuentran expuestas.

Palabras Clave: Seguridad de la información, empresas Tunjanas, Riesgos, vulnerabilidades, integridad, confidencialidad, disponibilidad, ISO 27001.

Abstract:

The study of the standard in an organization is carried out in order to improve practices and optimize the security processes of the company, since it is the center that connects the different systems to respond to the principles of information security such as they are integrity, confidentiality and availability.

This article aims to identify the problem that arises due to the lack of knowledge of ISO 27001 of the Information Security Management System by carrying out a study of some people who work in different companies in the city of Tunja, taking into account the risks and vulnerabilities to which they are exposed.

Keywords:

Information security, Tunjanas companies, Risks, vulnerabilities, integrity, confidentiality, availability, ISO 27001.

Introducción

La norma ISO 27001 busca mejorar las prácticas de seguridad de la información, con su implementación se busca la certificación y garantizar la adecuada aplicación de los recursos en las áreas de mayor potencial, optimizando sus ingresos y costos de seguridad.

Es necesario que se tomen medidas y se proteja de riesgos a los que pueda estar expuesta la información de una organización basándose en los tres pilares: la confidencialidad, la integridad y la disponibilidad, en el manejo de los datos se constituyen en los pilares de la seguridad de la información (Gómez, 2011); para dar cumplimiento y proteger el activo más importante de una organización es importante que se implemente herramientas tecnológicas, políticas, procesos y evaluación de riesgos.

Se pretende realizar una investigación para medir el nivel de conocimiento que tienen algunas personas que trabajen en empresas tunjanas sobre la norma aplicada para evaluar y prevenir el riesgo en el que se encuentra expuesta la información dentro de las organizaciones, con el fin de mejorar sus procesos, proteger y mantener la confidencialidad de la información previniéndola de futuros daños, además de buscar un enfoque innovador y crecimiento de las empresas.

Objetivo General

Analizar la aplicación y ampliación del conocimiento del Sistema de Gestión de Seguridad de la Información SGSI ISO/IEC 27001 en una muestra de 50 personas que trabajen en algunas empresas de la ciudad de Tunja, mediante una encuesta y un curso sobre la norma.

Objetivos específicos

1. Realizar una encuesta a empleados de diferentes empresas para medir su nivel de conocimiento respecto a la norma ISO/IEC 27001.
2. Crear un curso sobre la norma en la plataforma Google Class Room, con los temas mas relevantes separados por módulos, con el fin de capacitar a los empleados para que adquieran mayor conocimiento sobre la norma.
3. Analizar el desempeño y resultados obtenidos del curso aplicado con la finalidad de medir el conocimiento de la norma en algunas personas que trabajen en empresas pequeñas de Tunja.

Estado del Arte

1. Según el artículo" Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia)" Monsalve-Pulido, J. A., Aponte-Novoa, F. A., & Chaves-Tamayo, D. F. (2014)., El modelo de negocio de las empresas de hoy se está encaminando al uso de las tecnologías de la información y las comunicaciones (TIC), aumentando el uso de medios informáticos por parte de los usuarios y las probabilidades de ser vulnerables por medio de delincuentes informáticos, con esto se entiende que es necesario adaptar nuevos sistemas que mejores los procesos dentro de las empresas pero así mismo se debe evitar y controlar las amenazas contra la seguridad de la información.

2. De acuerdo con el artículo denominado" Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27001" Valencia-Duque, F. J., & Orozco-Álzate, M. (2017); se evidencia que existen diferentes alternativas para la implementación del Sistema de Gestión de la Información dentro de una organización con el fin de mejorar y proteger la información de amenazas externas o internas que puedan afectar el funcionamiento de un negocio.
3. Por último, Estupiñán, A. D. C. A., Pulido, J. A., & Jaime, J. A. B. (2013). Indican en su artículo "Análisis de Riesgos En Seguridad de La Información¨" habla de la aplicación de metodologías de análisis de riesgos es de utilidad a las organizaciones para tener un mayor control sobre sus activos, su valor y las amenazas que pueden impactarlas. Es de vital importancia que en las empresas se establezcan objetivos empresariales y, a partir de ellos, políticas de seguridad que permitan controlar la realización de los procesos para así optimizar el análisis de riesgos, con lo cual se busca mejorar las buenas prácticas y procesos dentro de las organizaciones para obtener mejores resultados.

Metodología

El presente artículo de reflexión se desarrolla mediante las siguientes fases:

Fase 1: Se realizará una encuesta, la cual se aplicará en una muestra de 50 personas que trabajen en empresas de la ciudad de Tunja, con el fin de determinar y medir el nivel de conocimiento que tienen sobre la norma ISO 27001.

