

Actividad [#1] – [Actividad 1 analisis de riesgos] [Seguridad Informática I]

Ingeniería en Desarrollo de Software

**Tutor: Elizabeth Guevara Roa**

**Alumno: Manuel Enrique Ramirez Lopez**

**Fecha: 14/04/2022**

***Indice***

*[Definición del contexto](#_Toc16195)* [1](#_Toc16195)

*[Delimitacion del problema](#_Toc6988)* [2](#_Toc6988)

*[Amenazas humanas](#_Toc7201)* [3](#_Toc7201)

*[Amenazas lógicas](#_Toc23558)* [4](#_Toc23558)

*[Amenazas físicas](#_Toc4507)* [5](#_Toc4507)

*[Vulnerabilidades del almacenamiento](#_Toc7108)*  [6](#_Toc7108)

*[Vulnerabilidades de comunicación](#_Toc7299)* [7](#_Toc7299)

# *Definición del contexto*

|  |
| --- |
| **Escenario principal:**  La clínica de salud tiene una finalidad social, por lo que se deberá regir bajo los principios de universalidad y solidaridad como herramientas para aumentar la cobertura, así como la calidad y calidez en la atención a sus usuarios. Por consiguiente, se te solicita formar parte del proyecto como analista e implementador de mecanismos de seguridad informática. En este contexto, el gerente te brinda la siguiente información sobre la clínica:  ● Se ubica dentro de una región cerca de la costa.  ● Tiene un servidor espejo.  ● Consta de 2 pisos, en los cuales se tiene solo una salida fija de emergencia.  ● La red cuenta con 4 servidores, 21 estaciones de trabajo y una impresora local.  ● Los equipos de la planta baja se encuentran conectados por cable de manera directa al módem. Los del piso de arriba son portátiles y se conectan vía Wifi.  ● Se cuenta con 3 turnos por cada consultorio.  ● Los equipos han estado lentos en el último mes y se están quedando sin espacio de almacenamiento.  ● Se cuenta con un dispositivo biométrico facial para el reconocimiento y asistencia de los empleados; sin embargo, los dispositivos de gerencia no están dados de alta.  ● El edificio está distribuido en dos áreas, divididas por escaleras de acceso junto a los ascensores.  ● Cada equipo cuenta con un usuario y contraseña básicos, por ejemplo:  o Usuario: Equipo1  o Password: Clinica 1  ● El *firewall* no se encuentra habilitado.  ● No se tiene denegado el uso del equipo para actividades personales, por ejemplo, el acceso a redes sociales o el manejo del correo electrónico o *whatsapp*.  ● El *Servidor 1* cuenta con la base de datos general. Este utiliza el software Oracle Database en un sistema operativo Linux. Por su parte, el *Servidor 2* se destina para alojar un sistema de control que descargaron de Internet, y que les ayuda para mantener los registros de los pacientes (se desconoce la fuente de este software). Los *Servidores 3* y *4* se encuentran en las oficinas generales; uno en planta baja, el cual pertenece al área de afiliación; y el otro en el piso superior, en el área administrativa financiera y dirección general.  ● El área administrativa financiera no cuenta con una alarma de seguridad para su acceso. |

# *Delimitacion del problema*

# **My First Board (1)**

# *Amenazas humanas*

# **5 amenazas**

# IMG_256**-**De personal interno que encuentre un “bug” sin ser de forma intencionada pero que a su vez se beneficie de ello.*(Robo)*

# **-**Sabotaje o compra de algun cracker a personal que tenga acceso a computadoras clave (Ya que se usa red lógica y cerrada) con el pretexto de “ten toma esta USB y solo conectala a X maquina”.*(Ingeniera social)*

# IMG_256

# **-**Cracker cuyo proposito es sacar ventaja de los datos de los clientes, ya que por la rama que se maneja de la empresa manejar una informacion tan delicada expone a los familiares de los internos y este sujeto busca enriquecerse a costa de los demás.*(Intrusos remunerados)*

# **-**Phareakers buscarian obtener una linea oficial de la clinica para con ello gastar bromas a clientes y así afectar a reputación del establecimiento.*(Ex-empleados)*

# IMG_256

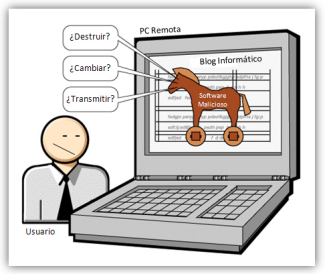
# **-**El uso de procesos inadecuados para la destrucción de informacion delicada (cuando rompes recetas, contacto de clientes, datos bancarios). *(Trashing)*

