



Proyecto para la Definición de un Sistema de Gestión de la Seguridad de la Información

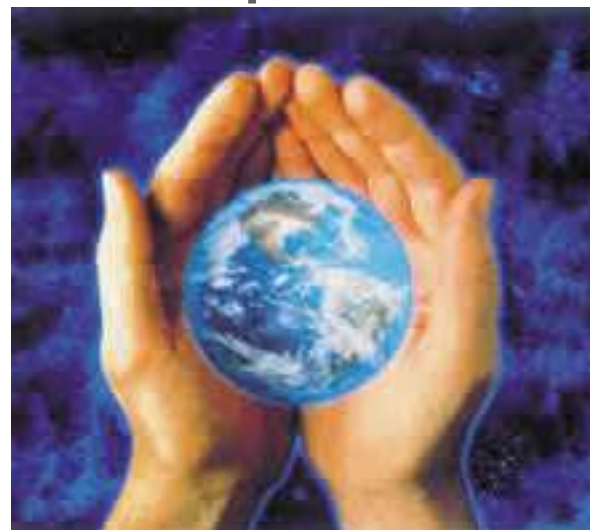
Pamplona, 27 de Mayo de 2010

Sistema de Gestión de la Seguridad de la Información (SGSI)



Un SGSI es un sistema de gestión para asegurar que la información está protegida frente a la pérdida de :

- Confidencialidad
- Integridad
- Disponibilidad



NORMAS APLICABLES



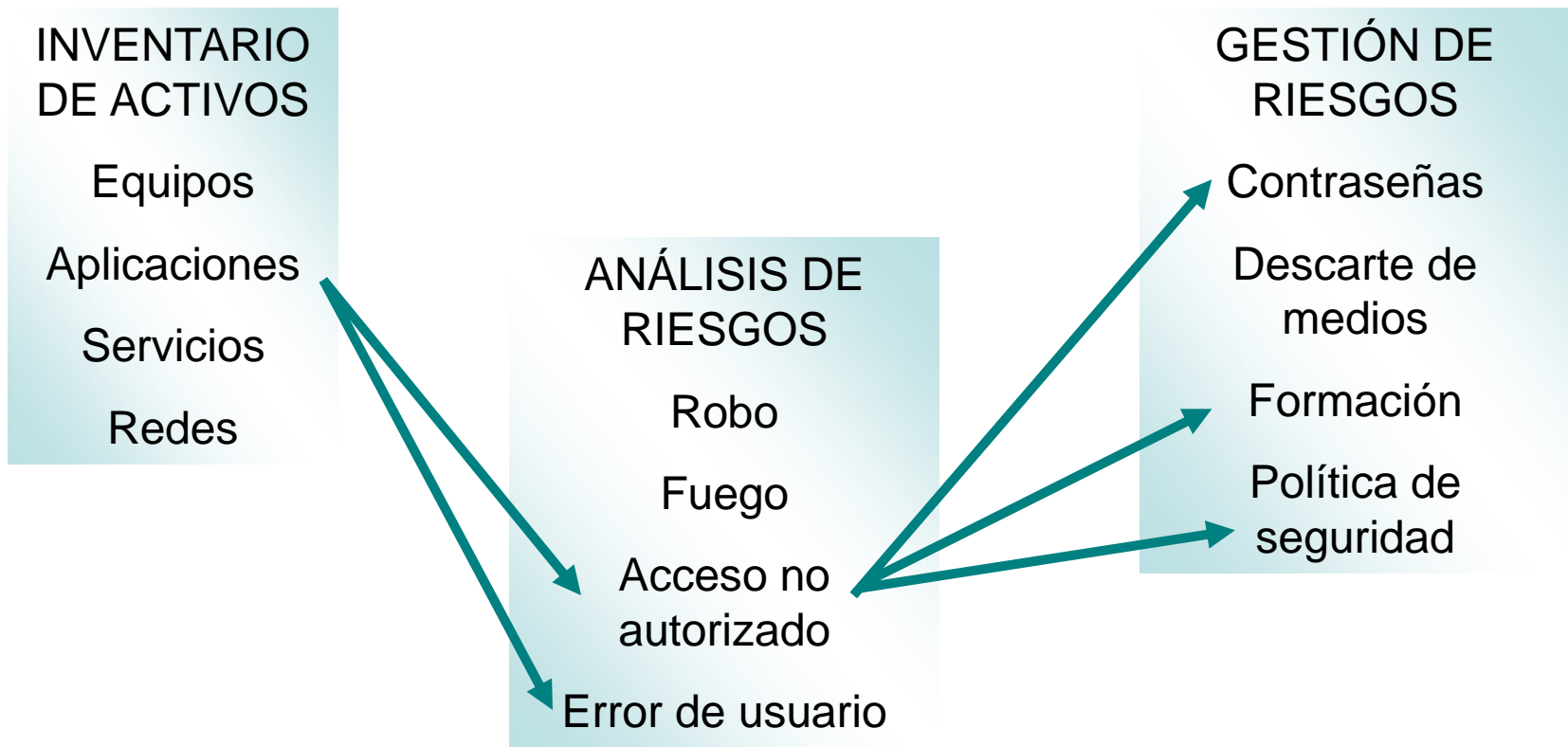
- Las pautas para realizar los elementos anteriores se recogen en la norma ISO 27001 (Certificable)
- La guía de buenas prácticas con el catálogo de controles a considerar se recoge en la norma ISO 27002 (Informativa)
- Más ayuda sobre técnicas en la UNE 71501, que son guías para la Gestión de la Seguridad de TI



