1 – COMPREENDER LA ESTRUTURA BASICA DE LA EMPRESA, para analizar que departamentos/actividades pueden ser certificadas por las normas ISO 72001/2

<u>DETERMINAR ACTIVOS PARA DETERMINAR ALCANCE DE LA SGSI</u>

Área FORMACION

A -Tiene un departamento independiente de gestión de Alumnos? Si____ No____

B - Tiene un departamento independiente de gestión de Docentes? Si____ No____

Área GESTION

C - Tienes un departamento independiente de Administración y Contabilidad? Si____ No____

C.1 – Preguntas específicas sobre este departamento en el apartado 2.

D - Tienes un departamento independiente para Proveedores? Si____ No____

E - Tienes un departamento independiente de Recursos humanos? Si____ No____

F - Tienes un departamento independiente para Armaren y materiales - Economato (tanto para alumnos como para la propia empresa? Si____ No____

Área COMUNICACION

G - Tienes un departamento independiente de Marketing, publicidad y divulgación? Si____ No____

H - Que otros departamentos independiente existen en la empresa? _____

I - Y cuales están juntos? _____

(*Por independientes* se considera que tienen estructura independiente, bases de datos independientes y procedimientos independientes, aunque sea el mismo responsable o ejecutor).

Hacer un pequeño diseño con la estructura de la empresa un rectángulo por cada departamento, dentro del rectángulo toda la actividad del departamento, y unas líneas a conectar cada uno que está conectado por trabajo (ejecución) , no por personas.

2 – CONOCER LOS DETALES BASICOS SOBRE CADA DEPARTAMENTO, REFERENTES A INFORMATICA Y SEGURIDAD DE LA INFORMACION

Una hoja por cada departamento. ***Cuestionario individual***

- Hay un responsable por este departamento_____
- Tiene bases de datos informática y en que formato? _____
- Que otros departamentos necesitan consultarlas _____
- Y cuales pueden modificarlas?_____
- Hay una red informática en este departamento?_____
- Es una red exclusiva del departamento?_____
- Tienes una cuenta de email individual para este departamento?_____
- El email tiene dominio proprio?_____

- Que otros departamentos necesitan acceder a misma cuenta de email?_____
- Como se transpone la documentación escrita a digital, que herramientas y almacenamiento?
- Hay ordenadores individuales para este departamento?
- Hay personas especificas para este departamento?
- Se existen, defina las limitaciones de recurso por utilizador para la red_____
- Cada utilizador tiene una llave única, con limitaciones en la red? _____
-

Especificas solo para determinados departamentos

- Como se hace la comunicación informática con el exterior _____
- ***A1, B1, C1, E1*** - Se hay, cuáles son los protocolos con el SEPE _____
- ***C1*** - Se hay, cuáles son los protocolos con otras entidades públicas? _____
- ***A1, B1, C1 -*** Como se envía esta documentación a entidades externas, como el SEPE?
- **C.1** – Hay alguna interacción informática con los bancos? _____
  (*Ejemplo:* Usar aplicaciones de transacciones por el sistema informático interno, enviar emails con órdenes al banco, etc…)

3 – ANALIZAR LAS REDES Y SISTEMAS INFORMATICOS INTERNOS

- Hay un responsable por las redes por cable y wi-fi
- Cuantas redes por cable independientes tenéis
- Cuantas redes de wi-fi independiente tenéis
- Hacer un pequeño dibujo de lo que es la red (desde la entrada de señal hasta cada ordenar
- Hacer un listado del material informático que se utiliza
- Routes , firewall, switch ordenadores, impresoras, bluetooth, cámaras, proyectores…
- Otros datos no referidos arriba

4 – ANALIZAR LAS REDES Y SISTEMAS INFORMATICOS EXTERNOS – SITE – OTROS DATOS DISPONIBLES

- Se puede acceder a la red desde el exterior?_____
- Se sin, existe alguna VPN activa o otra tipo de conexión cifrada y segura? _____
- Tiene un administrador para esas áreas? _____
- Que departamentos tienen área activa externamente _____

- La empresa tiene un SITE público? _____
- Tiene un administrador para esas áreas? _____
- El alojamiento es local en servidor proprio o externo?
- Hay interconexión entre el SITE y la red informática interna en general? _____
- Hay conexión entre los datos de cada departamento y el exterior, BBDD, otra información?
- Existen protocolos HTTPS para acceder al SITE
- Hay un responsable por el mantenimiento, gestión y supervisión del SITE
- Que departamentos generan información para el SITE
- Hay un encargado de revisar la información disponibilizada en el SITE
  (Se no sabe lo que significa, entiende o no sabe contestar alguna pregunta o sigla, por favor entre en contacto conmigo - nicsergio@gmail.com)

5 - SABER COMO SON LAS SALAS DE AULAS Y SUS PROTOCOLOS Y PROCEDIMENTOS

- Hay un responsable por las salas de clases?
- Tiene algún protocolo de ejecución general?
- Tiene algún protocolo de ejecución individual por ordenador
- Hay algún protocolo de ejecución cada vez que termina un curso
- Hay una definición de plaza (ordenador definido) en las aulas por cada alumno
- (el objetivo es saber cuántos alumnos aceden a cada ordenador, se es o no posible saber)
- Software necesarios en cada ordenador del aula y licencias existentes
- Software específicos de protección de red y datos
- Como se hace el acceso de cada alumno a cada ordenador
- El profesor tiene un ordenar en la aula de la empresa?
- Que software tiene instalados, licencias y de protección de redes
- Como se hace el acceso a eses ordenadores por parte de cada profesor
- Otros datos no referidos arriba

Establecer y Gestionar el SGSI
Establecer el SGSI
Definir el alcance y los límites del SGSI
Definir una política de SGSI
Definir el enfoque de la evaluación de Riesgos
Identificar los riesgos
Analizar y evaluar los riesgos
Identificar y evaluar opciones para el tratamiento de riesgos
Seleccionar objetivos de control y controles para el tratamientos de riesgos
Obtener la aprobación por parte de la dirección de los riesgos residuales propuestos
Obtener la autorización de la Dirección para implementar y operar el SGSI
Preparar una Declaración de aplicabilidad
Implementar el SGSI
Elaborar un plan de tratamiento de riesgos
Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados
Implementar los controles seleccionados en 4.2.1g para llegar a los objetivos de control
Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo estas mediciones van a ser utilizadas para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3c)
Implementar programas de formación y concienciación (ver 5.2.2)
Gestionar la operación del SGSI
Gestionar los recursos para el SGSI (ver 5.2)
Implementar procedimientos y otros controles capaces de permitir una rápida detección de eventos de seguridad y respuesta a incidentes de seguridad (ver 4.2.3[a])