Fase 2: Creación del Curso en la plataforma Google Class Room sobre la ISO 27001. Se realizará un estudio para medir el conocimiento de algunos empleados de diferentes empresas Tunjanas sobre

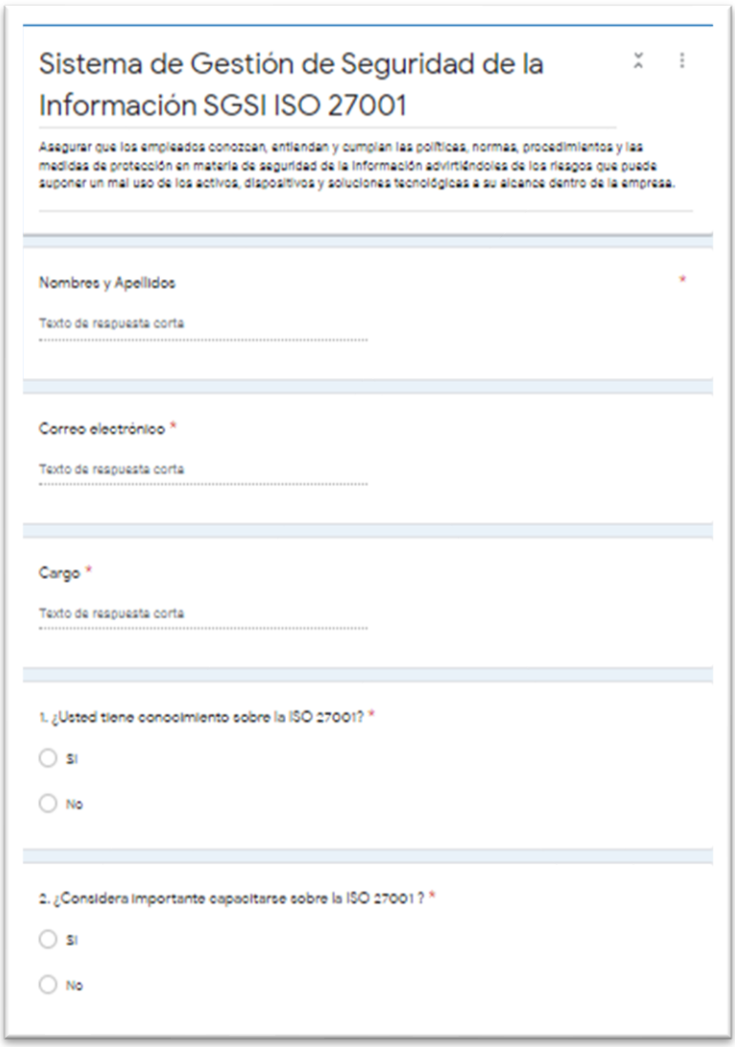
la norma, mediante la aplicación de un curso a el cual se dividirá en 6 unidades y contará con un material de apoyo para su respectivo desarrollo.

Fase 3: Análisis del desempeño y resultados obtenidos del curso aplicado a diferentes empleados de empresas de la ciudad de Tunja. Se analizarán los resultados obtenidos con la aplicación del curso para medir el grado de conocimiento del Sistema de gestión de seguridad de la información de los empleados que trabajen dentro de las empresas Tunjanas.

El diagnostico permitirá medir y estandarizar el nivel de conocimiento del Sistema de Gestión de Seguridad de la Información alineado a la norma de la ISO 27001 con el fin de que se puedan controlar las amenazas y riesgos de seguridad a los que están expuestos las empresas del municipio de Tunja.

Resultados:

Fase 1: Encuesta conocimiento ISO 27001



3. ¿Qué considera que se obtiene implementando la ISO 27001? *

- Se concentra en la satisfacción del cliente y en la capacidad de proveer productos y servicios que cumpla...
- Reducción de riesgos relacionados con la confidencialidad, disponibilidad e integridad de la información e...
- Sirve para establecer políticas y objetivos de innovación así como procesos para lograr dichos objetivos.

4. ¿Esta de acuerdo con que se implemente la ISO 27001 en la empresa en que esta trabajando actualmente, cual razon considera que seria mas relevante ? *

- [ ] Se asegura la informacion de la empresa
- [ ] Garantiza mayores beneficios para la empresa y los empleados
- [ ] Se asegura la integralidad de los datos confidenciales
- [ ] Reduce riesgos y daños en el activo mas importante de la empresa, es decir la información

5. ¿Usted actualmente se encuentra trabajando en alguna empresa? *

- SI
- No

Después de la sección 1 Ir a la siguiente sección

Sección 2 de 3

Trabajo en una empresa

Descripción (opcional)

6. ¿En la empresa donde usted labora tienen implementado el Sistema de Gestión de Seguridad de la Información?

- SI
- No

Después de la sección 2 Ir a la siguiente sección

Sección 3 de 3

La empresa tiene implementado el SGSI

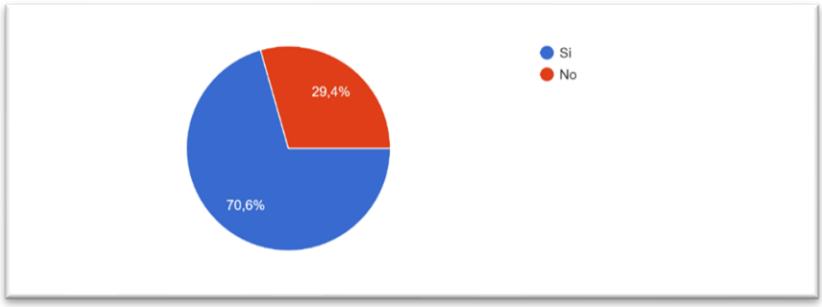
Descripción (opcional)

Por favor indique que políticas se manejan dentro de la empresa en el SGSI.

