DATOS DE LA ACTIVIDAD							
No. de Actividad:	**1.7**	**Investigación**	**Malware, Virus, Troyano y Gusano. Prácticas de seguridad**				
Unidad:	Unidad: 1: Riesgos de seguridad informática en infraestructura de red						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**Seguridad en ITI**					Clave	**MPF3608DSO**
Profesor:	Andrés Figueroa Flores						
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	28/02/2021
Compet. Genéricas	4.1, 4.5, 5.2, 5.5			Competencia Profesional		CP1-1	

1. Objetivo(s) de la actividad

Identificar los diferentes tipos de programas malignos en el ámbito de seguridad informática.

2. Instrucciones (Descripción) de la actividad

1. Elaborar un esquema sencillo sobre los 12 dominios de seguridad, considerar el estándar ISO/IEC 27002 (pág. 16 PDF CISCO Security).

2. Elaborar una tabla comparativa de las características de los Virus, Troyanos y Gusanos. Debe ser con todas las características de cada malware, características puntuales de cada uno de ellos, ejemplo: Gusanos: historia breve, etapas de infección, como mitigar este malware etc.

3. Ingresar a la plataforma https://www.netacad.com/, al curso de Cybersecurity Essentials revisar los siguientes temas:

- 3.1.1 Tipos de malware
- 3.3.1 Tipos de ciberataques
- 2.5.1 El modelo de ciberseguridad de ISO

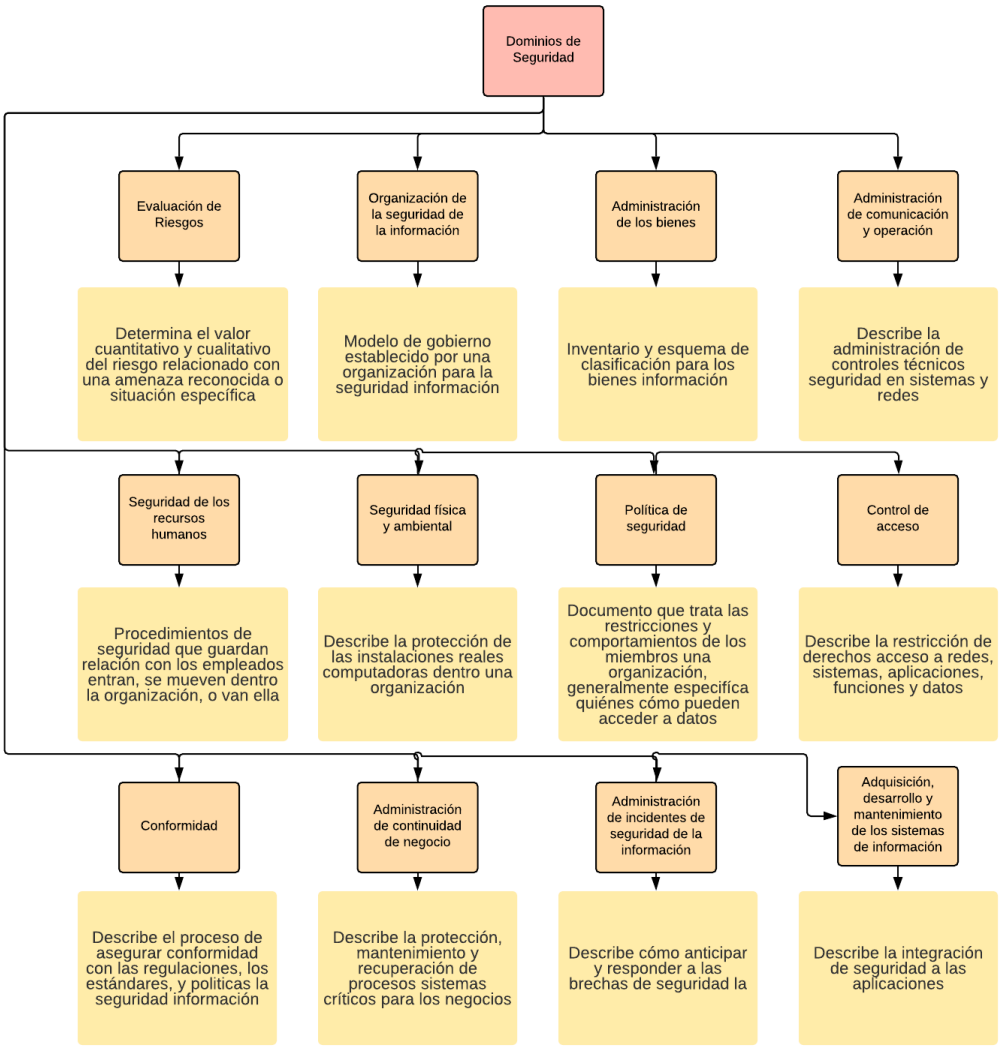
Contestar las siguientes actividades:

- 3.1.1.7 Actividad: identificar los tipos de códigos maliciosos
- 3.3.1.7 Actividad: identificar los ataques cibernéticos
- 2.5.1.5 Actividad: identificar los dominios y los controles de ISO/IEC 27000

4. Tomar impresión de pantalla completa (con nombre y registro) a cada actividad, recorta y pega en el archivo de WORD.

3. Desarrollo de la actividad

Los 12 dominios de seguridad



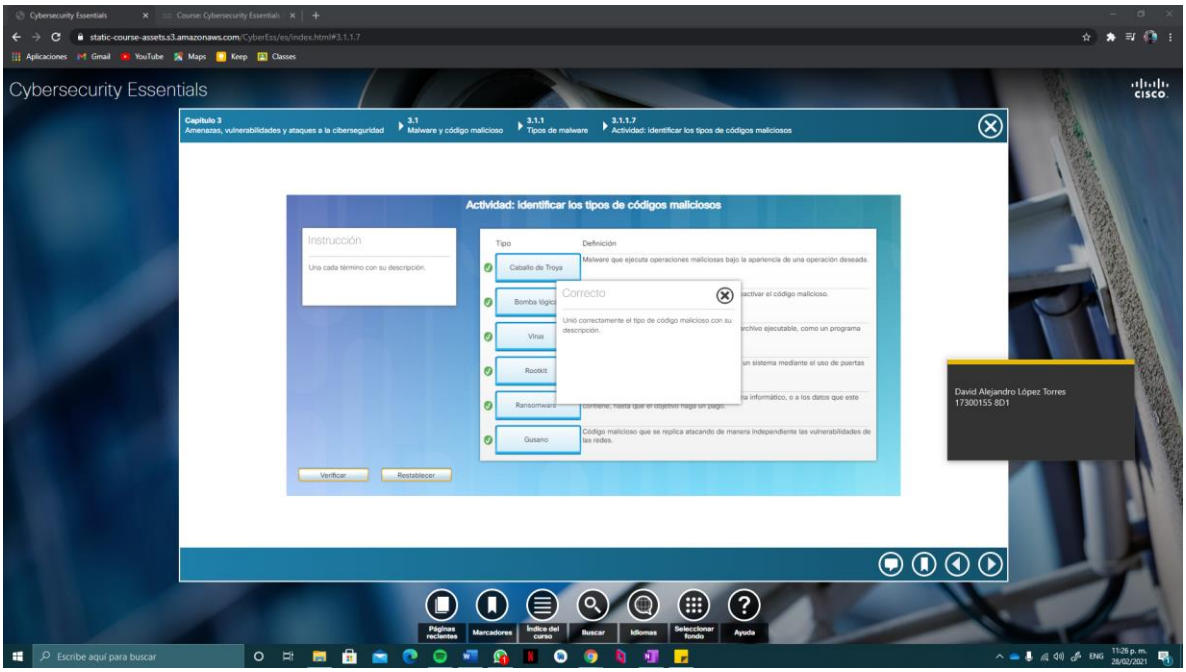
Virus, Gusano Troyano

Característica	Virus	Troyano	Gusano
Historia	El primer virus atacó una máquina IBM Serie 360, se llamaba Creeper, y fue creado en 1972 por Robert Thomas Morris. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a Creeper catch me if you can!» (Soy una enredadera, atrápenme si pueden). Para eliminar este problema fue creado el primer programa antivirus denominado Reaper. Sin embargo, el término virus no sería adoptado hasta 1984, aunque ya existían antes. El inicio de todo se dio en los laboratorios de Bell Computers. Cuatro programadores (H. Douglas Mellory, Robert Morris, Victor Vysottsky y Ken Thompson) desarrollaron un juego llamado Core Wars, que consistía en ocupar toda la memoria RAM del equipo contrario en el menor tiempo posible.	Desde sus orígenes, los troyanos han sido utilizados como arma de sabotaje por los servicios de inteligencia como la CIA, cuyo caso más emblemático fue el Sabotaje al Gasoducto Siberiano en 1982. La CIA instaló un troyano en el software que se ocuparía de manejar el funcionamiento del gasoducto, antes de que la URSS comprara ese software en Canadá. De acuerdo con un estudio de la empresa responsable del software de seguridad BitDefender desde enero hasta junio de 2009, «El número de troyanos está creciendo, representan el 83 % del malware detectado».	