JESUÏTES El Clot
Escola del Clot

M011-SEGURIDAD INFORMÁTICA Y ALTA SEGURIDAD

UF1- Seguridad Física, lógica y legislación

ACTIVIDAD 5

Curs: 2018-19

CFGS: ASIX2

Alumne : Arnau Subirós Puigarnau

Data : 17-11-2018

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

ACTIVIDAD 5 : Disponemos de una empresa que quiere cumplir con todos los requisitos de Seguridad Informática y queremos cumplimentar una justificación completa para pasar una evaluación de un organismo Certificador.

Justificar de cara a una inspección que nuestra instalación cumple correctamente en cada uno de los apartados que se indican en la tabla.

Generar un documento de trabajo completo, es decir textos + imágenes o esquemas complementarios que permitan justificar correctamente cada uno de los apartados enunciados en la tabla.
(Número de páginas mínimo 20.)

Factor de seguridad	Justificación
UBICACIÓN El edificio	Descripción detallada de la zona, urbana, industrial, rural etc.... tipo de edificio, detalles
Tratamiento acústico	Aislamiento previsto respecto al interior del edificio
Seguridad física del edificio	Sistemas biométricos,etc. aplicados al interior edificio Seguros ..... pas/act
Factores naturales	Seismos, inundaciones incendios, descuidos.....
Servicios e instalaciones cercanas	Afectación de vecindario, campos magn. ondas etc.
Seguridad del entorno	Sistemas biométricos, físicos activos y pasivos
Control de acceso	procedimientos de sistemas lógicos, pasivos y activos

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

ÍNDICE

1. Introducción
1.1. Auditoría de Seguridad de Sistemas de Información
1.1.1. Areas que abarca
1.1.2. Fases en la auditoría
1.1.2.1. Auditoría en la seguridad física
1.1.2.2. Auditoría en la seguridad lógica
2. Prefacio del informe
3. Informe de Seguridad Informática de Syptec S.A.
3.1. Ubicación de Syptec S.A.
3.1.1. Descripción del Centro de Trabajo
3.1.2. Características de las vías públicas que circundan al edificio
3.2. Tratamiento acústico
3.3. Seguridad física del edificio
3.3.1. Medidas de emergencia
3.3.1.1. ¿De qué consta un Plan de Emergencia?
3.3.1.2. Señalización
3.3.1.3. Sistemas y medidas contra incendios
3.3.1.4. Iluminación de emergencia
3.3.1.5. Locales y zonas de riesgo especial
3.3.2. Mantenimiento de las Instalaciones Generales de los Edificios
3.4. Factores Naturales
3.4.1. Incendios
3.4.1.1. Situación actual
3.4.2. Inundaciones
3.4.3. Descuidos
3.5. Servicios e instalaciones cercanas
3.5.1. Servicios e instalaciones cercanas
3.5.2. Radiaciones electromagnéticas
3.5.3. Señales radar
3.5.4. Instalación eléctrica
3.5.4.1. Picos y ruidos electromagnéticos
3.5.4.2. Cableado
4. Seguridad en el entorno
4.1. Alarmas de intrusión
4.2. Circuito cerrado de TV
4.3. Credenciales de identificación
4.3.1. Control de acceso(seguridad privada)
4.4. Sistemas biomçetricos de identificación
4.4.1. Control de acceso (C.P.D)
4.4.1.1. Ventajas de los Sistemas Huellas Dactilar
4.5. Seguridad física pasiva
4.5.1. SAI
4.5.2. Sistemas RAID
5. Control de acceso (procedimientos sistemas lógicos activos y pasivos)
5.1. Amenazas lógicas
5.1.1. Métodos de protección
5.1.1.1. Antivirus
5.1.1.2. Cortafuegos(firewall)
6. Conclusión

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

1. Introducción

1.1. Auditoría de Seguridad de Sistemas de Información

Consiste en un estudio que abarca la gestión y el análisis para identificar y corregir las vulnerabilidades que se pueden encontrar en las estaciones de trabajo, servidores o redes de ordenadores. También cabe destacar que se puede dividir en auditoría física y lógica. Obtenido el resultado, se detallan, archivan y reportan a sus responsables quienes tienen que tomar las medidas necesarias para establecer medidas preventivas de refuerzo. Gracias a esto sabremos la situación exacta de sus activos de información respecto a protección, medidas de seguridad y control.

1.1.1. Áreas que abarca

En esta auditoría se llegan a abarcar las siguientes áreas de seguridad, ya que forman parte de los objetivos de una revisión de la seguridad.

- Las amenazas físicas externas
- La protección de datos según está fijado en la LOPD (Ley Orgánica de Protección de Datos) de cuyo Reglamento de Desarrollo destacamos el artículo 96 que consiste en que: *"El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias."Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas"*

- Control de accesos adecuados físicos y lógicos
- Redes y comunicaciones: tipos de comunicaciones, protección de antivirus y las topologías.
- Desarrollo y uso de las políticas.
- Fundamentos de la seguridad: planes, políticas, funciones, etc.
- El desarrollo de aplicaciones en un entorno o lugar seguro.
- El control de producción

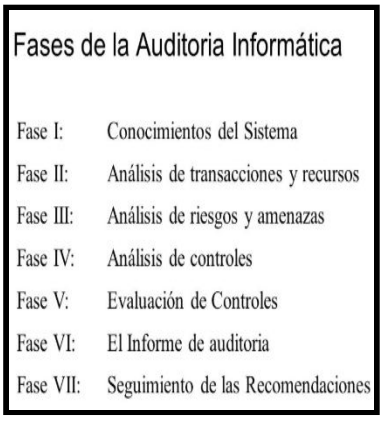
Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

