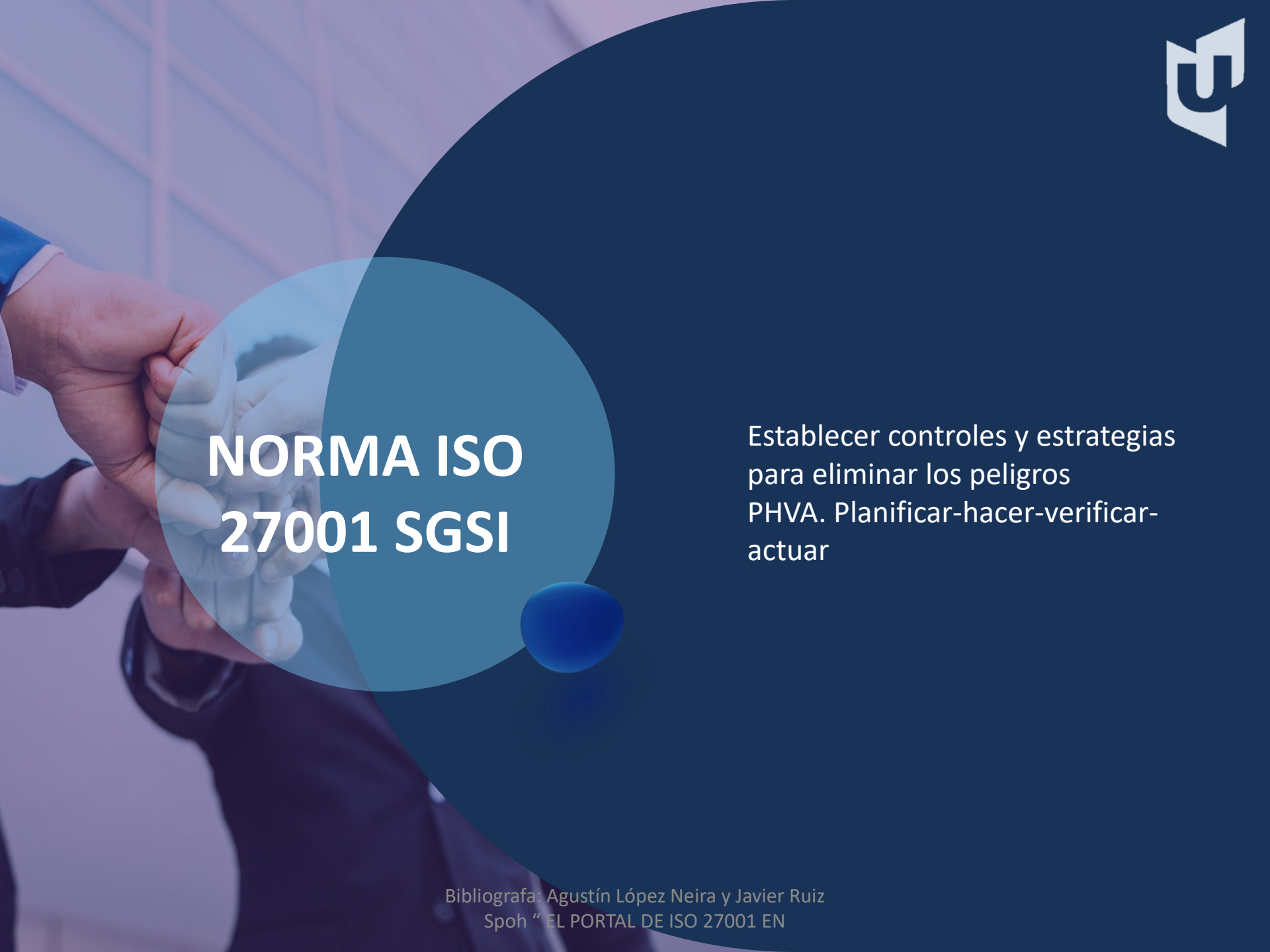
INICIO GRABACIÓN

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

SANJOSÉ
FUNDACIÓN DE EDUCACIÓN SUPERIOR

INDICE

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN



NORMA ISO 27001 SGSI

Establecer controles y estrategias para eliminar los peligros
PHVA. Planificar-hacer-verificar-actuar

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

CONCEPTOS

Contenido.

- Aspectos claves de la norma ISO 27001
- Análisis y evaluación de riesgos
- Implementar controles
- Plan para tratar los riesgos
- Proceso documental
- Auditorias internas
- Automatizar SGSI – ISO 27001

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

CONCEPTOS

Contenido.

Aspectos claves de la norma ISO 27001

- Solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) permite evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización propia o de terceros.

- Establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros.
  Basado en el ciclo de mejora continua o de Deming. El ciclo consiste, en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act).

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

CONCEPTOS

Contenido.