El primer gusano informático de la historia data de 1988, cuando el gusano Morris infectó una gran parte de los servidores existentes hasta esa fecha. Su creador, Robert Tappan Morris, fue sentenciado a tres años de libertad condicional, 400 horas de servicios a la comunidad y una multa de 10.050 dólares. Fue este hecho el que alertó a las principales empresas involucradas en la seguridad de tecnologías de la información a desarrollar los primeros cortafuegos.

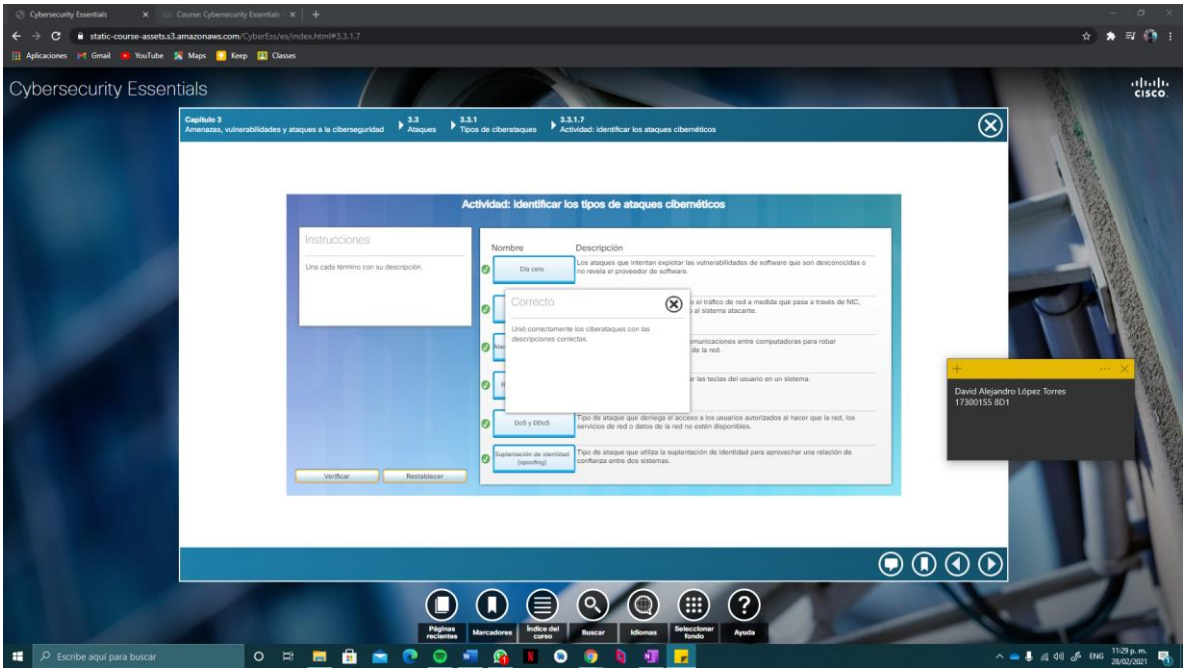
Definición	Software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo	Malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.	Malware que se replica para propagarse a otras computadoras. Este software malicioso suele utilizar una red informática para propagarse, aprovechando las fallas de seguridad en la computadora de destino para acceder a ella.
Propagación	Descarga de archivos desde fuentes no confiables	Abriendo correos de spam o no solicitados	Descarga de archivos dañados
Daños	Borra y altera archivos del ordenador sin consentimiento del usuario	Permite el control de un agente externo sobre nuestro ordenador	Autorreplica archivos y los reenvía a través de la red
Prevención	Asegurarse que los sitios de descarga sean confiables	Depuración de correspondencia no deseada	Dar limpieza y mantenimiento periódico al navegador
Remedio	1. Descargue e instale un analizador de virus. 2. Desconéctese de Internet. 3. Reiniciar el ordenador en el modo seguro. 4. Elimine todos los archivos temporales. 5. Ejecute un análisis antivirus.	Lo mejor es utilizar una solución antivirus fiable que pueda detectar y eliminar cualquier troyano de su dispositivo. Cuando elimine troyanos manualmente, asegúrese de eliminar cualquier programa de su equipo que esté relacionado con el troyano.	1. Adquiere un antivirus especializado en este tipo de malware. 2, Verifica que esté actualizado. Instálalo en tu dispositivo. 3. Inicia el proceso de análisis de tu sistema operativo. 4. Una vez identificados, procede a eliminarlos.