1.1.2. Fases en la auditoría

Las fases que hay que hacer en este tipo de auditoría son las siguientes:

- Elección de objetivos así como su alcance y la profundidad de la auditoría.
- Recopilación de la información y el análisis de cualquier fuente que nos pueda servir.
- Uso de un plan de trabajo, además de los recursos y plazos necesarios para realizarlos.
- Aplicación de pruebas y de entrevistas.
- Análisis de resultados con su respectiva valoración de riesgos.
- Presentación y las discusiones respecto al informe provisional.
- Informe final.



1.1.2.1. Auditoría en la seguridad física

- Consistirá en la evaluación de las protecciones físicas de datos, equipos redes, programas instalaciones y soportes, además habrá que considerar a las personas, que estén protegidas y que haya medidas de evacuación, salidas alternativas, alarmas, etc.
- Las amenazas pueden ser desde: vandalismo, explosiones, inundaciones, sabotaje, averías importantes, incendios, así como los demás que pueden afectar al trabajador impidiendo su trabajo afectando al funcionamiento correcto de la entidad como pueden ser huelgas, errores o negligencias.

1.1.2.2. Auditoría en la seguridad lógica

- Habrá verificaciones para comprobar que cada usuario solo podrá acceder a los recursos los cuales autorice el propietario con las posibilidades que se hayan fijado, por ejemplo: lectura, borrado, modificación, ejecución, etc.
- Se usarán métodos de autenticación, los cuales pueden ser desde la biometría el cual es uno de los más sofisticados hasta el método más usado que es la contraseña.
- Las contraseñas cumplirán las normas y los estándares de la entidad. Algunos aspectos para evaluar en las contraseñas serán, una longitud mínima, un número de intentos para introducirla por el usuario, cambiarlas con el tiempo, etc.

Nom i Cognoms | **Data**

Arnau Subirós Puigarnau | 17-11-2018

2. Prefacio del informe

La empresa Syptec S.A le ha pedido a su técnico informático, el Sr. Anau Subirós que realice un informe la seguridad de la empresa ya que en breve hay una auditoría y tiene que convencer al auditor que nuestro sistema está bien protegido con el objetivo de obtener el certificado de seguridad (ISO/IEC 27002**:2013 i ISO/IEC 27004***)*

En dicho Informe constan de 7 puntos :

- **Ubicación**
  - descripción detallada de la zona (rural, urbana…)
  - tipo de edificios
  - detalles
- **Tratamiento acústico**
  - aislamiento previsto respecto al interior del edificio
- **Seguridad física del edificio**
  - sistemas biométricos aplicados al edificio
  - seguros..
- Factores naturales
  - seïsmos, inundaciones, incendios..
- Servicios e instalaciones cercanas
  - afectación del vecindario
  - campos magnéticos...
- Seguridad del entorno
  - sistemas biométricos físicos activos y pasivos
- Control de acceso
  - procedimientos de sistemas lógicos activos y pasivos

** **ISO/IEC -** Son estándares de seguridad publicados por la Comisión Electrotécnica Internacional (IEC) y la Organización Internacional para la Estandarización (ISO).*

*****ISO/IEC 27002** –Tecnología de la información, técnicas de seguridad y código para la práctica de la seguridad de la gestión de la información.*

*****ISO/IEC 27004** –Métricas para la gestión de seguridad de la información. Proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.*

