**TIPOS DE AMENZAS**

¿Podemos pensar en una cuarta revolución industrial? Aunque en la historia de la humanidad podemos definir claramente tres revoluciones industriales, lo cierto es que existe una cuarta y, es precisamente, la que estamos viviendo en la actualidad, gracias a la aparición de las tecnologías de información y las comunicaciones (TIC), junto con Internet.

En las últimas dos décadas, las TIC han adquirido un valor en dimensiones que nunca antes había ocurrido en la historia, generando profundas transformaciones en todos los ámbitos socioeconómicos y, por supuesto, de la mano aparecieron conductas ilícitas cometidas sobre los datos, la información, los programas y todo aquel recurso tecnológico susceptible de ser manipulado ilícitamente.

La seguridad informática, o ciberseguridad, es una disciplina que se encarga de proteger la integridad y la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. La idea principal es que se pueda evaluar la seguridad de los sistemas de cómputo y redes para, posteriormente, protegerlos de los ataque informáticos que se pueden llevar a cabo a los sistemas.

Pero, ¿esto fue siempre así? A lo largo de la historia, esta seguridad se ha ido transformando, gracias a los controles y auditorías sobre los sistemas, explotando las vulnerabilidades que se puedan encontrar en los mismos. Se han implementado medidas de seguridad física y lógicas en conjunto con la seguridad en Internet.

Por otro lado, sería fantástico poder analizar de forma particular cuál es el impacto que ha causado en la sociedad, en sus normas jurídicas y éticas. Además, reconocer e identificar los delitos informáticos y las consecuencias legales que implican el no acatarlas.

Bien, ha llegado el momento de adentrarnos en el estudio de este maravilloso mundo de seguridad.

Ciberseguridad

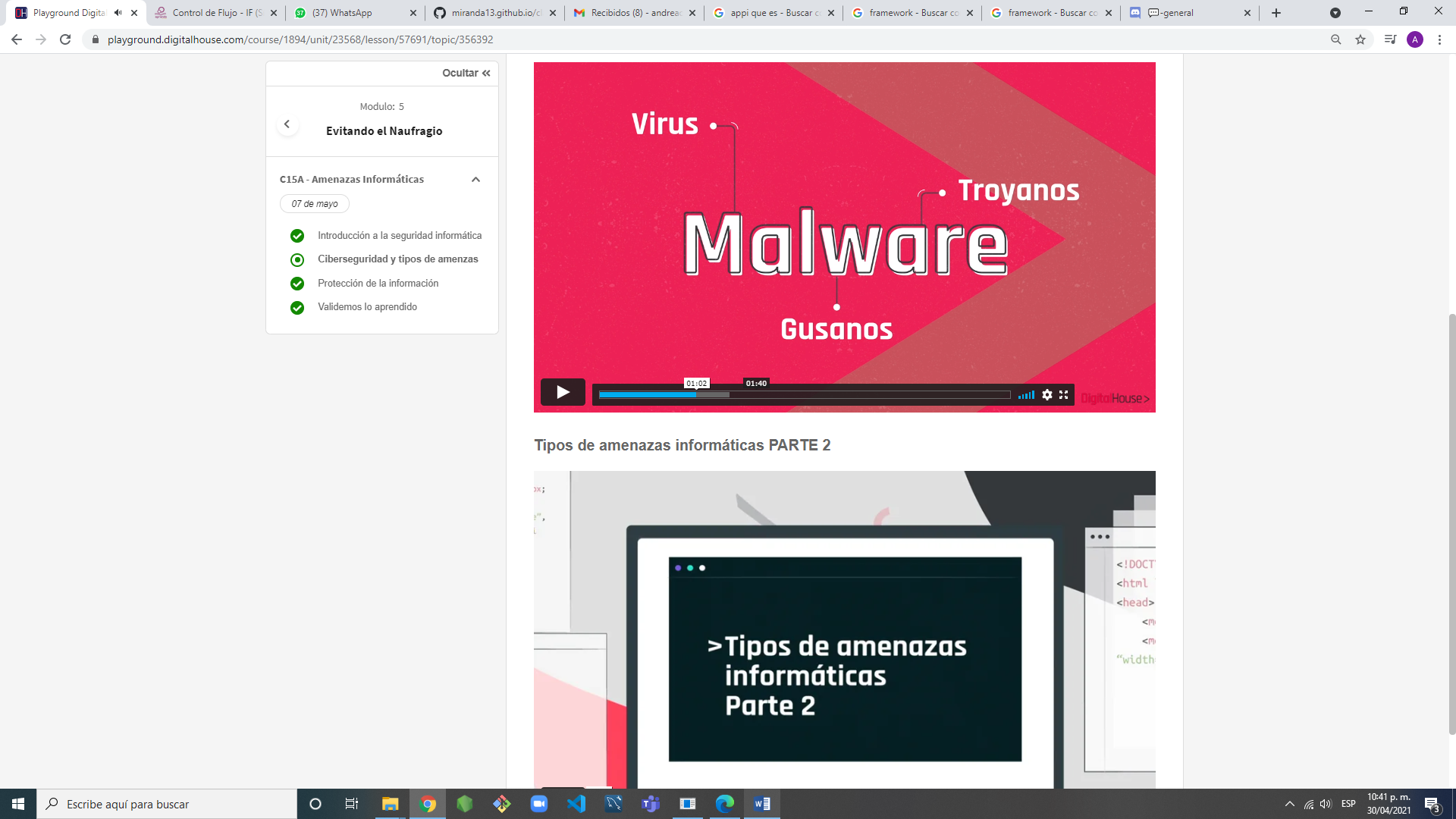
La seguridad informática se enfoca en la **protección de la infraestructura computacional** y todo lo vinculado con la misma, especialmente, en la información que se transmite a través de las redes de computadoras. Para minimizar todos los riesgos a la infraestructura y a la información se han creado a lo largo de la historia múltiples métodos, como estándares, protocolos, reglas, herramientas y obviamente leyes informáticas.