Texto de respuesta larga

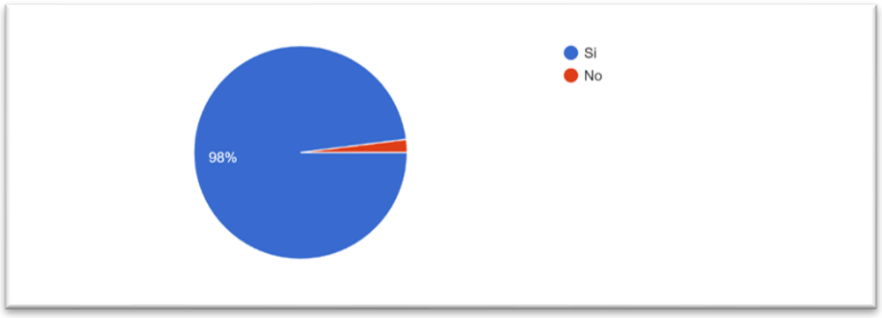
Tabulación encuesta:

1. ¿Usted tiene conocimiento sobre la ISO 27001?



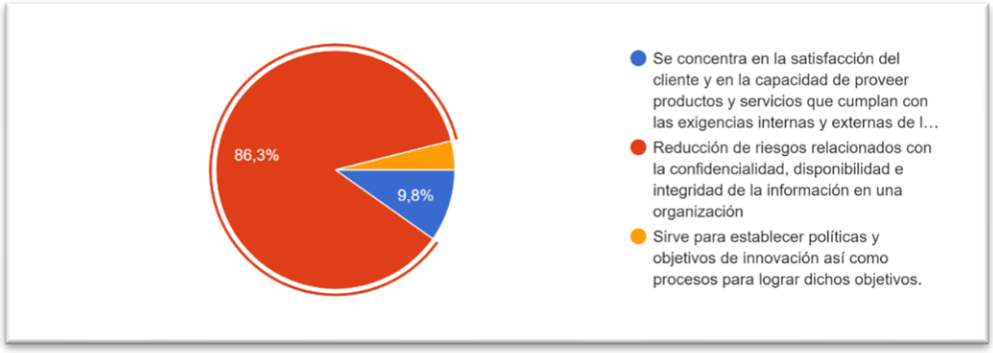
Como se puede observar el 70% de las personas tienen conocimiento sobre la norma o por lo menos saben de qué trata esto es positivo para el estudio que se está realizando.

2. ¿Considera importante capacitarse sobre la ISO 27001?



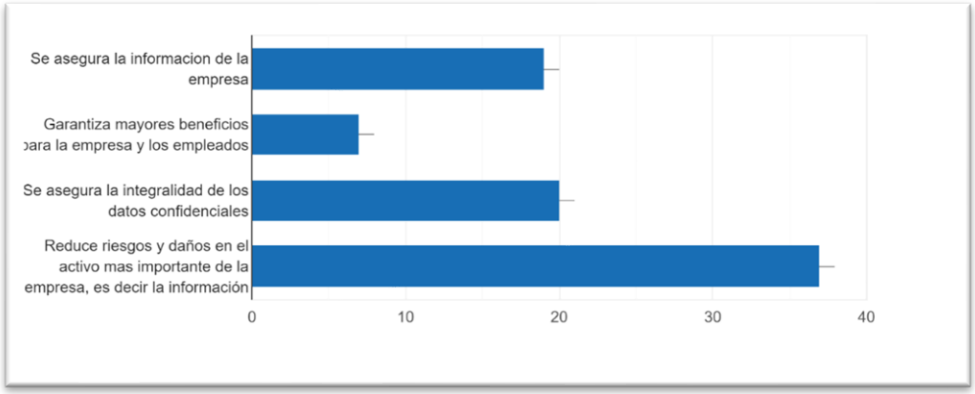
Se evidencia que el 98% de las personas consideran importante capacitarse sobre la norma; es importante tener presente que el fin de la ISO 27001 se implementa en las empresas con el fin de prevenirlas de amenazas y vulnerabilidades que pueda presentar en el funcionamiento de las actividades del negocio.

3. ¿Qué considera que se obtiene implementando la ISO 27001?



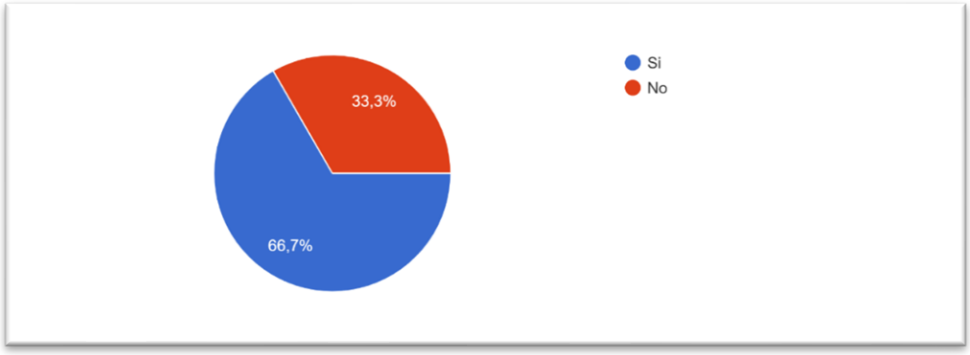
El 83,3% de las personas indica que al implementar la Iso se reducen riesgos.