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

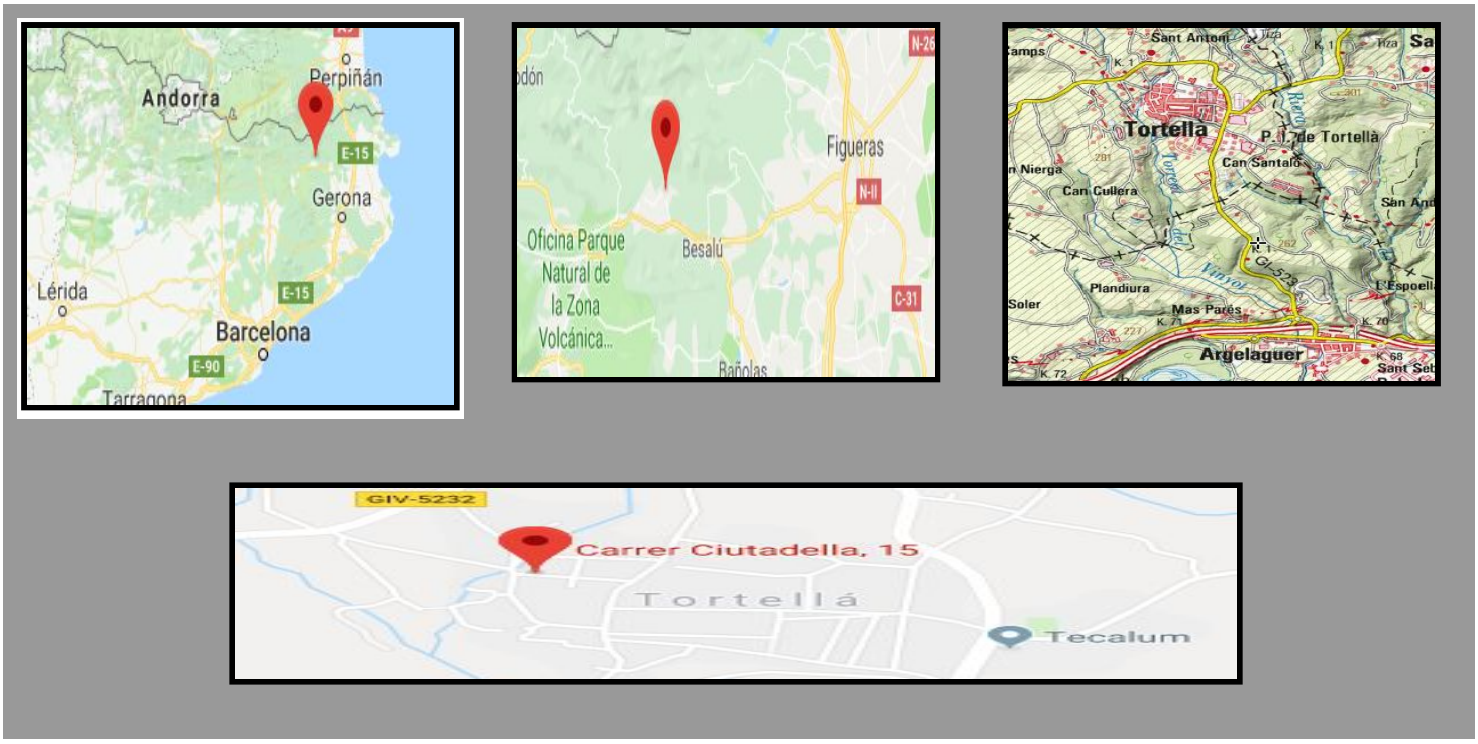
3. Informe de Seguridad Informática de Syptec S.A.

3.1. Ubicación de Syptec S.A

Syptec S.A. es una empresa de consultoría y tecnología informática fundada en Marzo del 2011. El conocimiento de nuestros técnicos abarca las principales entornos tecnológicos utilizados en el mercado: Bases de datos (DB2, Oracle, SQL Server, MySQL), Lenguajes de Programación (J2EE , JAVA, COBOL , NATURAL, .NET), Aplicaciones de gestión empresarial (SAP, BI...).

Ésta ubicada en Tortellà un pueblo de la comarca La Garrotxa, província de Girona.

Dirección : c/Ciutadella 15
Código Postal : 27853
Teléfono : 972-88-55-44
Número de trabajadores: 50
Horario: De Lunes a Viernes de 09h a 14h y de 16 a 19h



Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.1.1. Descripción del Centro de Trabajo

Zona de ubicación: Está ubicado a la salida del pueblo de Tortellà.
No de edificios del centro: 1
No de fachadas al exterior: :2
Dimensiones: 300 m2
Actividades en el edificio: Empresa de consultoría y tecnología informática
N° de personas que ocupan habitualmente el centro de trabajo: 30
Días laborales: trabajadores repartidos
● Turno de mañana
● Turno tarde
No residentes: 20
No trabajadores en total: 50
Cerramientos: piedra
Carpintería: aluminio anodizado
● El aluminio es práctico, cómodo y no requiere ningún tipo de mantenimiento. Es un material resistente que permite cerramientos herméticos y aislamiento acústico. El aluminio es de fácil instalación en todo tipo de construcciones ya sean nuevas o antiguas
Estructura: pilares de hormigón armado
Cubierta: Cubierta inclinada a 2 aguas (inclinación superior del 15%)
Suelo: (de la oficina) parquet
Salidas al exterior: 2
Instalaciones Técnicas existentes

1. Cuarto eléctrico: SI
2. Gas: SI
3. Aljibe de agua potable: SI
4. Fecales y pluviales: SI

3.1.2. Características de las vías públicas que circundan al edificio

Denominación de la vía/calle	Sentido de la circulación	Nivel de tránsito (alto/medio/bajo)	Tipo de estacionamiento
c/Ciutadella	doble sentido	bajo	doble fila
c/Freser	doble sentido	bajo	en línea
c/Olot	doble sentido	bajo	doble fila

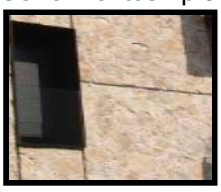
Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.2. Tratamiento acústico

Se ha contratado los servicios de la empresa Aislamientos AcustiK S.L (de la misma provincia de Girona) para que realizara un aislamiento térmico y acústico

- Cerramientos: piedra



- Carpintería: aluminio anodizado
  El aluminio es práctico, cómodo y no requiere ningún tipo de mantenimiento. Es un material resistente que permite cerramientos herméticos y aislamiento acústico. El aluminio es de fácil instalación en todo tipo de construcciones ya sean nuevas o antiguas
  (ver la imagen donde se observa el portal en aluminio anodizado de color cobre)

3.3. Seguridad física del edificio

3.3.1. Medidas de emergencia

Las medidas de Emergencia pretenden salvaguardar la integridad física de los ocupantes del centro de trabajo, tanto de la plantilla de la empresa como del personal ajeno de la misma, en el momento en que se produce una emergencia.