Debemos tener en cuenta que la seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información. No debemos confundir este término con el de seguridad de la información, ya que esta última puede estar en diferentes medios y no solo en los medios informáticos.

Bajo este último concepto, la seguridad informática va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a los equipos de cómputo, servidores, redes informáticas y todo aquel medio informático por el cual se transmita información.

**El atacante utiliza un software maligno:**

Un software maligno también se lo conoce como Malware



**Tipos de malware**

**Virus**

Es un componente de software cuyo objetivo es permanecer en un sistema copiándose a si mismo en varios lugares, es como un virus humano que se esparce por todo el cuerpo y en este caso ocurre lo mismo en la computadora el objetivo es destruir o inhabilitar archivos o programas que tengamos en nuestro dispositivo además de afectar el funcionamiento del mismo. No pueden afectar a otros dispositivos amenos que los pasemos por memoria usb, por eso se dice que son de poca infección por que se esparcen solo en la misma computadora sin afectar a otras.

El objetivo es destruir o inhabilitar archivos o programas

Se adhieren a los archivos ejecutables o también al registro maestro de arranque no pueden afectar a otros dispositivos a menos que lo pasemos por medio de un hadware como un usb esto pasaba a las computadoras más antiguas antes que estuvieran conectadas a la red, todo cambia cuando las computadoras con el tiempo se empiezan a conectar a la red y se crea el

**Gusano**

Este no solo se copia asi mismo en el sistema, sino que además utiliza la red para copiarse a otras computadoras a través de la vulnerabilidad de la red o agujeros de vulnerabilidad, por esto tienen una mayor capacidad de infección, se debe a la evolución de la tecnología el objetivo es saturar el funcionamiento del sistema

**Troyano**

Están basados en el mítico caballo de trolla

Es un programa sin licencia que instalamos y necesita de la ejecución del usuario. Puede crear backdoors que es una puerta trasera para que un dispositivo pueda ser usado de forma remota por alguien más y pueden usarlo para introducir spam esos avisos publicitarios, pero mucho más frecuentes y son muy similares a:

**Spywares**

Son un software espía que no dañan los dispositivos, pero si roban toda la información del sistema desde contraseñas, redes sociales etc. Suelen ingresar en troyanos o también pueden ser instalados.