# *Amenazas lógicas*

# IMG_256**5 amenazas**

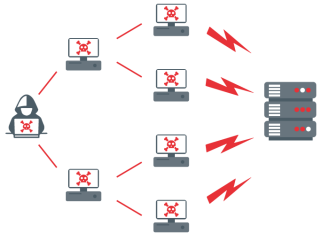
**-**Aprovechamiento de exploits en el sitio web para así infiltrase dentro de los servidores principales (recordemos que el firewall esta inhabilitado)

**-**Falta de supervicion en equipos expuesto, es decir equipos que están al alcance de “clientes” que a su vez insertan Gusanos para propagarse en toda la red del establecimiento.



**-**Pishing para obtener datos mas detallados de los clientes internos y así obtener ganancias a través de fraudes u obtención de informacion bancaria de los familiares de los clientes.

**-**Ataque “Denail of service (DoS)” para inhabilitar el sistema usado y así colapsar estructura internar, ya que los servidores no están preparados para resistir dicha carga masiva de datos.

**-**Gracias al caballo de troya se a insertado un malware de monitorizacion en los equipos y dicho craker se dedica a la obtención de informacion vital como los usuarios y contraseñas de cada equipo y así averiguar cual es la funcion que desempeñan.

# *Amenazas físicas*

# **5 amenazas**

# **IMG_256-**La principal amenaza que pueda en caso ocurrir es inundación ya que recordemos que esta ubicada en la costa y por alguna amenaza de tsunami pueda afectar las oficinas centrales y su informacion.

# **IMG_256-**Incendios ya que si no se cuenta con una correcta refrigeración como esta ubicada en climas húmedos y calurosos esta pueda afectar o provocar algun incendio electrónico dentro de las sedes principales.

# **IMG_256-**Adjunto al punto anterior tomas las medidas necesarias para sobre llevar el oxido que se pueda generar gracias al mar ya que las fuentes informáticas o mejor dicho la tecnología no va de mano con la humedad y las sales provenientes del mar.

# **IMG_256-**Tener una cúpula por manejarlo de una manera mas sencilla en caso de algun siniestro de terremoto ya que en la zona ubicada son mas frecuentes estos y con el movimiento pueda generar inconsistencias en los datos o alguna falla en cadena.

# **IMG_256-**Instalaciones electricas y reguladores de voltaje para no adquirir ruidos o picos de tension dentro de las instalaciones, adjunto contar con una planta en caso de emergencia o apagón general para así durar horas, días en lo que se restablece por completo.

# *Vulnerabilidades del almacenamiento*

**5 vulnerabilidades**



**-**Violación de datos, es decir que algun curioso ya dependiendo sus intenciones podrá ser hacker o cracker acceda de forma ilícita y podrá visualizar, robar, destruir o alterar datos almacenados en los distintos medios de almacenamiento.



**-**Perdida de datos o mejor dicho destrucción de la informacion almacenada estos acontecimientos pueden ser causados por algun “ataque terrorista”

**-**Secuestro de informacion, como se menciona en el punto anterior las intenciones pueden variar de los terroristas que van desde destruir a secuestrar informacion y de alguna manera cifrar-la de manera que sea imposible recuperarla a no ser de pagar algun rescate.

**-**Denegación de servicio “DoS” como forma parte de actos de terrorismo este metodo va de como lo dice la palabra deniega es decir bloquea toda acción de almacenaje, consulta o gestión de la informacion lográndolo de cierta forma saturando todas sus fuentes de procesado, comunicación y almacenaje.

**-**Malos procesos de mantenimiento en los medios de almacenaje (servidores) que va desde mala ventilación que provoca un mal funcionamiento y deterioro de el equipo usado hasta la mala planificación de cambios físicos de discos duros.