El establecimiento de las Medidas de Emergencia tienen como necesidad:

- ❏ Definir y clasificar las posibles situaciones de emergencia que se pueden dar en sus instalaciones.
- ❏ Conocer los medios de prevención y protección disponibles en el centro de trabajo.
- ❏ Fiabilidad y mantenimiento de todos los medios de protección y las instalaciones.
- ❏ Planificar la organización humana con los medios materiales existentes.
- ❏ Determinar la estructura jerárquica y funcional de las personas con una función específica asignada en la emergencia.
- ❏ Establecer las acciones a desarrollar para el control de la emergencia.
- ❏ Definir las misiones, normas de actuación y procedimientos de los diferentes equipos constituidos para actuar en caso de emergencia.
- ❏ Conocimiento por parte del personal de las medidas de seguridad adoptadas en las instalaciones y sus recorridos de evacuación.
- ❏ Acelerar y agilizar la actuación ante una emergencia desde el punto de vista de la comunicación misma, la intervención y la evacuación.
- ❏ Coordinarse con las distintas actividades empresariales que se encuentren en el mismo centro de trabajo.

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

- ❑ Avisar, informar y facilitar la intervención de los medios de ayuda exteriores.
- ❑ Conocimiento por parte del personal de las medidas de seguridad adoptadas en las instalaciones y sus recorridos de evacuación.

3.3.1.1. ¿De qué consta un Plan de Emergencia?

Un plan de Emergencia es un documento en el que deben estar descritos detalladamente los siguientes elementos:

- ❖ La organización para casos de emergencia:
  - ➢ Jefe de Emergencia
  - ➢ Jefe de 1ª Intervención
  - ➢ Equipo de 1ª Intervención
  - ➢ Equipo de 2ª Intervención
- ❖ El sistema de aviso de emergencia
- ❖ Plan de Evacuación
  - ➢ Equipo de Evacuación
  - ➢ Vías de Evacuación
  - ➢ Zonas de concentración del personal
  - ➢ Planos de situación
- ❖ Listado de teléfonos de emergencia

3.3.1.2. Señalización

Todos los sistemas de protección contra incendios, así como los sistemas de alarma y las vías y salidas de evacuación deberán estar señalizados.

Las vías que conduzcan a zonas o recintos sin salida deberán estar igualmente señalizadas con la señal "SIN SALIDA". Se realizarán ejercicios y simulacros periódicos con objeto de evaluar la eficacia de la señalización del edificio.

- Las salidas de emergencia del edificio deberán estar señaladas correctamente.

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.3.1.3. Sistemas y medidas contra incendios

Se deberá conocer los factores de resistencia y de estabilidad al fuego de paredes, parámetros, puertas,..., etc., con la finalidad de constatar cuáles son los sectores de incendio del edificio.

- Los extintores deberán estar colocados a una altura máxima de 170 cm.
- La colocación y ubicación de dichos sistemas de extinción no deberá suponer un riesgo añadido de golpes, lesiones, caídas, desprendimiento,..., etc.
- El acceso a los sistemas de protección contra incendios deberá estar garantizado en todo momento. No se ocultaran detrás de elementos estructurales o decorativos.

3.3.1.4. Iluminación de emergencia

La iluminación de emergencia deberá estar mantenida en todo el edificio. Se deberá instalar iluminación de emergencia en todas las escaleras En cada planta, se deberá instalar una lámpara de emergencia marcando el sentido de salida, en el marco de la puerta que comunica con las escaleras.

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.3.1.5. Locales y zonas de riesgo especial

Se deberán señalizar las puertas y los accesos a los recintos donde se encuentren instalaciones singulares tales como, cuadros eléctricos, aljibes, bombas de agua,...Igualmente en dichas instalaciones se colocarán las señales de peligro y de prohibición propias de los posibles riesgos, como por ejemplo,"PELIGRO DE INCENDIO","RIESGO ELÉCTRICO"...etc.

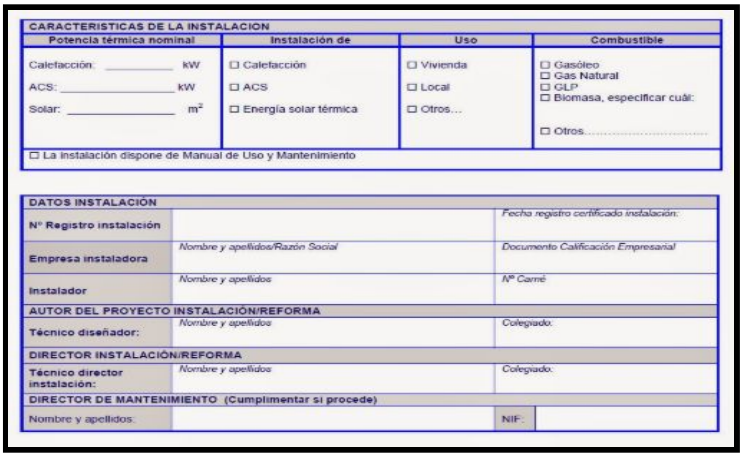
3.3.2. Mantenimiento de las Instalaciones Generales en los Edificios.

Según lo estipulado en la Reglamentación específica para cada una de las instalaciones generales:

a) Los aparatos, equipos, sistemas y componentes de las instalaciones generales de los edificios, se someterán a operaciones de revisión después de un incendio y , con la frecuencia que establezca la legislación vigente para los diversos tipos de instalaciones, el fabricante, suministrador o instalador, o e su defecto con frecuencia mínima anual.

b) Las actas de las revisiones que deben ser realizadas por empresas autorizadas y registradas por el órgano competente de la Administración, en las que debe figurar el nombre, sello y número de registro correspondiente así como la firma del técnico que ha procedido a las mismas, deben estar a disposición de los servicios competentes de inspección en materia de prevención de incendios, al menos durante cinco años a partir de la fecha de su expedición.

c) En cada tipo de instalación, se deben sustituir o reparar los componentes averiados cada vez que se detecten.