**Rootkits**

Logran esconderse de los softwares antimalware o antivirus, pueden realizar modificaciones a los archivos internos del sistema incluso a las cuentas de usuario.

**Botnets**

**Mezcla entre**

Bot: robot

Net: red

Es una red de robot que es puesto por un atacante para ser atacadas todas al mismo tiempo, se utiliza principalmente para robo de identidad o de información bancaria, chantaje etc.

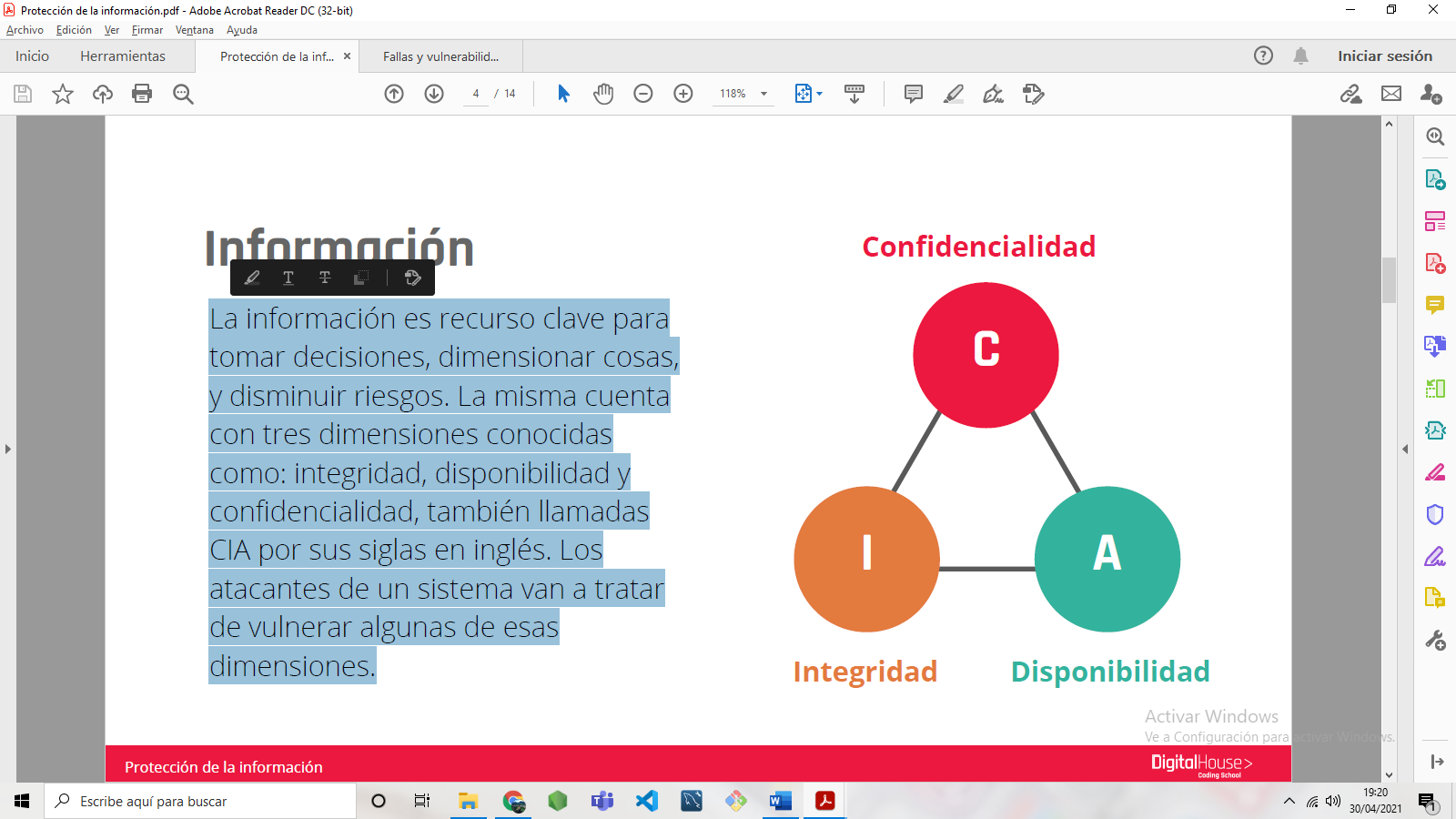
**Ramsomware**

Softwares de secuestro, son utilizados por ciber atacantes para secuestrar redes de empresas y pedir rescate por ellas, se encuentran en correo o deseados o correos parecidos a los originales