4. ¿Está de acuerdo con que se implemente la ISO 27001 en la empresa en que está trabajando actualmente, cual razón considera que sería más relevante?



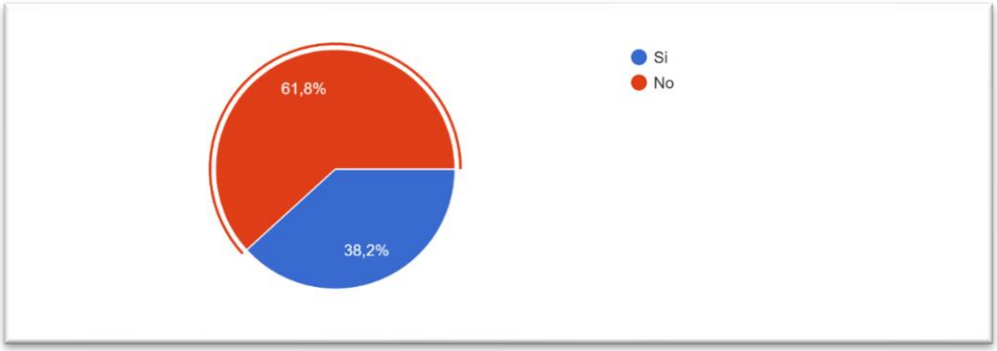
- Para el 72,5% de las personas es importante Reducir los riesgos a los que pueda estar expuesta la información, ya que se considera el activo más importante dentro de una organización.
- El 39,2 % de las personas considera que la ISO 27001 asegura la integralidad de los datos confidenciales.
- El 13,7% que la norma Garantiza mayores beneficios para la empresa y los empleados.
- El 37,3% Se asegura la información de la empresa.

5. ¿Usted actualmente se encuentra trabajando en alguna empresa?



El 66,7 % de las personas encuestadas se encuentran actualmente laborando en alguna empresa de la ciudad de Tunja, el 33,3% no se encuentran trabajando actualmente.

6. ¿En la empresa donde usted labora tienen implementado el Sistema de Gestión de Seguridad de la Información?



En este punto se analiza que hay un gran porcentaje 61,8% de la no implementación de la ISO 27001 del Sistema de Gestión de Seguridad de la información en algunas empresas Tunjanas, lo que demuestra que es necesario diseñar estrategias que permitan a las empresas mejorar sus sistemas para preservar y cuidar del activo más importante, la información.

7. La empresa tiene implementado el SGSI

Por favor indique que políticas se manejan dentro de la empresa en el SGSI.

Estas fueron algunas de las respuestas

- Ninguna

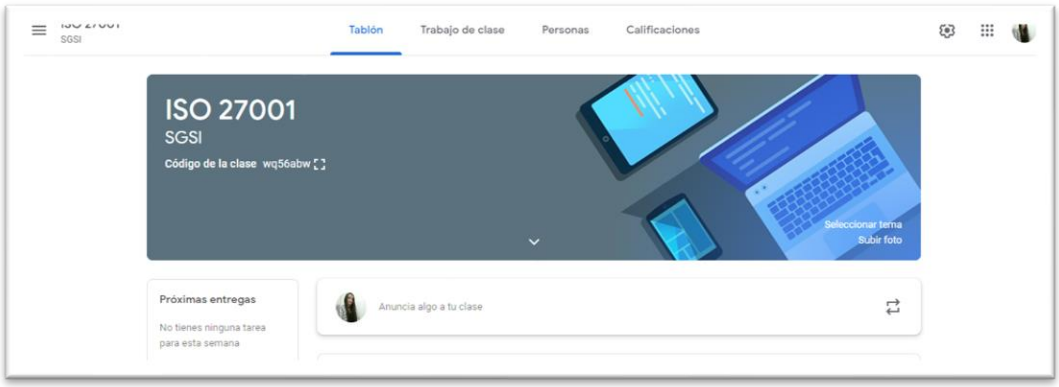
- La empresa carece de políticas relacionadas con el sistema de gestión de la seguridad de la información.
- No tienen políticas del sistema de gestión de la seguridad de la información
- Política de tratamiento de datos, Política de seguridad de la información
- Definición de los objetivos: Compromiso, comunicación y revisiones.
- Perfiles de acceso con los debidos permisos de acuerdo con el cargo
- Tabla de retención documental en la cual se almacena la información de manera segura y ordenada
- Se establecen manual de funciones y políticas de seguridad
- No tengo conocimiento, pero laboro en Bancolombia
- Confidencialidad de los datos, y no dar acceso a bases de datos de la IPS
- Manejo de información / control interno
- Control de información, reducción de riesgos
- Seguridad de la información
- Plataforma con códigos de ingreso
- Políticas de Calidad
- La confidencialidad e integridad de los datos y de la información
- Revisiones periódicas de riesgos de seguridad y los controles

Fase 2: Realización del Curso en la plataforma Google Class Room sobre la ISO 27001.