CARACTERISTICAS DE LA INSTALACION			
Potencia térmica nominal	Instalación de	Uso	Combustible
Calefacción: ____ kW ACS: ____ kW Solar: ____ m²	☐ Calefacción ☐ ACS ☐ Energía solar térmica	☐ Vivienda ☐ Local ☐ Otros...	☐ Gasóleo ☐ Gas Natural ☐ GLP ☐ Biomasa, especificar cuál: ☐ Otros.....
☐ La instalación dispone de Manual de Uso y Mantenimiento			

DATOS INSTALACIÓN		
Nº Registro instalación		Fecha registro certificado instalación:
Empresa instaladora	Nombre y apellidos/Razón Social	Documento Calificación Empresarial
Instalador	Nombre y apellidos	Nº Carné
AUTOR DEL PROYECTO INSTALACIÓN/REFORMA		
Técnico diseñador:	Nombre y apellidos	Colegiado:
DIRECTOR INSTALACIÓN/REFORMA		
Técnico director instalación:	Nombre y apellidos	Colegiado:
DIRECTOR DE MANTENIMIENTO (Cumplimentar si procede)		
Nombre y apellidos:		NIF:

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.4. Factores Naturales

A continuación vamos a detallar los posibles factores naturales que le podrían afectar a dicha empresa

3.4.1. Incendio

- ➔ Grado de negatividad: Muy Severo
- ➔ Frecuencia de evento: Aleatorio
- ➔ Grado de impacto: Alto

3.4.1.1. Situación actual

- La oficina donde están ubicados los servidores cuenta con un extintor cargado, ubicado muy cerca a esta oficina. De igual forma todos los pisos de la institución cuenta con un extintor debidamente cargados.
- Se ejecutó un programa de capacitación sobre el uso de elementos de seguridad y primeros auxilios, a todo el personal perteneciente a la brigada de emergencia. Lo que es eficaz para enfrentar un incendio y sus efectos.
- Realiza una copia de seguridad diariamente al servidor de Backup y además realizar Backup del servidor mensual, almacenando en donde lo dispongan (CDROM, disco duro, base de datos u otros medios de almacenamientos).

- Analizando el riesgo de incendio, es necesario almacenar los Backup en lugares donde la acción calorífica de un incendio no alcance los dispositivos de almacenamiento. Por ende, se colocarán en lugares estratégicamente distantes y cercanos a los extintores, para en caso de emergencia sea más fácil controlar el fuego y proteger los dispositivos de almacenamiento

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.4.2. Inundaciones

- ➔ Grado de negatividad: Medio
- ➔ Frecuencia de evento: Aleatorio
- ➔ Grado de impacto: Medio

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

- Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.
- Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

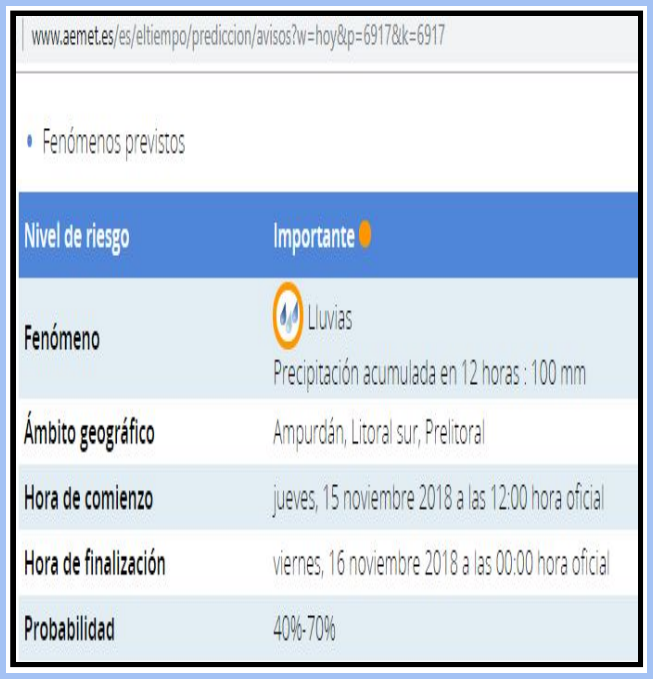
La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

En esta empresa tiene folletos divulgativos del Plan Inuncat (Pla de Emergencia para las Inundaciones a Catalunya sobre las inundaciones con la colaboración de Protecció Civil)

Nom i Cognoms	Data
Arnau Subirós Puigarnau	17-11-2018

Syptec S.A. debido a su situación geográfica está pendiente de las notificaciones de **AEMET** (Agencia Estatal de Meteorología y el **METEOCAT** (Servicio Meteorológico de Catalunya)

Avisos de AEMET



Avisos del METEOCAT

3.4.3. Descuidos

A menudo se descuida la seguridad sobre el acceso, pero hay que tener en cuenta que cuando existe acceso físico a un recurso ya no existe seguridad alguna sobre el mismo, con el consiguiente riesgo.