Aspectos claves de la norma ISO 27001

PLANIFICAR	Definir la política de seguridad Establecer al alcance del SGSI Realizar el análisis de riesgo Seleccionar los controles Definir competencias Establecer un mapa de procesos Definir autoridades y responsabilidades
HACER	Implantar el plan de gestión de riesgos Implantar el SGSI Implantar los controles

CONTROLAR	Revisar internamente el SGSI Realizar auditorías internas del SGSI Poner en marcha indicadores y métricas Hacer una revisión por parte de la Dirección
ACTUAR	Adoptar acciones correctivas Adoptar acciones de mejora

Bibliografía
Spoh " EL PORTAL DE ISO 27001 EN

CONCEPTOS

Contenido.

fases de un SGSI basado en la norma ISO 27001

La norma ISO 27001 establece las siguientes fases para elaborar un SGSI

1. Análisis y evaluación de riesgos.
2. Implementación de controles
3. Definición de un plan de tratamiento de los riesgos o esquema de mejora
4. Alcance de la gestión
5. Contexto de organización
6. Partes interesadas
7. Fijación y medición de objetivos
8. Proceso documental
9. Auditorías internas y externas

Bibliografa: Agustín López Neira y Javier Ruiz Spohr " EL PORTAL DE ISO 27001 EN

ANALISIS Y EVALUACION DE RIESGOS: Identificar amenazas, consecuencias

Una amenaza se define como cualquier **evento que puede afectar los activos de información** y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. Ejemplos pueden ser: ataques informáticos externos, infecciones con malware, una inundación, un incendio o cortes de fluido eléctrico.

Una omisión o despiste por parte del personal de la empresa, como el uso de una simple pulsera imantada, para que se pueda llegar a producir un daño grave, e incluso irreparable, de la información.

Elaborar una **adecuada gestión de riesgos** que permita a las organizaciones conocer cuáles son las principales vulnerabilidades de sus activos de información.

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

ANALISIS Y EVALUACION DE RIESGOS: Identificar amenazas, consecuencias

Un **proceso de identificación de riesgos** implica:

- Identificar todos aquellos activos de información que tienen algún valor para la organización.
- Asociar las amenazas relevantes con los activos identificados.
- Determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

ANALISIS Y EVALUACION DE RIESGOS:
Identificar amenazas, consecuencias

El **impacto en el negocio de un fallo de seguridad** que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información, **evaluando de forma realista la probabilidad de ocurrencia** de un fallo de seguridad en relación a las amenazas, vulnerabilidades e impactos en los activos.

A**nalizar también sus consecuencias potenciales**, muchas y distinta gravedad: desde una simple dispersión de la información a la pérdida o robo de datos relevantes o confidenciales.

Una **metodología de evaluación de riesgos** esta compuesta de las siguientes fases:

1. Recogida y preparación de la información.
2. Identificación, clasificación y valoración los grupos de activos.
3. Identificación y clasificación de las amenazas.
4. Identificación y estimación de las vulnerabilidades.
5. Identificación y valoración de impactos: identificar, tipificar y valorar los impactos.
6. Evaluación y análisis del riesgo.

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

La implementación de controles

La norma ISO 27001 establece en su última versión: ISO/IEC 27001:2013 hasta 113 puntos de control (en la versión anterior del 2005 eran 133).

Los 113 controles están divididos por grandes objetivos:

- Políticas de seguridad de la información.
- Controles operacionales.

Cada empresa, según su parecer, puede añadir más puntos de control si lo considera conveniente, así como personalizarlos **para adaptarlos a su propio Plan de Control Operacional**, pero siempre deben estar alineados a lo que pide la norma.

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

F ormas de afrontar el riesgo

El **riesgo** básicamente de **tres formas diferentes**: eliminarlo, mitigarlo o trasladarlo.

Eliminar el riego

Si es muy crítico, hasta el punto de que pueda poner en peligro la propia continuidad de la organización, debe poner todos los medios para tratar de eliminarlo, que haya un **posibilidad cero de que la amenaza se lle gue realmente a producir.**

mitigarlo

En la gran mayoría de ocasiones **no es posible llegar a la eliminación total riesgo,** ya sea porque es imposible técnicamente o bien porque **la empresa decida que no es un riesgo suficientemente crítico. La** organización puede aceptar el riego, ser consciente de que la amenaza para la informa ción existe y dedicarse a monitorearlo con el fin de controlarlo.

Se trata de **implantar las medidas preventivas o correctivas necesarias** con el fin de **reducir la posibilidad de ocurrencia** o el impacto de riesgo.

trasladarlo

Esta relacionada con la **contratación de algún tipo de seguro** que compense las consecuencias económicas de una pérdida o deterioro de la información.