ESTRUCTURA DEL SGSI



ELEMENTOS DEL SGSI



ACTIVIDADES PRINCIPALES



Tarea 1 - Lanzamiento del proyecto

Tarea 2 - Definición del alcance, los objetivos y la Política de Seguridad

Tarea 3 - Inventario de activos, análisis de riesgos y controles

Tarea 4 - Documentación

Tarea 5 - Implantación y formación

Tarea 6 - Auditoría interna y revisión SGSI

Tarea 7 - Apoyo para Auditoría de certificación

Tarea 1 -Lanzamiento del Proyecto

1. Reunión inicial y realización de entrevistas

Objetivos:

- Presentar el proyecto a la organización
- Definir el alcance y los límites del sistema
- Comprender el funcionamiento de la organización
- Conocer qué información se maneja en la organización y cómo se gestiona
- Conocer las expectativas, las prioridades y los objetivos de la organización
- Definir el conjunto de activos a proteger



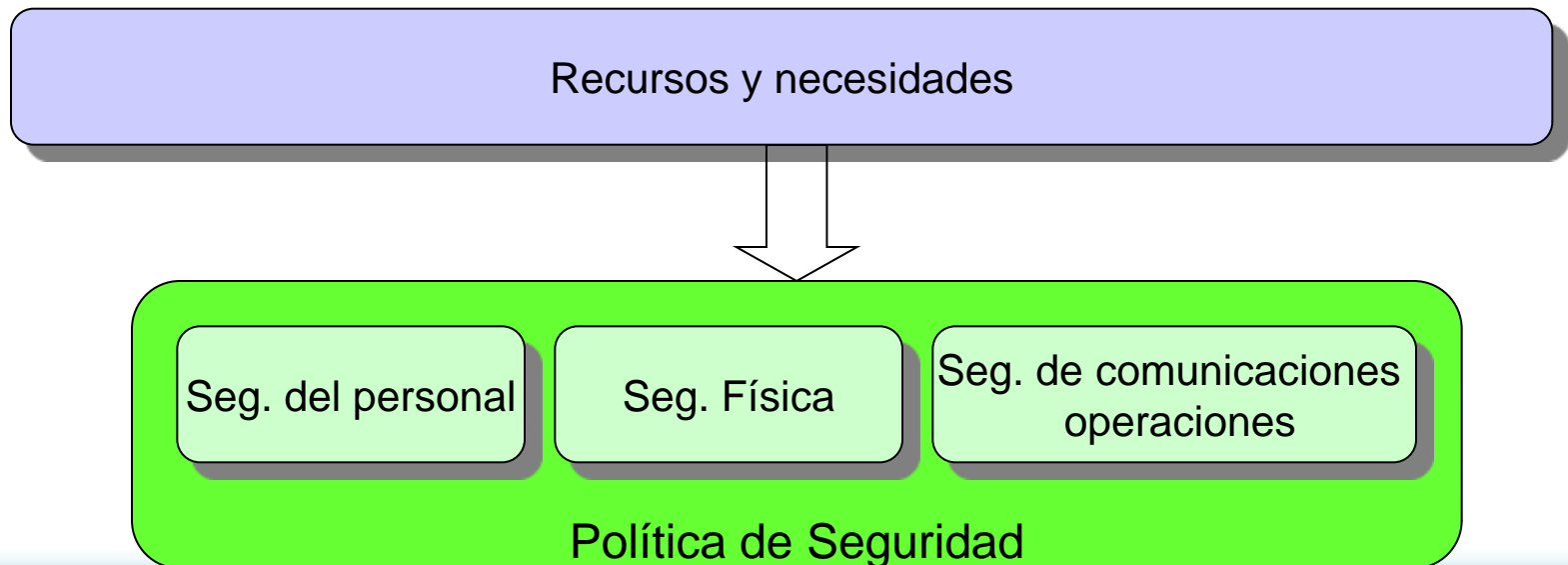
Tarea 2 Política de Seguridad



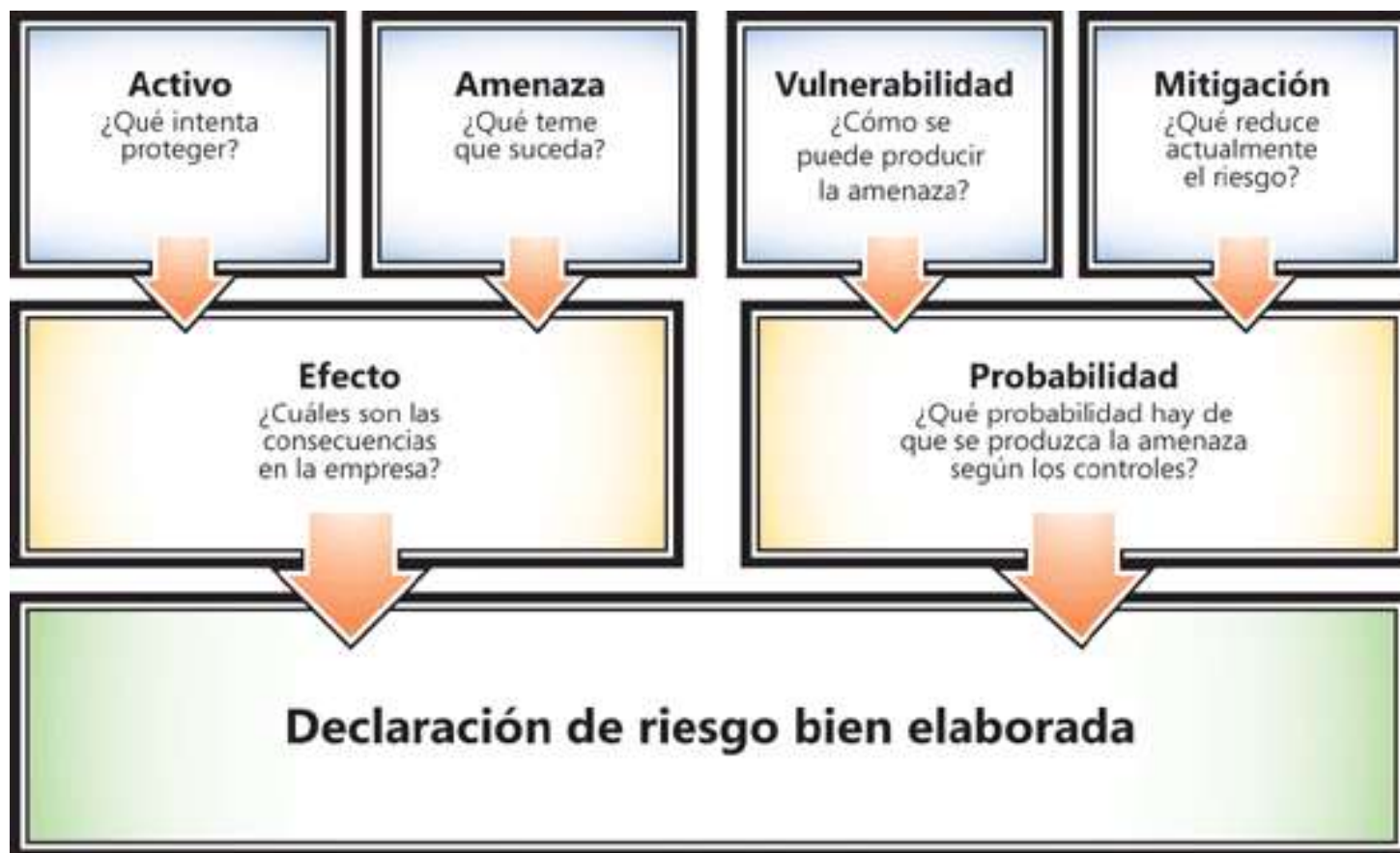
Debe cubrir todos los aspectos de la seguridad: seguridad física, seguridad lógica, seguridad del personal.

