**Participantes:**

* **Alejandro Hernando**
* **Jorge Garriguez**
* **Marco Batista**
* **Raúl Leonel Cadena**
* **Saul Sáez**
* **Ivan Martín**

\* Reunir información acerca de qué sabéis sobre un plan de seguridad (sin mirar fuentes externas)

* Documento donde se recogen todos los posibles riesgos en una empresa y soluciones para los mismos
* La serie de normas que se ponen para detectar vulnerabilidades y solucionarlas.
* Plan para prevenir ataques informáticos y para en un futuro protegerte mejor de estos.
* Es un guión que siguen las empresas de seguridad para proteger a los clientes de los futuros problemas.

\* Recopilar información acerca de qué es un plan de seguridad (mirando fuentes externas)

**(Introducción, qué es un plan de seguridad)**

Un plan de seguridad informática te permite entender donde puedes tener vulnerabilidades en tus sistemas informáticos, para una vez detectadas, tomar las medidas necesarias para prevenir esos problemas. No necesitas que tu plan de seguridad informática sea un documento demasiado extenso que cubra cualquier tipo de seguridad imaginable. Debe ser capaz de ayudar a proteger los datos y los sistemas críticos de tu negocio, asegurándote además que se ajuste a la legislación vigente y a la Ley de Protección de Datos.

**¿Qué debemos proteger, de que protegerlo y cómo protegerlo?**

Para ello debemos saber que es la seguridad informática: conjunto de medidas encaminadas a proteger el hardware, software, información y personas.

1º¿Qué debemos proteger?

* Hardware
* Software
* Datos

2º¿De qué debemos protegerlo?

**3 tipos de amenazas:**

* Personas
  + Uno mismo: podemos compartir o mandar la información sin querer con otras personas
  + Los hackers: Estas personas entran sin permiso en un ordenador, para poder conseguir información de la persona a la que atacan.
  + Ransomware: un ciberdelincuente secuestra tu ordenador, es decir, lo bloquea y no puedes acceder a él a menos que pagues un “rescate”.
* Lógicas/fraudes
  + Virus
  + Gusanos
  + Troyanos
  + Keylogger
  + Spyware
  + Hijackers
  + Adware
  + Pharming
  + Spam y hoaxes
  + Cookies
  + Rogueware
* Físicas
  + Amenazas físicas:
    - Roturas
    - Incendios
    - Inundaciones
    - Cortes de corriente eléctrica
  + Soluciones:
    - Tener copias de seguridad
    - Sistemas de alimentación ininterrumpidos
    - Cuidar nuestro equipo

**3º¿Cómo podemos protegernos?**

* En la navegación web:
  + No lo descargues y ejecutes ficheros desde sitios sospechosos.
  + Analiza con un antivirus todo lo que descargues
  + Mantén actualizado tu navegador
  + Configura el nivel de seguridad de tu navegador
  + Instala un firewall
  + Descarga los programas desde los sitios oficiales

* Precauciones con el correo electrónico:
  + No abras ficheros adjuntos sospechosos o que no haya solicitado
  + Utiliza un filtro anti-spam
  + Analiza los anexos con un antivirus
  + Desactiva la lista previa de tu cliente de correo
  + No facilites tu cuenta de correo electrónico a desconocidos ni la publiques alegremente
  + No respondas a mensajes falsos ni a cadenas de correos
  + Borra el historial del destinatario cuando reenvíes mensajes a múltiples direcciones.
* Cuando utilices comercio electrónico:
  + La web empiece por HTTPS
  + Observa que aparece un candado en tu navegador
  + Asegurate de la validez de los certificados (pulsando en el candado) que coinciden con la entidad solicitada que sean vigentes o válidos
  + Evita el uso de equipos públicos para realizar transacciones comerciales
  + Cierra tu sesión cuando acabes
  + Instala alguna herramienta de antifraude para evitar acceder a páginas fraudulentas.

**Aun siguiendo las medidas anteriores:**

* Un antivirus nos protege de muchas de las amenazas anteriormente explicadas.
* Pero una protección muy eficaz es tener actualizado nuestro equipo ya que así tendrá menos vulnerabilidades
* También activado el firewall para evitar cualquier entrada de un amenaza a través de la red aunque muchos antivirus ya protegen de eso y no hace falta tenerlo activado pero tenerlo activado y actualizado es esencial para la protección de nuestro equipo.
* Otros métodos son la correcta utilización de nuestro ordenador y de la red así como el sentido común.

\* Comparación y análisis

La idea principal de que es un plan de seguridad si que sabíamos de que trataba, es decir, que consiste en buscar los distintos puntos debiles para así corregirlos de distintas futuras amenazas. También nos hemos dado cuenta de que no es tan sencillo hacer un plan de seguridad, ya que hay muchas amenazas de las que protegerse y que tampoco existe una seguridad al 100% frente a ellas, aunque si que se pueden evitar hasta cierto punto siguiendo los pasos mencionados anteriormente.