La gestión de riesgos debe garantizar a la organización la tranquilidad de tener suficientemente identificados los riesgos y los controles pertinentes, lo cual le va a permitir actuar con eficacia ante una eventual materialización de los mismos.

Bibliografa: Agustín López Neira y Javier Ruiz
Spoh " EL PORTAL DE ISO 27001 EN

Se debe **mantener el equilibrio** entre el costo que tiene una actividad de control, la importancia del activo de la información para los procesos de la empresa y el nivel de criticidad del riesgo.

Establecimiento de un rango para cada control

A cada punto de control se le debe **asociar un rango o factor determinado**. Por ejemplo, el acceso a un área segura podría dividirse en:

Rango 1. No hay establecida ninguna medida de seguridad.

Rango 2. Existe alguna medida de seguridad pero no se ha establecido una pauta concreta ni periodicidad.

Rango 3. Existen una serie de medidas establecidas, pero no se ha determinado una evaluación de las mismas.

Bibliografa: Agustín López Neira y Javier Ruiz
Spoh " EL PORTAL DE ISO 27001 EN

Rango 4. Los controles tienen establecidos una periodicidad, evaluación y seguimiento.

Rango 5. Son actividades ligadas al propio negocio, se trata de un factor interno de la empresa que lo gestiona y está implementada dentro de la propia organización.

Ejemplo, es más seguro instalar un dispositivo que controle la temperatura (saltará la alarma antes de que se produzca un posible incendio) que tener un sistema anti incendio que avisa cuando ya hay humo (la situación peligrosa ya ha empezado a producirse).

Todos los controles **siguen un ciclo de mejora continua** vinculado al plan de tratamiento de riesgos y asociados a la evaluación de los mismos para el **cálculo del riesgo residual**, que es el riesgo bruto mitigado por los controles.

Mediante el proceso de mejora continua es posible comprobar la eficacia de los controles o si es necesario cambiar de rango o factor de seguridad, realizando las modificaciones que sean necesarias.

Los controles están **incluidos en el anexo A de la norma ISO 27001** y su nivel de detalle y especificidad los diferencian de los existentes en otras normas, que tienen un carácter más generalista y transversal.

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

Alcance de la gestión

En la planeación para la implementación de un SGSI **es importante definir el alcance** para la implementación del sistema en una organización.

Teniendo en cuenta que existen organizaciones que difieren en tamaño por el número de empleados, volumen de información manejada, número de clientes, volúmenes de activos físicos y lógicos, número de sedes u oficinas, entre otros elementos, **se hace necesario determinar cómo se debe implantar un SGSI**.

F ijación de objetivos

Fijar unos objetivos **para la gestión de riegos**, **deben poder ser medibles,** aunque no es necesario que sean cuantificables.

S**er eficientemente comunicados al conjunto de los empleados de la empresa,** puesto que todos los profesionales deben ser conscientes de que participan en un objetivo común, y que un descuido o una mala actitud pueden acarrear consecuencias muy negativas.

Bibliografa: Agustín López Neira y Javier Ruiz
Spoh " EL PORTAL DE ISO 27001 EN

Además, todas las personas que trabajan en la organización deben **poseer las competencias necesarias en materia de seguridad de la información** según su puesto o función en la empresa.

C**ada objetivo** definido tiene que estar **asociado a unos indicadores** que permitan realizar un seguimiento del cumplimiento de las actividades.

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

El proceso documental

La norma ISO 27001 da mucha importancia a la **documentación**, manera muy estricta cómo se debe gestionar la documentación y exigiendo que la organización cuente con un procedimiento documentado para gestionar toda la información. Esta cuestión es **fundamental para la obtención de la certificación**.

La documentación puede ser presentada en diversos formatos: documentos en papel, archivos de texto, hojas de cálculo, archivos de vídeo o audio, etc. Pero en cualquier caso constituye un marco de referencia fundamental y debe estar lista en todo momento para que pueda ser consultada.

Se debe **gestionar tanto los documentos internos** (políticas diversas, procedimientos, documentación del proyecto), **como lo externos** (diferentes tipos de correspondencia, documentación recibida con equipamiento). Por este motivo, la gestión de documentación es una tarea compleja e integral.

Con el objetivo de que las empresas gestionen eficazmente los documentos, la norma ISO 27001 **exige la aplicación de un método sistemático** para su mane jo, así como la **redacción de un procedimiento para su gestión**.

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

Auditorías internas y revisión por la dirección

Las auditorías internas

Llevar **a cabo auditorías internas cada cierto tiempo** para poder comprobar que el sistema se encuentra en un estado idóneo.

Existen **dos grandes tipos de auditorías internas:**

- **Gestión**. Donde se supervisa el liderazgo, el contexto, etc.
- **Controles**. En este caso se auditan los 113 controles, normalmente se realiza por personal más experto y puede realizarse en años distintos

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

Las auditorías internas

El plan de auditoría interna

Se debe contar con el nivel de importancia de los procesos y de las áreas que van a ser auditadas y, además, hay que tener en cuenta los resultados obtenidos de auditorías previas.

