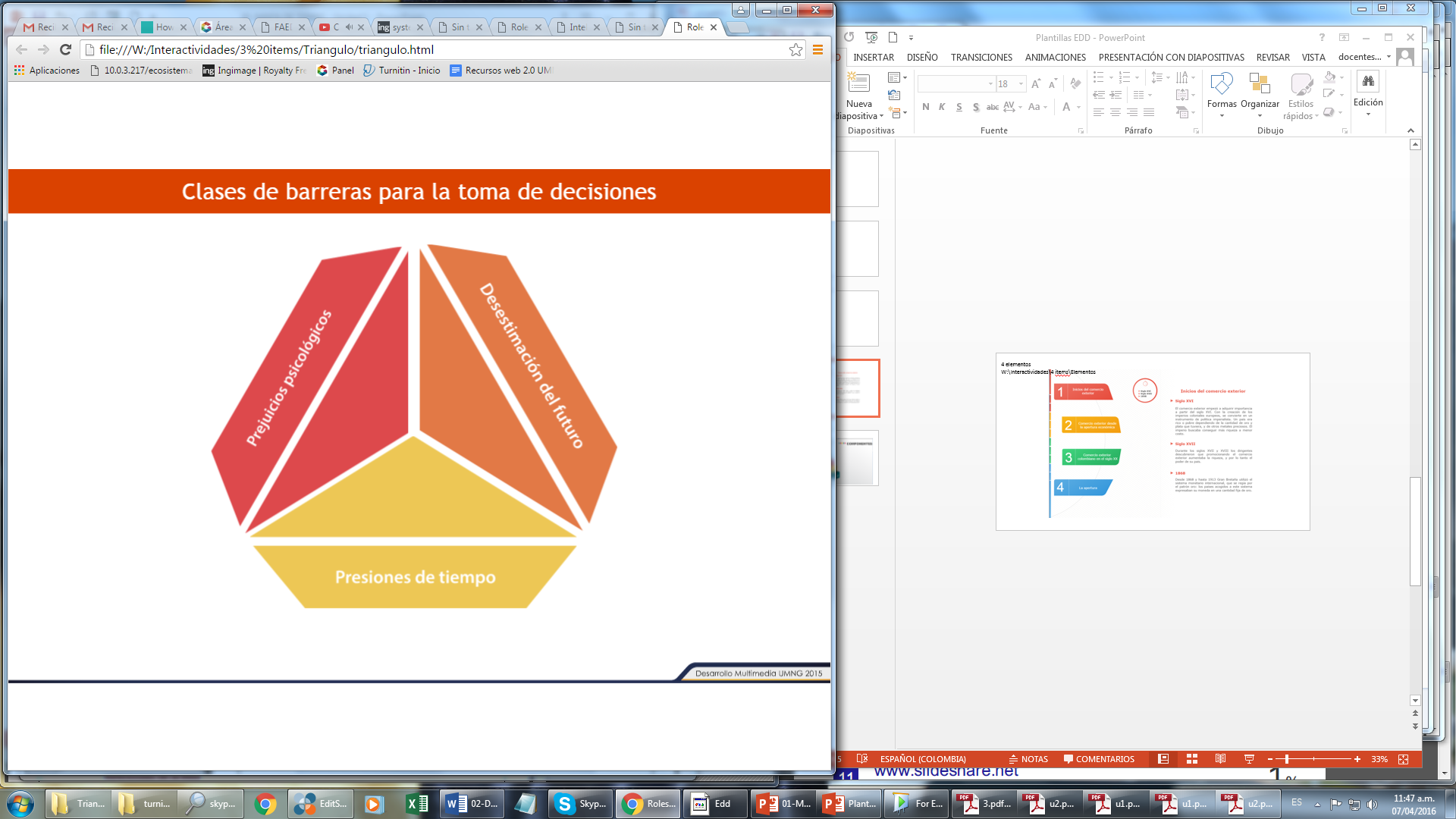


Mapa conceptual / Interactividad



|  |  |
| --- | --- |
| **INSTRUCCIÓN: Para conocer las recomendaciones contra el web hacking, haga clic en cada elemento de la interactividad.** | |
| **Contramedidas para evitar el web hacking** | |
| Inyección SQL | * Validar la entrada de los datos verificando el tamaño y tipo de los datos y filtrar la entrada de caracteres SQL. * No permitir que se vean los mensajes de error que devuelve el gestor de la base de datos, ya que estos muestran la consulta o parte de la consulta de SQL. * Programar las aplicaciones con todas las técnicas y metodologías de seguridad informática, determinándolas como la regla más importante.     ISS\_2834\_01239 |
| XSS | * Mantener el navegador web actualizado y tener habilitadas todas las medidas de seguridad. * Tener cuidado antes de dar clic en un enlace, puede contener código malicioso con XSS. * Descargar complementos para filtrar ataques XSS, aunque actualmente la mayoría de navegadores ya cuentan con esta condición. * Finalizar la sesión tan pronto termine de usar una página web, esto dificulta que los hackers roben las ‘cookies’. * Hacer un filtrado de los datos de entrada de los formularios y verificar que el tipo de datos y la longitud de cada campo sea igual al esperado. Se deberá filtrar caracteres especiales que puedan resultar peligrosos. * Escanear las aplicaciones en busca de código XSS. Existen varios escáneres de seguridad web especializados en encontrar código XSS, varios de ellos de código abierto.     03E08146 |
| Directorio o Path Traversal | * Instalar actualizaciones del software. * Usar de escáneres de vulnerabilidad. Algunas aplicaciones hacen escaneos sobre las cadenas introducidas buscando cadenas como ‘..’, ‘../’ o ‘..\’ * Escoger no trabajar con intervenciones del usuario al utilizar llamadas al sistema. * Filtrar y validar todas las entradas a través de aplicaciones web.   ISS\_10348\_01192 |