**PROTECCIÓN DE LA INFORMACION**

La información es recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos. La misma cuenta con tres dimensiones conocidas

como: integridad, disponibilidad y confidencialidad, también llamadas CIA por sus siglas en inglés. Los atacantes de un sistema van a tratar de vulnerar algunas de esas dimensiones.



**Integridad**

Consiste en que la información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser. Un ejemplo de esta dimensión sería el ataque a una base de datos y la modificación de los datos que hay en la misma, con lo cual podemos seguir viendo la información, pero la misma es errónea debido a que la original fue alterada.

**Disponibilidad**

Significa que la información una persona/usuario debe poder tener acceso a la información en el momento que lo necesita, es decir, en tiempo y forma. Un típico ataque a este tipo de dimensión es el ataque de denegación de servicio.

**Confidencialidad**

Refiere a que la información tiene que estar disponible únicamente para las personas que tienen acceso a esta información y bloqueada para el acceso a terceros. Por ejemplo, los datos

personales e historiales médicos.

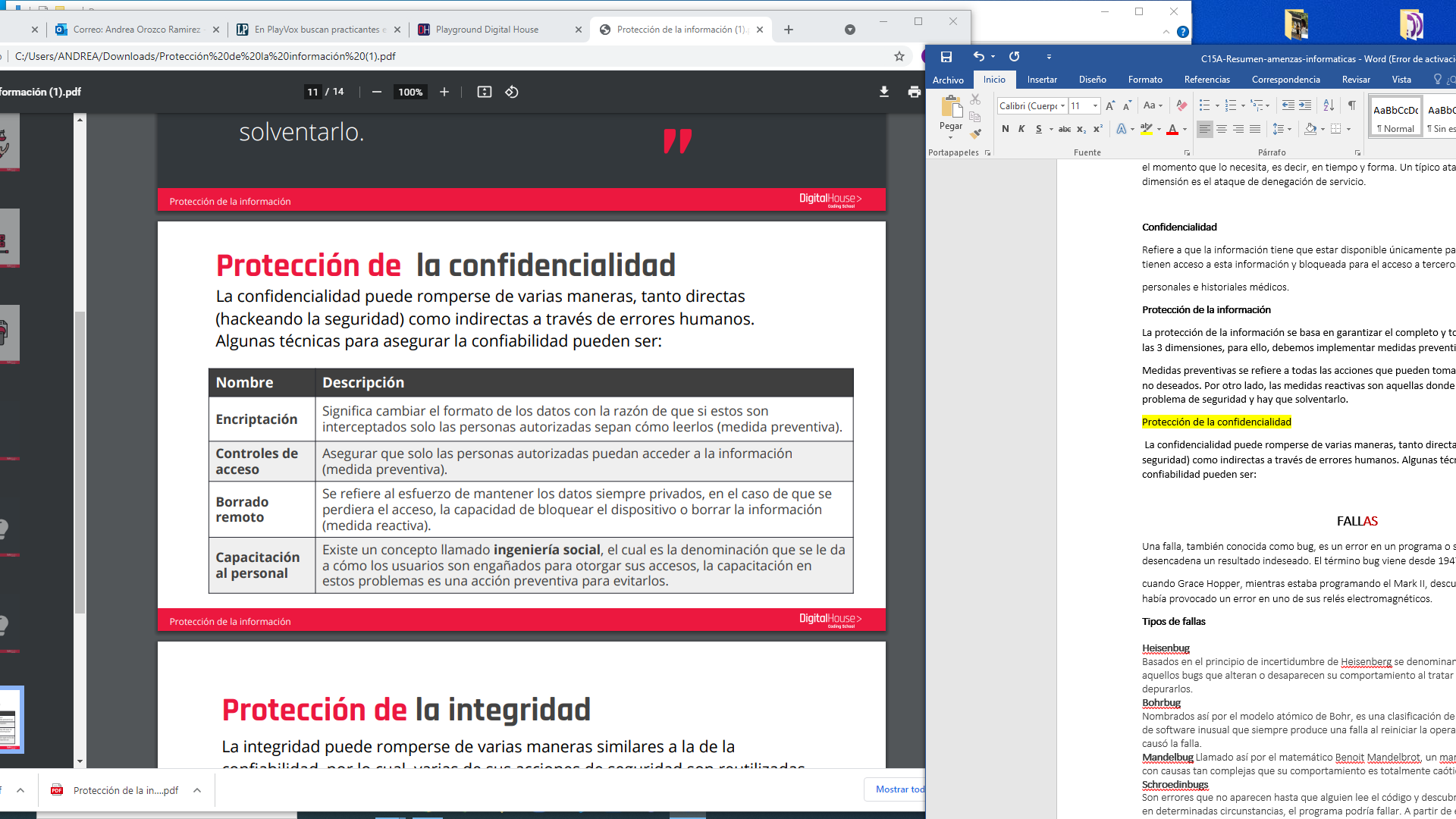
**Protección de la información**

La protección de la información se basa en garantizar el completo y total funcionamiento de las 3 dimensiones, para ello, debemos implementar medidas preventivas y reactivas

Medidas preventivas se refiere a todas las acciones que pueden tomarse para evitar problemas no deseados. Por otro lado, las medidas reactivas son aquellas donde ya se ocasionó un problema de seguridad y hay que solventarlo.

Protección de la confidencialidad

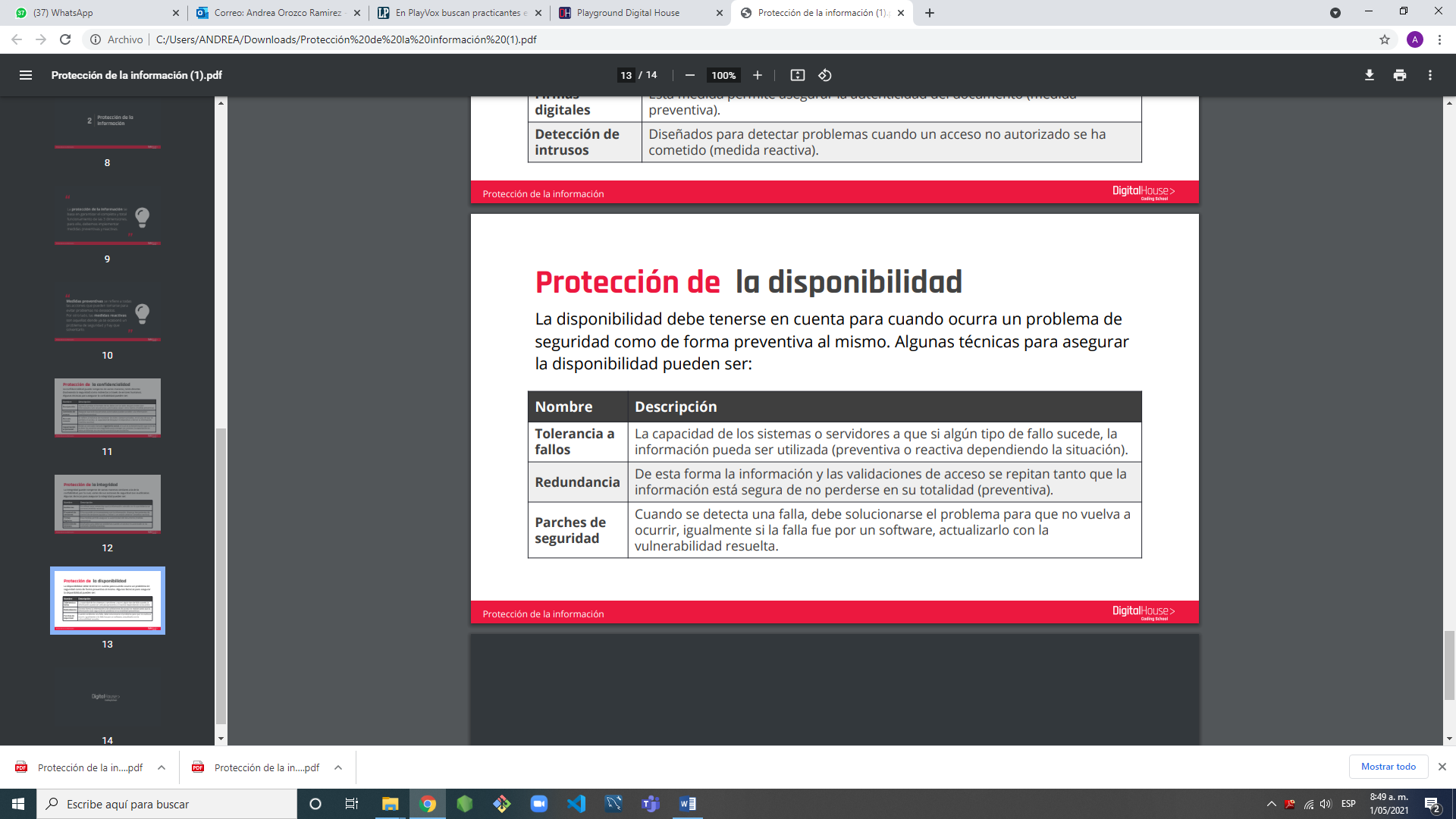
La confidencialidad puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos. Algunas técnicas para asegurar la confiabilidad pueden ser:



Protección de la integridad

La integridad puede romperse de varias maneras similares a la de la confiabilidad, por lo cual, varias de sus acciones de seguridad son reutilizadas. Algunas técnicas para asegurar la integridad pueden ser:

Protección de la disponibilidad

La disponibilidad debe tenerse en cuenta para cuando ocurra un problema de seguridad como de forma preventiva al mismo. Algunas técnicas para asegurar la disponibilidad pueden ser

**FALLAS**

Una falla, también conocida como bug, es un error en un programa o sistema operativo que desencadena un resultado indeseado.

El término bug viene desde 1947 cuando Grace Hopper, mientras estaba programando el Mark II, descubrió que un insecto (bug) había provocado un error en uno de sus relés electromagnéticos.

En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer unos tipos generales de bugs según su comportamiento.

**Tipos de fallas**

**Nombre Descripción**

**Heisenbug**

Basados en el principio de incertidumbre de Heisenberg se denominan a

aquellos bugs que alteran o desaparecen su comportamiento al tratar de

depurarlos.

**Bohrbug**

Nombrados así por el modelo atómico de Bohr, es una clasificación de un error

de software inusual que siempre produce una falla al reiniciar la operación que

causó la falla.

**Mandelbug** Llamado así por el matemático Benoit Mandelbrot, un mandelbug es un fallo

con causas tan complejas que su comportamiento es totalmente caótico.

**Schroedinbugs**

Son errores que no aparecen hasta que alguien lee el código y descubre que,

en determinadas circunstancias, el programa podría fallar. A partir de ese

momento, el “Schroedinbug” comienza aparecer una y otra vez.

**VULNERABILIDAD**

Una vulnerabilidad es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información. La evaluación o detección de vulnerabilidades permite reconocer, clasificar y caracterizar los agujeros de

seguridad.

Pasos para detectar una vulnerabilidad

Si bien no existe un método único para detectar vulnerabilidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.

● Evaluar cómo está constituida la red e infraestructura de la empresa.

● Delimitar quién puede y debe acceder a la información confidencial.

● Probar que las copias de seguridad realizadas funcionen.

● Identificar las partes más sensibles y esenciales del sistema.

● Realizar auditorías del estado de la seguridad informática