Se monto el curso en la plataforma Google Class Room, donde se dividió en 6 Unidades o módulos, cada uno tenia en promedio entre 5 y 7 preguntas.

Enlace de la clase https://classroom.google.com/

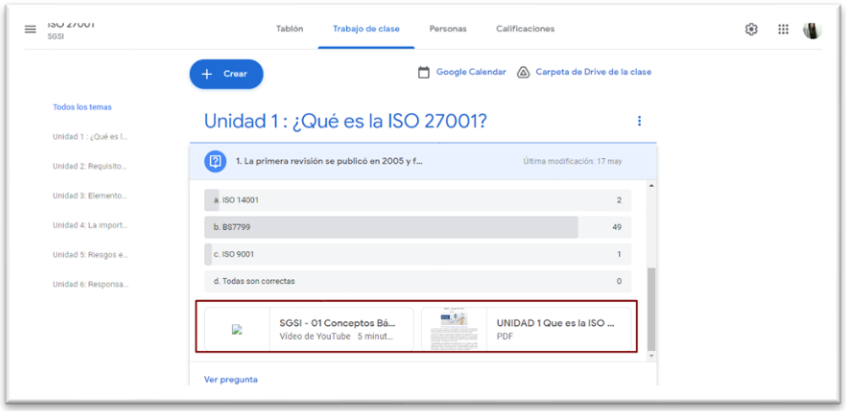
Código de la clase: wq56abw



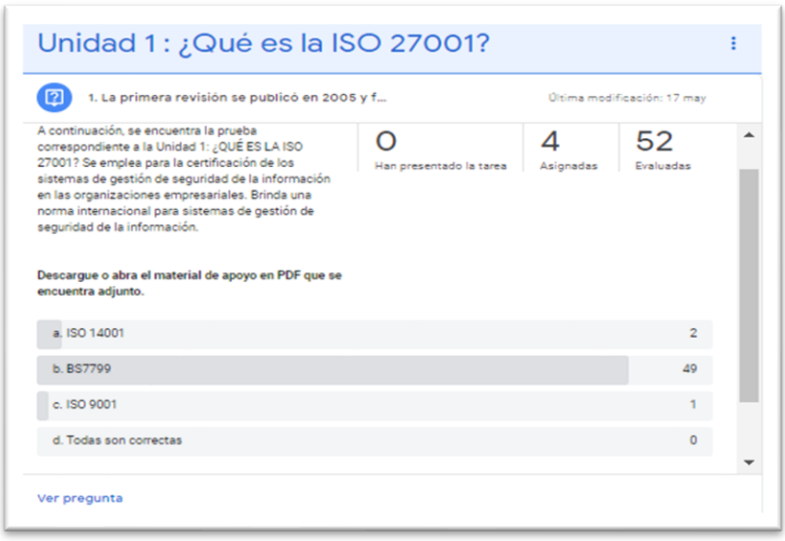
Grafica N°1 Plataforma Google Class Room

Grafica N° 2 Unidades curso

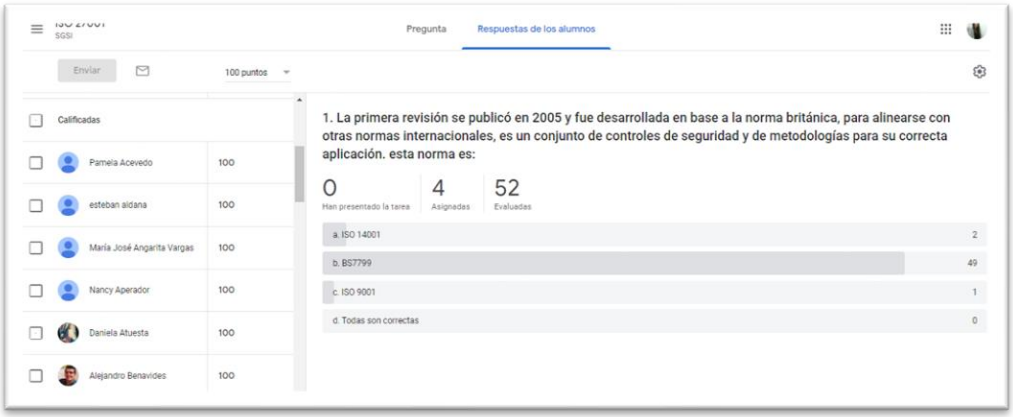
Se creó un material de apoyo en archivo PDF y videos de YouTube con la temática por unidad para apoyarse y responder el curso.



Grafica N° 3 Material de Apoyo



Grafica N° 4 Ilustración curso Unidad 1



Grafica N° 5 Respuestas curso Unidad 1

Unidad 1: *¿QUÉ ES LA ISO 27001?* Se emplea para la certificación de los sistemas de gestión de seguridad de la información en las organizaciones empresariales. Brinda una norma internacional para sistemas de gestión de seguridad de la información.

1. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica, para alinearse con otras normas internacionales, es un conjunto de controles de seguridad y de metodologías para su correcta aplicación. esta norma es:

    a. ISO 14001
    b. BS7799
    c. ISO 9001
    d. Todas son correctas

2. ¿La ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande?:

    a. Verdadero
    b. Falso

3. La seguridad de la información es parte de la gestión global del riesgo en una empresa ¿Dónde interviene la gestión de seguridad de la información en una empresa?

    a. La estructura y auditorias
    b. La ciberseguridad, la gestión de la continuidad del negocio y seguridad de la información.
    c. En la dirección y el teletrabajo
    d. Por área

4. Para certificarse en ISO 27001 en la auditoría de certificación se tienen en cuenta los pasos relacionados en el módulo:

    a. Revisión de documentación, auditoría principal y visitas de supervisión.
    b. Definición de la política, objetivos y alcance.
    c. Contratación de Auditores externos
    d. Ninguna es correcta

5. Las visitas de supervisión después de emitir el certificado en ISO 27001, se deben realizar por un periodo de:

    a. 5 años.
    b. 2 años
    c. 3 años
    d. 1 año

Unidad 2: REQUISITOS DE SEGURIDAD Los requisitos de la norma ISO 27001 son declaraciones que se elaboran para hacer posible la evaluación de los resultados.

1. Una de las declaraciones de requisitos de la norma ISO 27001 es:

    a. Cumplimiento en el negocio
    b. Integración en las primeras etapas de un proyecto
    c. Niveles de Prueba
    d. Todas son correctas

2. Las formas sistemáticas de identificación pueden prevenir algunos aspectos de ser olvidado o pasado por alto, se refiere a:

a. Adoptar los métodos para identificar los requisitos
b. Evaluar los requisitos según el valor de la información para el negocio
c. Resultados de las opiniones de las partes interesadas.
d. Definir los criterios para que se produzca la aceptación del producto

3. Que es un requisito de seguridad según la norma ISO 27001:

a. Evaluaciones en las diferentes áreas de la empresa
b. Resultados de las opiniones de las partes interesadas
c. Alcance y ámbito de aplicación de la norma
d. Son declaraciones que se elaboran para hacer posible la evaluación de los resultados.

4. Las personas que evalúan los resultaos y pueden emitirlos opiniones de las partes interesadas son:

a. Personas que tienen diferentes roles en la organización
b. La alta gerencia
c. La dirección de la empresa
d. Personal externo

5. En la evaluación según el valor de la información para el negocio, todos los requisitos deben priorizarse según con los propósitos de negocio que se encuentran destinados a protegerse.

a. Verdadero
b. Falso

6. Para llevar a cabo las pruebas de seguridad del Sistema de Gestión de Seguridad de la Información, se debe tener en cuenta:

a. Establecer ciertas condiciones que desencadenen en la necesidad de realizar una prueba.
b. Establecer rutinas para realizar las pruebas sistemáticas
c. Utilizar diferentes niveles de prueba
d. Entorno realista para el ensayo
e. Todas son Correctas

Unidad 3: ELEMENTOS O FASES PARA LA IMPLEMENTACIÓN DEL SGSI. Definir lineamientos que permita mitigar los posibles riesgos de seguridad de la información.

1. En la Fase 1 del Sistema de gestión de Seguridad SGSI segun la ISO 27001 se debe definir primero:

a. El Riesgo
b. La Política
c. El Alcance
d. Los Objetivos

2. El análisis de activos de información y la definición de amenazas y vulnerabilidades, se refiere a:

a. Selección de controles a implementar
b. Gestión de Riesgo
c. Activos de información
d. Análisis de Riesgos

3. Según la metodología vista, para la evaluación de riesgo se debe identificar las siguientes fases:

a. Cumplimiento de la norma, análisis de Riesgo y adaptación de políticas
b. Activos de Información, Vulnerabilidades, amenazas, requisitos legales y contractuales y riesgos
c. Auditoria, documentación y verificación
d. Ninguna es correcta

4. Todo aquello que tiene valor para la organización, incluyendo soportes físicos (edificios o equipamientos), intelectuales o informativas (Ideas, aplicaciones, proyectos, etc.), se refiere a:

a. Activos de Información
b. Amenazas
c. Vulnerabilidades
d. Ninguna es correcta

5. Aquellas cosas que puedan suceder y dañar el activo de la información, tales como desastres naturales, incendios o ataques de virus, se refiere a:

a. Las Amenazas

b. Las Vulnerabilidades
c. Los Activos de Información
d. Todas son correctas

6. Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información se refiere a:

a. Las Amenazas
b. Las Vulnerabilidades
c. El Riesgo
d. Activos de Información

Unidad 4: LA INFORMACIÓN El activo imprescindible de su organización para su respectiva solución, las preguntas que encontrará corresponden a todos los contenidos vistos en la unidad y que usted debe estar en capacidad de responder.

1. Los sistemas de información que soportan los procesos del negocio (ventas, facturación, contabilidad, contratación) en una empresa están formados por:

a. Activos intangibles, como la reputación, el software, el know-how de los empleados o la propiedad intelectual.
b. Activos tangibles, es decir, en ordenadores, discos duros, carpetas, archivos, etc.
c. Los activos que sean archivos en formato digital con datos, como documentos de texto, bases de datos y hojas de cálculo.
d. Activos tangibles, que podemos inventariar, y también activos intangibles.