y

adecuarse a las necesidades y recursos de la organización



Tarea 3 - Análisis de riesgos



Tarea 4 - Documentación



- Análisis de riesgos
- Selección de controles
- Procedimientos para implantar los controles
- Procedimientos para la gestión del SGSI
- Plan de seguridad
- Plan de concienciación



Tarea 5 - Implantación y formación



- Puesta en marcha del plan de seguridad
- Puesta en marcha del plan de formación





Tareas 6 y 7 - Auditorías

Auditoría interna

- Se revisará el SGSI para comprobar que se ajusta a la norma y a los requisitos de la organización
- Se decidirán las acciones correctoras a tomar y se implementarán

Auditoría de Certificación

- Visita previa del Organismo de Certificación y emisión del informe de no conformidades
- Implantación de medidas correctoras
- Auditoría de Certificación.
- Obtención del Certificado

Implantación de la ISO 27701 en CITI Navarra

Mayo 2010

Índice

1. Introducción

- ¿Quiénes somos?
- ¿A quien van dirigidos los servicios del Colegio?

2. NTIC's en CITI Navarra

3. ISO 27001 en CITI Navarra.

- El “Por que”de este proyecto
- Principales problemas salvados.
- Factores claves del éxito.

1. Introducción: ¿Quiénes somos? (I)

¿Qué es un Colegio Profesional?

El Colegio es una corporación profesional de Derecho Público que tiene como finalidad esencial la ordenación y defensa del ejercicio de la profesión del ingeniero técnico industrial.

¿Cómo queremos ser percibidos?

- ✓ **Por los colegiados:** como una organización propia con retorno rentable de la inversión (no económico).
- ✓ **Por los estudiantes:** como un puente entre la universidad y el mercado laboral.
- ✓ **Por los clientes:** como una organización prestadora de servicios de valor añadido.
- ✓ **Por la sociedad:** como una entidad que vele por la calidad del trabajo realizado por ingenieros técnicos industriales.
- ✓ **Por la empresa y la administración:** como colaborador y/o proveedor reconocido de servicios.
- ✓ **Por el personal:** como empresa sólida en la que desarrollarse personal y profesionalmente.
- ✓ **Por otros colegios:** como referente en gestión e innovación.

¿Qué compromisos asumimos?

- ✓ Orientación al cliente.
- ✓ Profesionalidad en nuestros servicios.
- ✓ Comportamiento ético.
- ✓ Compromiso con la sociedad.

1. Introducción: ¿Quiénes somos? (II)

CITI Navarra en datos

- ✓ Representa a más de **2.300** ingenieros técnicos industriales colegiados en Navarra.
- ✓ Cuenta con **10 personas** contratadas.
- ✓ Dispone de más de **1.000 m² de instalaciones** en Pamplona.
- ✓ Esta gobernado por una **Junta de Gobierno**, compuesta por 10 personas.
- ✓ La **facturación** media anual es superior al 1.000.000 €.
- ✓ La media en **inversión en I+D**, es mayor al 20% anual. (últimos 5 años)
- ✓ Existe una apuesta clara por la **calidad en los servicios** y el medio ambiente (EFQM 300+ en 2008, ISO 9001, ISO 14.000, ISO 27.001, Sello compromiso RSC)
- ✓ Etc.

1. Introducción: ¿A Quien van dirigidos los servicios del Colegio?

Ingenieros técnicos
industriales

COLEGIADO: una vez acabada la carrera y cumpliendo unos determinados requisitos, cualquier ingeniero técnico industrial se puede colegiar y disfrutar de todos los servicios del Colegio en condiciones especiales.

Estudiantes de
ingeniería técnica
industrial

ESTUDIANTE ACREDITADO: los estudiantes del último curso de cualquiera de las especialidades de Ingeniería Técnica Industrial en la Universidad Pública de Navarra, UPNA, o bien de otras universidades pero empadronados en Navarra podrán utilizar varios de los servicios que ofrece el Colegio en condiciones especiales.

Empresas y otros
profesionales

EMPRESAS Y PARTICULARES: cualquier persona una vez se registre en CITI Navarra, podrá utilizar algunos de los servicios que ofrecemos.