- Un error típico de seguridad por acceso físico es el de tomas de conexión a la red informática no controladas, de acceso libre: un atacante con los suficientes conocimientos técnicos puede causar graves daños.

Por ello, en dicha empresa todos los accesos a la red están autenticados con tu usuario y clave de mediante wifi , bien mediante los ordenadores de uso público (que requieren también identificación previa).

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

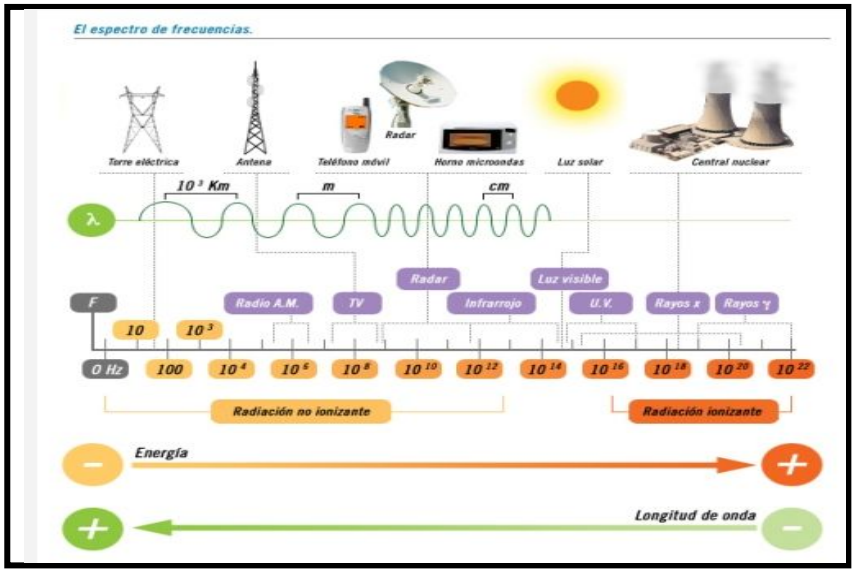
3.5. Servicios e Instalaciones cercanas

3.5.1. Radiaciones electromagnéticas

La evolución tecnológica y la necesidad de sistemas de telecomunicación para la interconexión de dispositivos ha producido un cambio social y empresarial de una magnitud difícilmente imaginable años atrás. Tanto es así que actualmente resulta común en las conversaciones hablar de Wifi,Bluetooth, 3G, 4G como algo habitual entre la población, desde los más jóvenes hasta incluso las personas mayores.
El avance tecnológico ha necesitado de un incremento generalizado de elementos radiantes para intercomunicarse y dar lugar a un conjunto de aplicaciones y sistemas inteligentes orientados principalmente a facilitar nuestra vida. No obstante, esta necesidad de comunicación nos ha llevado a vivir constantemente en un entorno lleno de radiaciones que alteran nuestro medio de vida natural.

- Cualquier aparato eléctrico emite radiaciones y que dichas radiaciones se pueden capturar y reproducir si se dispone del equipamiento adecuado.

- Los fallos del suministro eléctricos y las radiaciones electromagnéticas pueden alterar el funcionamiento de los equipos y los datos almacenados de forma magnética



Nom i Cognoms **Data**

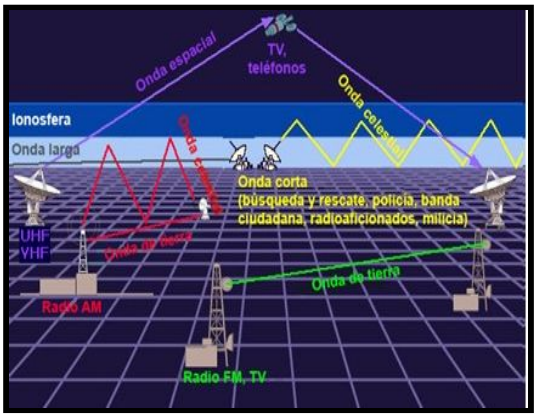
Arnau Subirós Puigarnau 17-11-2018

3.5.2. Señales Radar

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiada desde hace varios años.

- Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor.
- Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana





3.5.3. Instalación eléctrica

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

- En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.



Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.5.3.1. Picos y ruidos electromagnéticos

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

- **Syptec S.A**. dispone Supresor de picos de tensión y ruido **(Tripp-Lite ISOTEL4ULTRA) p**ara prevenir las caídas del sistema, reinicios y problemas comunes de rendimiento como cuando se encienden y apagan periféricos ruidosos. La supresión de sobretensiones con capacidad nominal de 3330 joules/92,000 amperes ofrece protección de grado de red

3.5.3.2. Cableado

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

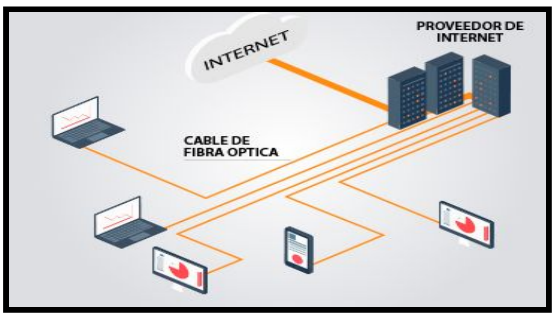
Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

