# PREGUNTAS A LA ACADEMIA CALDERÓN PARA CERTIFICARSE ISO 27001 y 27002

1. ¿Qué áreas se van a certificar? ¿sólo para cursos de formación? ¿también para cursos de conducir?
2. ¿Estarían dispuestos a facilitar los procedimientos que se aplican actualmente?
3. ¿Dispone de un inventario de los dispositivos conectados a la red?
   * 1. Es necesario documentarlo
4. En lo que respecta a la red necesitamos aclaraciones sobre los siguientes puntos:
   1. Hay un responsable por las redes por cable y wi-fi
   2. Cuantas redes por cable independientes tenéis
   3. Cuantas redes de wi-fi independiente tenéis
   4. Hacer un pequeño dibujo de lo que es la red (desde la entrada de señal hasta cada ordenar
   5. Hacer un listado del material informático que se utiliza
   6. Routes , firewall, switch ordenadores, impresoras, bluetooth, cámaras, proyectores…
   7. Otros datos no referidos arriba
5. ¿Qué información almacenan en la academia , y por cuanto tiempo se guarda?
6. ¿Qué medios físicos de almacenamiento/ o lógicos se usan?
7. ¿Como se gestionan los flujos de información en los diferentes procesos?
8. Necesitamos el organigrama de la empresa por departamento, empleados y sus funciones:
   * 1. Es necesario documentar los perfiles.
9. Procedimientos donde haya información involucrada:
   * 1. Contratación de cursos con la administración
     2. Definición de cursos
     3. Selección y asignación de alumnos a cursos
     4. Procedimiento de alta de alumnos, asignación de equipos y acceso al aula virtual
        + 1. ¿Qué perfil se encarga de asignar a cada sujeto de la formación el acceso al aula virtual, se le facilita Usuario/contraseña para acceder al sistema?
          2. ¿Tendría cada alumno la posibilidad de cambiar la contraseña asociada al usuario dado?
          3. ¿Cuál es la política para eliminar de datos de los alumnos al terminar cursos?
     5. Procedimiento para hacer backup de informacion sensible

¿Tienen alguna forma de backup?

* + - * 1. ¿en dispositivos de almacenamiento externo? ¿en la nube?
        2. ¿se almacenan físicamente en otra ubicación geográfica?
        3. ¿cada cuánto tiempo se hace el backup? ¿es incremental?

¿siguen algún método para recuperar información en caso de pérdida?

¿qué método se aplica para crear el backup?

* + 1. Procedimientos de interacción con la administración:
       - 1. ¿El SEPE accede de alguna manera a los datos de la academia o es la academia la que envía los datos al SEPE? ¿existen certificados electrónicos asociados a la empres, específicos para el envío seguro de documentos? ¿hay un responsable de envío de datos firmados digitalmente o son varias las personas que lo pueden hacer¿, si son varias ¿cada una tiene su propio certificado o se usa uno común de la empresa?
    2. ¿Hay otros en los que te quieras certificar?

1. Seguridad en los equipos:
   * 1. ¿Tienen controles de acceso a determinadas páginas desde los equipos en clase?
     2. ¿Qué software de seguridad se utiliza para la protección de los equipos?
     3. ¿Con qué frecuencia se hace mantenimiento tanto de los equipos de los empleados como de los alumnos?
2. Seguridad de red:
   * 1. ¿Con qué frecuencia se modifican las claves de acceso a redes?
     2. ¿Se monitorean las redes de la empresa?, ¿con qué frecuencia?¿Se registra y guarda la informacion de los equipos que se conectan a la red?
3. ¿Existe un sistema de seguridad física en los centros donde se almacenan datos sensibles?(alarmas , cámaras, .……)
4. Otras cuestiones que van saliendo para preguntar a la Autoescuela Calderón:
5. ¿El personal de la academia tiene posibilidad de teletrabajar? ¿disponen de equipos portátiles proporcionados por la empresa? ¿existen VPN para conexión desde casa?
   * 1. Destrucción/reciclado de equipos informáticos obsoletos (ordenadores, discos duros, tarjetas de memoria, pen-drive, impresoras...).
6. Destrucción/reciclado de documentación impresa y soportes digitales (CD, DVD).
   * 1. En la adquisición de equipos de segunda mano/nuevos ¿hay un método de maquetación - instalación de software, antivirus, configuración de seguridad? ¿hay renting de equipos?, en caso afirmativo ¿se formatean a bajo nivel con el proceso necesario antes de devolver los equipos?

# DETERMINAR ACTIVOS PARA DETERMINAR ALCANCE DE LA SGSI

## 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.

# *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?

* + Existen perfiles con diferentes permisos de cara al acceso a la red y a recursos compartidos?

-

# *ANALISIS DE LAS REDES Y SISTEMAS INFORMATICOS EXTERNOS – SITE – OTROS DATOS DISPONIBLES*

* + Se puede acceder a la red desde el exterior?
  + En caso afirmativo ,¿ 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)

# *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