2. NTIC's en CITI Navarra

Integración de distintos sistemas NTIC'S, para la mejora de los servicios que presta el Colegio:

- ✓ **Desarrollo a medida de un nuevo programa de gestión.**
- ✓ **Puesta en marcha de una herramienta de Gestión documental.**
- ✓ **Puesta en marcha del Visado electrónico.**
- ✓ **Automatización de los procesos por medio de flujos de trabajo.**
- ✓ **Desarrollo a medida de una nueva web, totalmente dinámica.**
- ✓ **Puesta en marcha de un servidor de aplicaciones.**
- ✓ **Nuevo servicio ERP, en modo SaaS, para empresas externas.**
- ✓ **Puesta en marcha de un CPD, con 4 servidores en cluster.**
- ✓ **Nuevo servicio de alojamiento web, para empresas.**

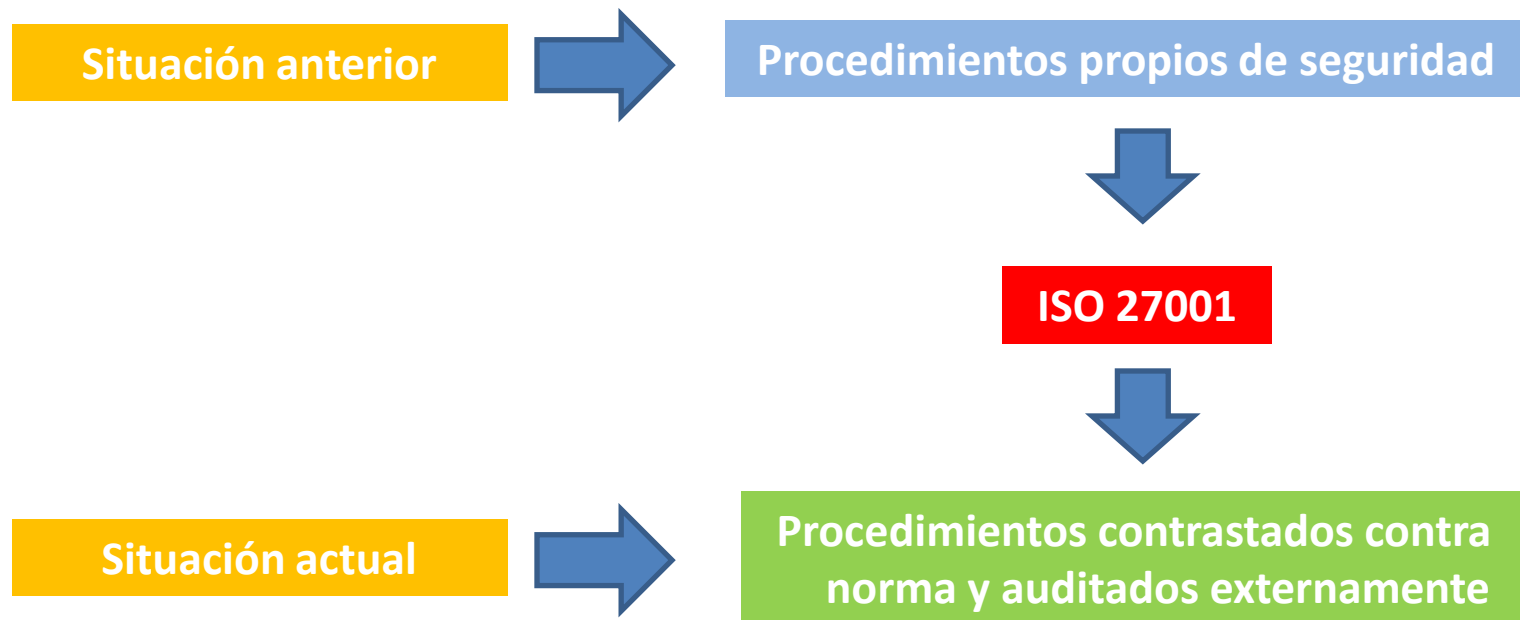
3. ISO 27001 en CITI Navarra: El “POR QUE” de este proyecto (I)

Se maneja gran cantidad de información:

- ✓ De la propia gestión interna
- ✓ Custodia de los trabajos profesionales de nuestros colegiados
- ✓ Datos de clientes de nuestros colegiados
- ✓ Toda la información de empresas que trabajan en modo remoto contra nuestros sistemas.
- ✓ Gestión de correos electrónicos de nuestros colegidos
- ✓ Gestión y alojamiento de páginas web de empresas externas.
- ✓ Etc.