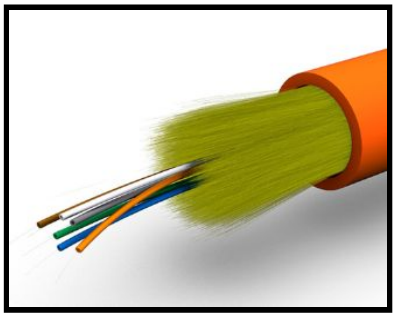
- **Interferencia**: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
- **Corte del cable:** la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- **Daños en el cable**: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

Nom i Cognoms	Data
Arnau Subirós Puigarnau	17-11-2018

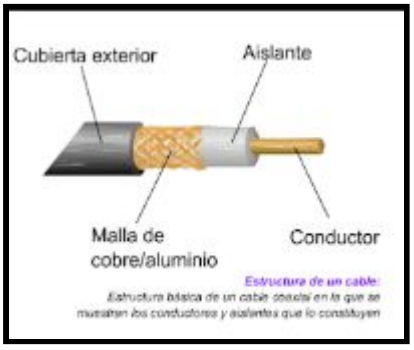
En Syptec S.A. utiliza cables de fibra óptica para las redes WAN i cables s coaxiales para redes LAN

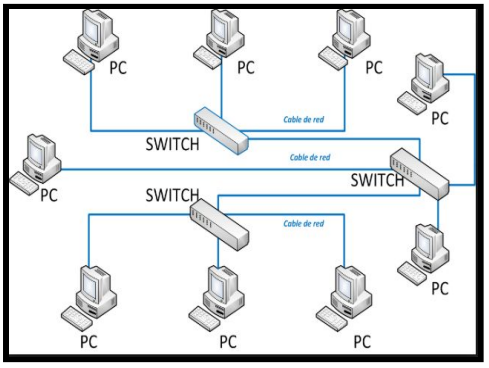
Utiliza fibra óptica para conectarse a Internet ya que esta tecnología no sufre interferencias ocasionadas por los cambios de tensión, temperatura, u otros cables, ni pérdidas en función de la distancia a la central, como ocurre con el ADSL.





Y en la red LAN mediante switch se usará el conector BNC (cable coaxial)





Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.6. Seguridad en el entorno

3.6.1. Alarma contra intrusión

Esta empresa dispone de un un sistema de alarma VISONIC Powermaster 30 G2 conectado con una C.R.A (Central Receptora de Alarmas)

Caracterísitcas :

- Central PowerMaster 30 PG2 PowerG con módulo GPRS GSM350

- 6 detectores PIR con cámara inalámbrica NextCAM PG2

- 2 detector cto. magnético

Nom i Cognoms	**Data**
Arnau Subirós Puigarnau	17-11-2018

- 2 detector rotura de cristal

- 1 detector de humo

- mando para el control remoto

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.6.2. Circuito Cerrado TV

Syptec S.A. dispone de un circuito cerrado de TV utilizando el videograbador Center SV

Características:

- Software de administración remota para PC
- Gestión y configuración de sitios remotos
- Visualización en vivo
- Reproducción y búsqueda
- Alarmas, eventos, informes
- Audio bidireccional

- 4 Domo Spectra IV SL día/noche, 1/4, 540 TVL, zoom óptico x23, interior, montaje empotrado, cúpula clara, 24V

3.6.3. Credenciales de identificación

El uso de credenciales implica que la persona se identifica por algo que posee en este caso la tarjeta de identificación con un PIN único

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.6.3.1. Control de acceso (seguridad privada)

- El Servicio de Vigilancia es el encargado del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.
- A cualquier personal ajeno a la planta se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, etc.
- El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa

Syptec tiene contrato los servicios de vigilancia con la Pycseca Seguridad S.A.

3.6.4. Sistemas biométricos de identificación

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es(manos, ojos, huellas digitales y voz.

3.6.4.1. Control de acceso (C.P.D.)

En Syptec utilitza sistemas biométricos de identificación (huella dactilar) para poder acceder a los CPD (Centro de Procesamiento de Datos)

En este lugar donde se centralizan servicios de datos, servicios de e-mail, de usuario, etc..donde hay los servidores con varios procesadores, unidades de disco, sistemas de comunicaciones avanzadas (varios routers, switchs), equipos de alimentación redundantes, dispositivos de copia de seguridad, etc.. es necesario y prioritario un nivel de acceso restringido.

3.6.4.1.1. Ventajas de los sistemas Huella Dactilar

- ❏ Imposible suplantación de Identidad: Lo que impide que unos empleados puedan realizar marcajes a otros empleados.
- ❏ No precisa de ningún soporte: El no necesitar de tarjeta repercute en un menor coste de implantación, a la vez que nos evita tener que reponer tarjetas que se han deteriorado o perdido.

- Olvidos de Tarjeta: En los sistemas de tarjeta es muy habitual que un trabajador olvide la tarjeta, esta circunstancia no podría pasar con los sistemas de huella dactilar.
- Imagen de Modernidad: Un terminal de huella dactilar da imagen de modernidad y de estar a la última en las nuevas tecnologías a las empresas que implantan este sistema en un sitio visible a los visitantes

3.6.5. Seguridad física pasiva

3.6.5.1. SAI

Una vez que la corriente se pierde las baterías del SAI se ponen en funcionamiento proporcionando la corriente necesaria para el correcto funcionamiento.