Actividades de Cisco

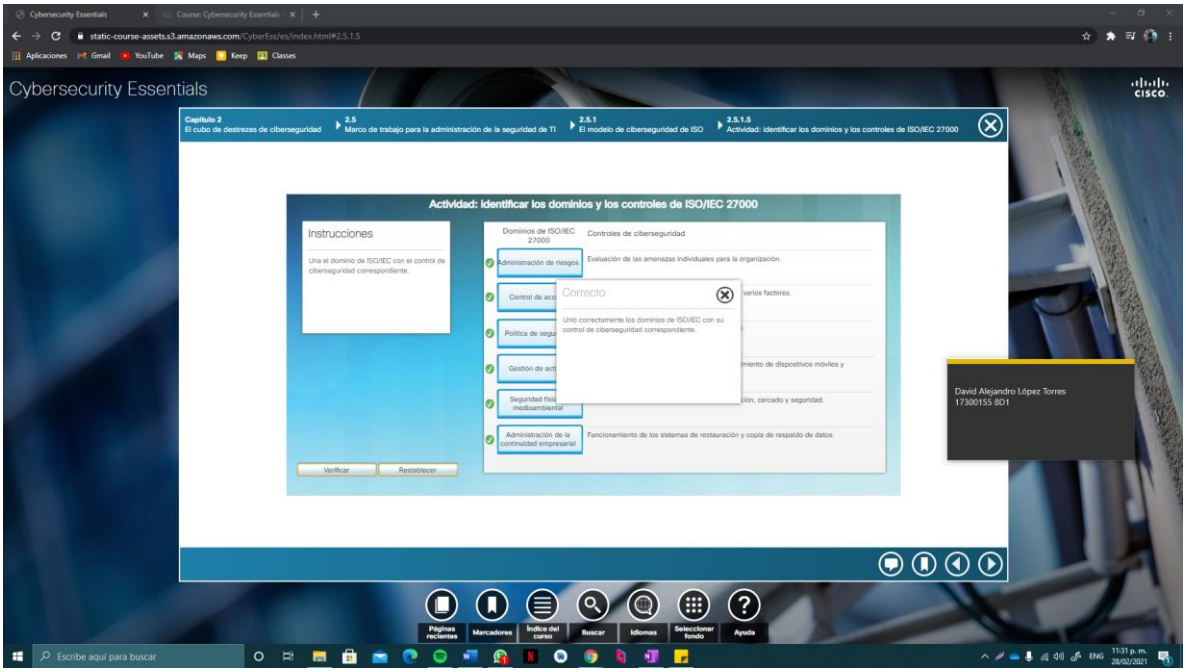
Actividad 3.1.1.7



Actividad 3.3.1.7



Actividad 2.5.1.5



4. Reflexión

Con el desarrollo de esta actividad se ha resaltado el riesgo que representan los diferentes malwares para la seguridad de la información y la integridad de los sistemas. Conocer las diferentes características de cada uno nos permite desarrollar estrategias de pronta detección, prevención y eliminación estos riesgos en cualquier sistema informático vulnerable. Conocer los dominios de seguridad nos permite conocer y establecer políticas de seguridad para la información dentro de un sistema informático mediante la evaluación de riesgos.

Referencias:

- Cisco Systems Networking Academy. (n.d.). Ccna Security 1 1 Esp. Calameo.Com. Retrieved February 28, 2021, from https://es.calameo.com/books/004487660148cc6293440

- Xataca. (2018) ¿Cuál es la diferencia: malware, virus, gusanos, spyware, troyanos, ransomware, etcétera? Retrieved February 28, 2021 from: https://www.xataka.com/basics/cual-es-la-diferenciamalware-virus-gusanos-spyware-troyanos-ransomware-etcetera