2. Llamamos activos de información a toda información que tiene valor para la empresa y que, por tanto, tendremos que proteger. ¿En qué formato se encuentran los activos de información de las empresas hoy en día?

a. En papel, en formato digital y en las personas, con su conocimiento o know-how.
b. Fundamentalmente en papel.
c. Solo en formato digital en ordenadores y dispositivos electrónicos como móviles.
d. En la cabeza de las personas, los activos de información son su conocimiento del negocio o know-how.

3. Los tres pilares sobre los que se sostiene la seguridad de la información son:

a. Disponibilidad, integridad y criticidad.
b. Integridad, autenticidad y criticidad.

c. Disponibilidad, autenticidad e integridad.
d. Disponibilidad, integridad y confidencialidad.

4. La confidencialidad es la propiedad que hace referencia a:

a. Que la información se encuentre libre de errores y modificaciones causadas de forma accidental.
b. Que la información se encuentre cifrada y alojada en un lugar seguro de la organización.
c. Que la información no se pone a disposición o no se revela a individuos, entidades o procesos no autorizados.
d. Que la información solamente sea accesible por su propietario, independiente de que haya o no más procesos de negocio que requieran su acceso.

5. La disponibilidad es la propiedad que hace referencia a:

a. la información sea accesible cuando sea necesaria.
b. Que la información no sea robada por un ciberdelincuente.
c. Que la información mantenga los mismos datos que en su último acceso.
d. La seguridad de la misma desde un punto de vista global en el ámbito empresarial.

6. La integridad es la propiedad que hace referencia a:

a. Que la información se encuentre libre de errores o modificaciones en su contenido provocados de forma accidental o intencionada por ciberdelincuentes o insiders.
b. Que la información pueda ser accesible por los empleados de la empresa que requieran su uso para desempeñar las labores cotidianas de la organización.
c. Que la información sea accesible únicamente por los empleados que deben conocer su contenido.
d. Que la información se encuentre libre de errores o modificaciones en su contenido, provocados exclusivamente por ciberdelincuentes o insiders.

7. Un dato personal es:

a. Un documento de identificación como la cédula.
b. Un correo electrónico si se puede asociar a una persona física.
c. Todas las opciones son correctas.
d. Una fotografía.

8. Si la empresa recoge datos personales, desde ese momento tiene capacidad para hacer con ellos lo que más convenga a la organización, sin que los usuarios puedan hacer ejercer ningún tipo de derecho:

a. Sí, siempre que el usuario haya aceptado los términos y condiciones del servicio.
b. Sí, siempre que los datos personales se encuentren en formato físico.
c. No, ya que existen derechos y libertades que deben ser respetados de acuerdo a lo indicado en la ley.
d. Sí, porque así lo establece el Reglamento General de Protección de Datos, el RGPD.

Unidad 5: Riesgos en SGSI.

1. ¿Qué se debe tener en cuenta para levantar un inventario y como se clasifica de acuerdo con los modelos estándar de la ISO 27001?
a. Clasificación de la información e Inventario de activos
b. Propiedad de los Activos, Clasificación de la Información, Inventario de Activos y Etiquetado y manipulado de la información.
c. Ninguna es correcta

2. Para Clasificar los activos se hacen de acuerdo con:

a. A la información, si es de carácter público o privado
b. La confidencialidad, integridad y disponibilidad
c. Todas son correctas

3. A qué nivel se refiere la clasificación de un activo de acuerdo con la confidencialidad: indica que los activos de información que se maneja son de carácter confidencial y en caso de ser conocida, por terceros no autorizados, genera un impacto negativo de índole legal, operativa, perdida de imagen o económica:

a. Alto
b. Medio
c. Bajo
d. Ninguna es correcta

4. El planear según las cuatro fases del SGSI consiste en:

a. Aceptación del Riesgo, Valoración del riesgo, Planificación del tratamiento del riesgo, establecer el contexto

b. Establecer el contexto. Implementación del plan tratamiento de riesgo, Monitoreo y revisión continuos de los riesgos.
c. Establecer el contexto, valoración del riesgo, monitoreo y revisión continuos de los riesgos.
d. Todas son correctas

5. El hacer según las cuatro fases del SGSI consiste en:

a. Valoración del riesgo, monitoreo y revisión continuos de los riesgos
b. Establecer el contexto
c. Implementación del plan tratamiento de riesgo
d. Mejorar los procesos

6. El Verificar según las cuatro fases del SGSI consiste en:

a. Implementación del plan tratamiento de riesgo
b. Valoración del riesgo
c. Monitoreo y revisión continuos de los riesgos
d. Revisión de las áreas

7. Según el proceso de gestión del riesgo en la seguridad de la información, mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información, se refiere al proceso de SGSI:

a. Verificar
b. Actuar
c. Planificar
d. Investigar

Unidad 6: RESPONSABILIDAD Y ROLES PARA EL SGSI

1. ¿Quiénes deben aplicar y cumplir el manual de políticas de SGSI?

a. Los funcionarios solamente
b. El oficial de seguridad de la información
c. Clientes, proveedores y funcionarios de toda la organización
d. Todas las personas externas e internas

2. ¿Quién es el encargado de supervisar el cumplimiento de la política SGSI?

a. El gerente de la empresa
b. El oficial de seguridad de la información
c. Todos los funcionarios.

d. Los auditores

3. ¿Cuáles son los principios que rigen una política de SGSI, relacionados con la separación de funciones?

a. Automatizar todo, prohibir todo, proteger todo, no autorizar nada, implementar lo mejor en cuanto a TICS
b. Necesidad de saber, menor privilegio, separación de deberes, rotación de trabajo, cuidado necesario, debida diligencia, altos privilegios.
c. Uso autorizado, permisos para todo, requisitos claros, aplicaciones nuevas, gestión de vulnerabilidades.
d. Las funciones por área.