Syptec utiliza RIELLO UPS Multi Sentry MSN 15

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.6.5.2. Sistemas redundantes (RAID):

Syptec utiliza un servidores NAS que tiene incorporado controladora RAID (utilizamos RAID de hardware) y tiene compatibilidad con RAID 0, 1, 5, 6, 10 e intercambio directo (hot plug) de unidades de disco duro

3.7. Control de acceso (procedimiento de sistemas lógicos activos y pasivos)

La seguridad lógica aplica mecanismos y barreras que mantengan a salvo la información a nuestra empresa desde su propio medio. Utilizando :

- Se limita el acceso a determinados aplicaciones, programas o archivos mediante claves o a través de la criptografía.
- Se otorgan los privilegios mínimos a los usuarios del sistema informático. Es decir, sólo se conceden los privilegios que el personal necesita para desempeñar su actividad.
- Cerciorarse de los archivos, las aplicaciones y programas que se utilizan en la compañía se adaptan a las necesidades y se usan de manera adecuada por los empleados.
- Controlar que la información que entra o sale de la empresa es íntegra y sólo esta disponible para los usuarios autorizados.

Nom i Cognoms **Data**

Arnau Subirós Puigarnau 17-11-2018

3.7.1. Amenazas lógicas

Para evitar posibles amenazas lógicas en nuestra organización, es importante que todos los empleados, especialmente los administradores de los equipos, tomen conciencia del cuidado que deben poner para que no se materialicen posibles daños en la compañía

- Es fundamental implementar mecanismos de prevención, detección y recuperación ante posibles amenazas lógicas como virus, gusanos, bombas lógicas y otros códigos maliciosos

- La expansión de la cultura de la seguridad entre los empleados puede ahorrar muchos disgustos a la entidad, muchas veces implementando medidas tan sencillas como, por ejemplo:
    - No ejecutar programas de los que se desconozcan su procedencia.
    - No utilizar programas no autorizados por la dirección.
    - No abrir correos personales desde los equipos de la compañía.
    - No visitar páginas web que no sean propósito de la empresa.
    - Instalar y actualizar habitualmente un software dedicado detectar y eliminar códigos maliciosos que puedan albergar los ordenadores.
    - Realizar chequeos de los correos electrónicos recibidos para comprobar que no suponen una amenaza para la entidad

---

**** **ISO/IEC 27002** recomienda que para protegerse de las amenazas lógicas, la empresa debe contar con dos o más programas (procedentes de diferentes vendedores) encargados de detectar y reparar códigos malicioso para mejorar las probabilidades de éxito ante un ataque. ****

3.7.1.1. Métodos de protección

Para proteger los ordenadores de posibles ataques, Syptec S.A. ha de implementado medidas de seguridad a su alcance , mostrando una actitud lo más alerta posible en cuanto a seguridad se refiere. Cualquier acto o acción que no esté explícitamente autorizada, no debería poder llevarse a cabo. Entre las medidas a poner en práctica, es vital el uso de un buen antivirus actualizado, contar con un firewall bien configurado, realizar copias de seguridad con frecuencia, hacer uso de técnicas de cifrado y auditorías, entre otras.

3.7.1.1.1. Antivirus

Los antivirus son herramientas encargadas de prevenir la infección de los ordenadores, además de detectar y eliminar virus y otras amenazas lógicas de los equipos informáticos.

Syptec S.A. utiliza ESET Secure Business que tiene las siguientes características:

★ Seguridad para el correo electrónico

- ★ Seguridad para endpoints: *Los endpoints son los equipos de escritorio, teléfonos inteligentes, impresoras, que forman parte de nuestra Red de Área Local (LAN)*
- ★ Seguridad para servidores de archivos
- ★ Seguridad para móviles

3.7.1.1.2. Cortafuegos (Firewall)

Un cortafuegos o firewall funciona de filtro entre redes facilitando las comunicaciones autorizadas y evitando los accesos ilícitos. Entre los objetivos de un cortafuegos se encuentra: evitar que usuarios de Internet accedan sin autorización a redes privadas conectadas a Internet y, permitir sólo el tráfico autorizado a través de políticas de seguridad preestablecidas

Syptec utiliza **Firewalls de hardware** que són más costosos que los cortafuegos de software y más complicados de utilizar. Estos cortafuegos normalmente están instalados en los routers que utilizamos

Se utiliza un **Firewall de Cisco (ASA5506-SEC-BUN-K9**)

3.7.1.1.3. Copias de seguridad

Las copias de seguridad se utilizan con el fin de recuperar la información del sistema en el caso de que se produzca la pérdida de la misma. La información se almacena en dispositivos de almacenamiento que se depositan en un lugar seguro. De esta manera, se consigue restaurar el sistema en el caso de que se produzca un fallo.

Los backups deben almacenarse en lugares seguros y lo más alejados posibles de la información respaldada. De nada sirve tener copias de seguridad actualizadas en un armario de las instalaciones donde se encuentra la información si un incendio puede destruir el edificio y acabar con ellas

Nom i Cognoms	Data
Arnau Subirós Puigarnau	17-11-2018

4. Conclusión

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro nuestra empresa .

Tener controlado el ambiente y acceso físico permite:

- ❏ Disminuir siniestros
- ❏ Trabajar mejor manteniendo la sensación de seguridad
- ❏ Descartar falsas hipótesis si se produjeran incidentes
- ❏ Tener los medios para luchar contra accidentes

Firma y sello (Técnico informático) **Fecha y lugar**

Fdo: D/Dª _____

syptec
SERVICIOS Y PRODUCTOS TECNOLÓGICOS