Es necesario definir los criterios utilizados durante la auditoría, el alcance, la frecuencia y los métodos utilizados.

Si se detectan problemas o desviaciones entre los objetivos de seguridad planteados y los resultados obtenidos, **el equipo auditor comprueba si se están aplicando las medidas necesarias, proponiendo nuevas medidas en caso necesario.**

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

Cómo automatizar el Sistema de GestióndeSeguridaddelaInformación según ISO 27001

Un software de automatización permiten poder llevar a cabo una **gestión muy eficaz y exhaustiva de cualquier tipo de riesgo:** operacionales, financieros, industriales, legales u operativos, ajustándolos completamente a las necesidades de cada una de las organizaciones y facilitando, en gran medida, la adecuación a la normativa.

Aspectos a tener en cuenta en este tipo de herramientas que facilitan la automatización de la gestión de riesgos son:

- Poner en marcha **procesos de identificación automática** de los riesgos a los que está expuesto cada organización.
- **Alinear cada riesgo con propuestas de posibles controles** para conseguir reducir los riesgos de las compañías.
- Poner en marcha un automático del **seguimiento del tratamiento** de riesgos.
- **Realizar proyecciones y simulaciones** que permitan visualizar los resultados que se podrían obtener con la implantación de los controles definidos en el plan de tratamiento de riesgos.

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

La plataforma ISOtools facilita la automatización de la ISO 27001

La ISO 27001 para los SGSI es sencilla de implantar, automatizar y mantener con la Plataforma Tecnológica ISOTools.

Con ISOTools se da cumplimiento a los requisitos basados en el ciclo PHVA (Planear – Hacer – Verificar – Actuar) para establecer, implementar, mantener y mejorar el Sistema Gestión de la Seguridad de la Información, así como se da cumplimiento de manera complementaria a las buenas prácticas o controles es- tablecidos en ISO 27002.

ISOTools también permite aplicar los requisitos de otras normas de Seguridad de la Información como PMG SSI de los Servicios Públicos de Chile, entre otros.

Este software, permite integrar la ISO 27001 con otras normas, como ISO 9001, ISO 14001 y OHSAS 18001 de una forma sencilla gracias a su estructura modular

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

Sectores más interesados en la implementación de este sistema

Resulta especialmente interesante, y casi necesaria, en los **siguientes sectores**:

- **Salud**.
- **Sector público**.
- **Sector financiero**.

Sector de la salud

Especialmente atractiva para las organizaciones médicas, tanto públicas como privadas, por los siguientes motivos:

- La **información** que manejan es especialmente **crítica y confidencial**.
- Los requisitos y medidas planteados por la ISO 27001 garantizan la **confidencialidad y seguridad de la información de los pacientes** y trabajado- res ante cualquier amenaza.
- En todo momento **se preserva la confidencialidad, integridad y disponibilidad** de la información.
- Con la aplicación de este sistema se consiguen **ventajas adicionales** como: mejorar la calidad de los servicios, disminuir los tiempos de espera o agilizar las comunicaciones internas y externas del hospital o centro de salud.

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

Sectores más interesados en la implementación de este sistema

Sector público

El sector público y la administración en general también son ámbitos muy interesados en la esta norma ISO 27001. El principal motivo es que permiten poner en marcha **sistemas y protocolos que garanticen la confidencialidad y gestión adecuada de la gran cantidad de datos** que manejan, muchos de ellos personales y con un alto nivel de criticidad.

Sector financiero

La ISO 27001 es muy necesaria para el sector financiero en general, y el de las grandes empresas en particular, con el fin de **asegurar los recursos humanos y financieros de las organizaciones.**

Algunas ventajas de la certificación ISO son:

- Lograr ventaja competitiva.
- Garantizar la gestión de la calidad.
- Controlar y reducir los riesgos operativos y comerciales.
- Cumplir con la legislación y normativa de cada país y sector.
- Poner en marcha procesos de mejora continua.

CONCLUSIONES

- La adopción de normas, como ISO 27001 nos dan mas garantía, para establecer políticas organizacionales que conduzca a la confidencialidad de la información
- Las auditorias nos ayudan a tener mas tranquilidad en nuestras actividades cotidianas en un ambiente laboral

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN

INICIO RECESO

Bibliografa: Agustín López Neira y Javier Ruiz
Spoh “ EL PORTAL DE ISO 27001 EN

FIN DE RECESO

Bibliografa: Agustín López Neira y Javier Ruiz
Spoh “ EL PORTAL DE ISO 27001 EN

FIN DE GRABACIÓN

Bibliografa: Agustín López Neira y Javier Ruiz Spoh " EL PORTAL DE ISO 27001 EN