4. ¿Qué es una política de seguridad de la información?

a. Una forma de controlar todo para que nadie haga nada que no esté permitido
b. Un capricho del gerente para poner más trabajo a cada empleado
c. Es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información, además contiene la definición de la seguridad de la información desde el punto de vista de la empresa.
d. Todas son correctas

5. ¿Cómo se conforma el comité de seguridad de la información?

a. Se conforma de manera formal y sus roles y funciones las cuales se encuentran documentadas en el manual de los sistemas de gestión dentro de la empresa.
b. Se conforma por decisión de la gerencia.
c. Se conforma por el oficial de cumplimiento y el gerente de la empresa.
d. Ninguna es correcta

Conclusiones

- De la muestra realizada a las personas encuestadas se concluye que es necesario implementar la ISO27001 para la reducción de riesgos y vulnerabilidades a la que puede estar expuesta una organización, teniendo en cuenta que la información es el activo más importante.
- De acuerdo con el curso aplicado a empleados de diferentes empresas de la ciudad de Tunja se evidencio que se obtuvieron resultados positivos, ya que la media de la clase está en un 84,86% lo que indica que el curso es una buena estrategia para mejorar el nivel de conocimiento de los empleados dentro de las empresas.
- Las organizaciones deben incorporar estrategias para mejorar el conocimiento de los empleados sobre el Sistema de Gestión de Seguridad de la Información además de adaptar procesos y políticas que garanticen la protección de la seguridad mediante los tres pilares de la seguridad: confidencialidad, integridad y disponibilidad; teniendo en cuenta los recursos económicos y humanos con los que se cuenta dentro de la organización.
- Se evidencia que en algunas empresas de la ciudad de Tunja hay un índice alto de ausencia de la implementación de la ISO 27001, lo que puede ocasionar que existan grandes pérdidas y daños dentro de las organizaciones.
- Es importante que en las empresas Tunjanas se implemente el sistema de Gestión de información para así evitar y controlar amenazas internas y externas además de buscar la mejora de los procesos con la certificación de la Norma ISO/IEC 27001 ya que es la conexión de los diferentes sistemas dentro de la organización.
- Se concluye, por último, que dentro de algunas empresas donde trabajan los funcionarios encuestados no manejan Políticas del Sistema de gestión de Seguridad de la información, es importante que se implementen Manuales con las políticas que manejen las organizaciones para las buenas prácticas y buen funcionamiento.

Bibliografía

1. Valencia-Duque, F. J., & Orozco-Álzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista Ibérica de Sistemas e Tecnologías de Información.
2. Ascanio, J. G. A., Trillos, R. A. B., & Bautista, D. W. R. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. Tecnura, 19(46), 123-134.
3. Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. Scientia et technica, 17(47), 334-339.
4. Miranda Cairo, M., Valdés Puga, O., Pérez Mallea, I., Portelles Cobas, R., & Sánchez Zequeira, R. (2016). Metodología para la implementación de la Gestión Automatizada de Controles de Seguridad Informática. Revista Cubana de Ciencias Informáticas, 10(2), 14-26.
5. Monsalve-Pulido, J. A., Aponte-Novoa, F. A., & Chaves-Tamayo, D. F. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). Facultad de Ingeniería, 23(37), 65-72.
6. Estupiñán, A. D. C. A., Pulido, J. A., & Jaime, J. A. B. (2013). Análisis de Riesgos en Seguridad de la Información. Ciencia, innovación y tecnología, 1, 40-53.
7. Portillo Gómez, E. (2015). Estrategia de innovación como marco para la adopción de un Sistema de Gestión de Seguridad de la Información (Bachelor's thesis, Universidad Piloto de Colombia).
8. Gutiérrez, G. V. R., Jaime, J. A. B., & González, I. A. D. (2018). Gestión de seguridad de la información en las organizaciones. Investigación e Innovación, 111.
9. Alvarez Isaza, Z. M. (2016). ISO/IEC 2700: 2013-sistemas de gestión de seguridad de la información (Bachelor's thesis, Universidad Piloto de Colombia).
10. Giraldo Bedoya, N. M., & Arias Vanegas, C. (2020). Razones de la falta de certificación de las organizaciones colombianas en la norma ISO/IEC 27001: 2013.
11. Gómez Galindo, D. M. (2018). Desarrollo del sistema de gestión de seguridad de la información (SGSI) alineado con el estándar ISO 27001 y sus requisitos básicos en la aplicación del ciclo PHVA.