# *Vulnerabilidades de comunicación*



**5 vulnerabilidades**

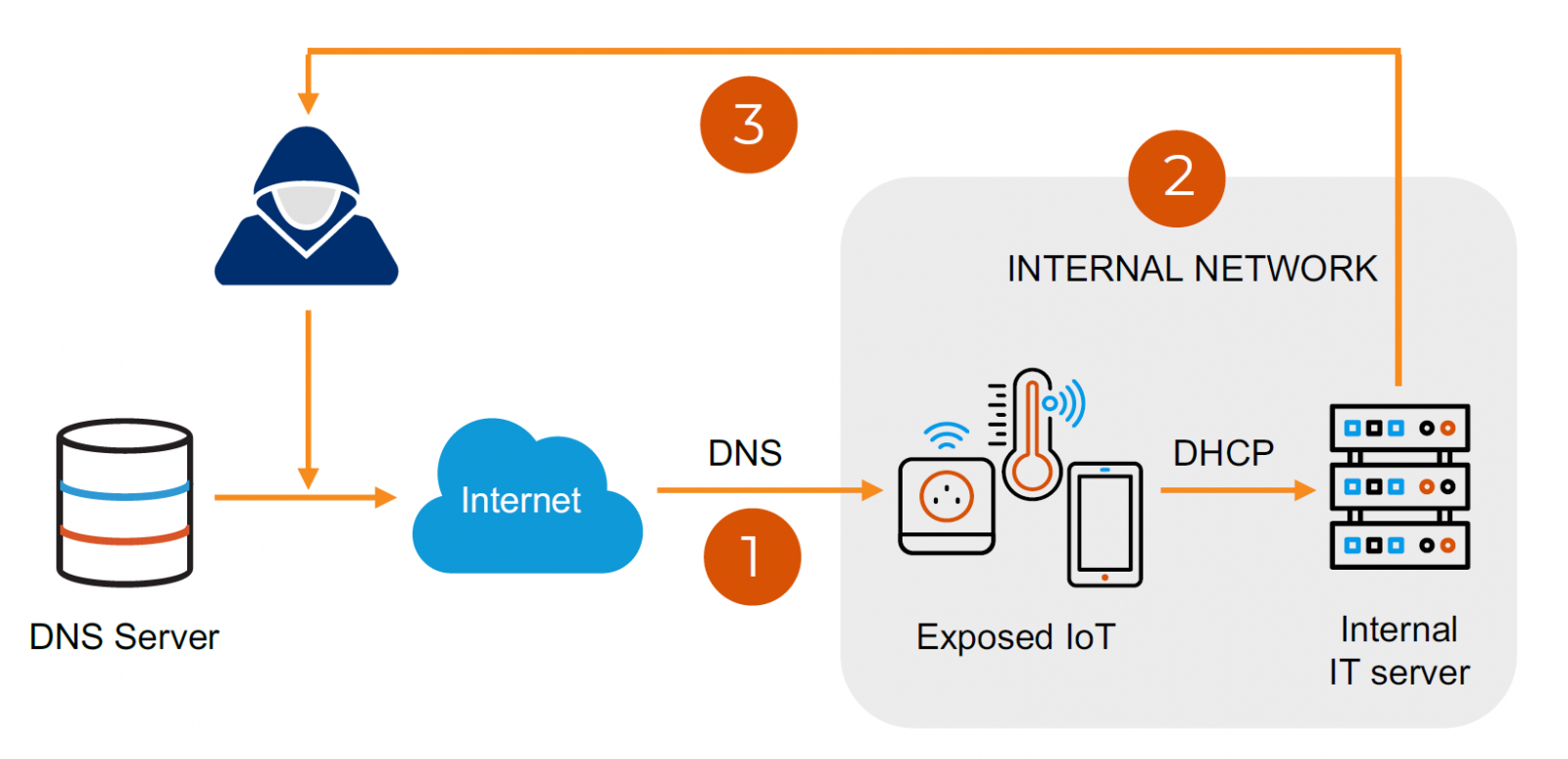
**-**Software vulnerable, el uso inadecuado del software fuera de la estacion de trabajo, que este abierto al publico en general.

**-**Equipo de desarrollo, establecer las bases para mantener actualizado el sistema y que el equipo de desarrollo en turno este en constante mejora del sistema.



**-**Falta de activación de firewall en cada equipo ya que esto hace vulnerable al sistema de ataques externos (internet) y perdida de informacion o suplantación de software que conlleva a fraudes.

**-**Ataques “DoS” Denegación de servicios, con una masiva de conexiones simultaneas buscan saturar o mejor dicho tirar el sistema generando así perdidas importantes.



**-**Amenazas de malware que este mismo se pueda infiltrar desde la red o directamente con algun personal interno que tenga malas intenciones colocándolo en computadoras-servidores principales.