3. ISO 27001 en CITI Navarra: El “POR QUE” de este proyecto (II)

Para asegurar los procedimientos de SGSI:



3. ISO 27001 en CITI Navarra: El “POR QUE” de este proyecto (III)

Para mejorar la imagen externa

Historicamente CITI Navarra ha tenido la confianza de sus colegiados



ISO 27001



Aumento de la confianza en nuestros SGSI



Nuevos servicios apoyados en las NTIC's

3. ISO 27001 en CITI Navarra: El "POR QUE" de este proyecto (IV)

Plan estratégico:

AÑO 2004



AÑO 2006



AÑO 2007



AÑO 2008



AÑO 2009



3. ISO 27001 en CITI Navarra : **Principales problemas salvados (I)**

Aspectos Humanos:

- ✓ **Formación de una persona en la norma**
- ✓ **Apoyo externo a través de una consultora**
- ✓ **Sensibilización al resto del personal.**
- ✓ **Información de los cambios al resto del personal.**

3. ISO 27001 en CITI Navarra: **Principales problemas salvados (II)**

Aspectos Tecnológicos:

- ✓ **Cambio de los sistemas cortafuegos.**
- ✓ **Instalación de un SAI por cada servidor físico.**
- ✓ **Virtualización de todos los servidores.**
- ✓ **Contratación de líneas ADSL con distintas compañías de telecomunicaciones.**
- ✓ **Balanceo de las líneas ADSL.**
- ✓ **Nueva copia de seguridad diaria y externa.**
- ✓ **Instalación de cámara de seguridad en CPD**
- ✓ **Instalación de control de accesos en CPD.**

3. ISO 27001 en CITI Navarra: **Factores claves de éxito**

- ✓ **Directrices claras desde dirección, demostrando en todo momento las mejoras conseguidas.**
- ✓ **Empezar por los procesos más sencillos y más fáciles de vender internamente.**
- ✓ **Involucrar a todo el personal de la organización en la puesta en marcha del sistema**
- ✓ **El personal esta acostumbrado a cambios**
- ✓ **Existía previamente un sistema ISO 9001 montado, así como una política de calidad EFQM implantada.**

Gracias por su atención

Para más información:

Contacto: Antonio Rodríguez Fernández

Empresa: CITI Navarra

Teléfono: 948150600

Email: arodriguez@citinavarra.com



REDISOFT



Soluciones
informáticas
integrales

Ángel M^a Manrique

- ✚ REDISOFT OFIMÁTICA S.L. es una empresa creada hace 9 años y ubicada en Tudela.
- ✚ Prestación de servicios y soluciones integrales a las empresas y organizaciones.
- ✚ Formada por profesionales con 20 años de experiencia.
- ✚ Buscando la confianza y seguridad del cliente en sus datos.



- ✚ ¿Por qué obtener una ISO de Seguridad de la Información?
 - ✚ Las organizaciones dependen absolutamente de la información.
 - ✚ Tan importante como el control financiero o la gestión de la calidad.
 - ✚ Es un activo vital para la continuidad y desarrollo de una empresa.
 - ✚ Garantía de la confidencialidad, integridad y disponibilidad de la información.
 - ✚ Evaluar, cuantificar y minimizar los riesgos ante incidentes.
 - ✚ Obtener criterios para la toma de decisiones.

- ✚ ¿Cómo ha afectado este cambio en el día a día?
 - ✚ Definir y mejorar los procesos (hemos puesto “calidad” a la seguridad)
 - ✚ Recopilar información (aportamos seguridad, confianza e imagen, mejoras en las relaciones con terceras partes).
 - ✚ Mantener un inventario de activos.
 - ✚ Facilitar la integración de nuevo personal a la empresa.

✚ ¿Qué beneficios estamos obteniendo?

- ✚ Disponer de planes de contingencia ante incidentes.
- ✚ Mejoras en el control de las personas.
- ✚ Estrategia de seguridad basada en el negocio y no en la tecnología, se basa en las personas.
- ✚ AYUDA a mejorar procesos, la seguridad es una actividad de la gestión.
- ✚ Reducir los riesgos a niveles aceptables.
- ✚ Diferenciarnos de la competencia (Para ser sinceros).

- ✚ ¿Qué problemas estamos teniendo y hemos tenido?
 - ✚ Necesidad de nuevas herramientas informáticas
 - ✚ Requiere un esfuerzo continuo



Muchas gracias
por su atención.



angelmari@redisoft.es

