**Tarea 3 Modelando Amenazas**

Presentado Por:

Jose Fernando Ararat Moreno

Presentado a:

Mag. Cesar Antonio Villamizar

Universidad Nacional abierta y a distancia-UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Information Security

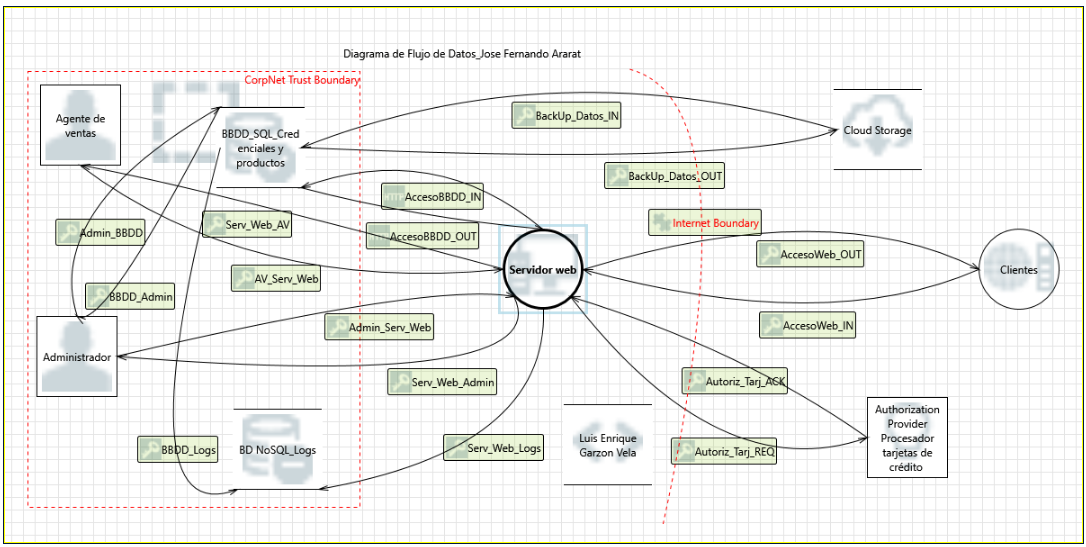
2024

**Objetivos**

* Evaluar los riesgos de seguridad de la información en los procesos de desarrollo de software de acuerdo don estándares y la política de seguridad de la organización para garantizar la calidad en los productos de software.
* Realizar lectura correspondientes a la unidad 2.
* Publicar en el foro de la actividad la pregunta y la respuesta argumentada.
* Elaborar una presentación electrónica en línea, presentando la información relevante.
* Instalar la herramienta Threat Análisis and Modeling Tool 2016 y realizar un diagrama de flujo.
* Identificar amenazas.
* Documentar las amenazas.
* Valorar las amenazas.
* Describir la mitigación de las amenazas.

.

**Diagrama de Flujo de Datos (DFD)**



**Enlace de la presentación**

<https://unadvirtualedu-my.sharepoint.com/:p:/g/personal/jfararatm_unadvirtual_edu_co/EWvn6p7jU81Ij1MWgvGTPu8Bznn_6hcmzopeY2mCiAD3jA?e=hQTCjb>

**Trabajo Individual**

1. Documentar las amenazas.

|  |  |
| --- | --- |
| **Descripción de la amenaza** | **Data Flow sniffing** (rastreo del flujo de datos): esta se produce cuando un atacante puede observar y analizar el tráfico de la red. |
| **Objetivo** | Obtener información confidencial o sensible |
| **Técnicas de ataque** | 1. Análisis de paquetes. 2. Monitoreo de redes. 3. Ataque de intermediario. 4. Análisis de metadatos. |

|  |  |
| --- | --- |
| **Descripción de la amenaza** | **Spoofing the servidor web process** (Suplantación del proceso web del servidor)**:** se produce cuando un atacante puede obligar a un servidor web a realizar una solicitud a un sitio web o servicio web que no está autorizado realizar. |
| **Objetivo** | Tomar el control del servidor web |
| **Técnicas de ataque** | 1. Inyección de código. 2. Manipulación de encabezados HTTP. 3. Explotación de vulnerabilidades. |

|  |  |
| --- | --- |
| **Descripción de la amenaza** | **Data Store Inaccessible** (Almacén de datos inaccesible)**:** se produce cuando un atacante impide que los usuarios legítimos o con permisos accedan normalmente al almacén de datos. |
| **Objetivo** | Interrumpir las operaciones comerciales y/o robar datos confidenciales |
| **Técnicas de ataque** | 1. Ataques de denegación de servicio. 2. Ataques de ransomware. 3. Ataques de malware. 4. Ataques de ingeniería social. 5. Ataques físicos. |

|  |  |
| --- | --- |
| **Descripción de la amenaza** | **weak credential storage** (almacenamiento de credenciales débiles)**:** se ejecuta cuando las credenciales de acceso se almacenan de forma insegura, esto permite que los atacantes acceder de manera fraudulenta a sistemas, cuentas y datos. |
| **Objetivo** | Obtener acceso a credenciales almacenadas para acceder a sistemas, cuentas o datos sin autorización. |
| **Técnicas de ataque** | 1. Ataques de fuerza bruta. 2. Ataques de relleno de credenciales. 3. Ataques de phishing. 4. Ataques de malware. |

|  |  |
| --- | --- |
| **Descripción de la amenaza** | **Cross site request forgery** (Falsificación de petición en sitios cruzados)**:** se produce cuando un atacante engaña al navegador web de un usuario autenticado para que envíe una solicitud no deseada a una aplicación web vulnerable. |
| **Objetivo** | Tomar el control de la cuenta del usuario y realizar acciones no autorizadas en su nombre. |
| **Técnicas de ataque** | 1. Sitios web maliciosos. 2. Correos electrónicos de phishing. 3. Scripts entre sitios (XSS). |

Tabla 1. Documentación de las amenazas

1. Valorar las amenazas.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Probabilidad de Ocurrencia (P)** | | | **Impacto Potencial (I)** | | **P** | **I** | **Riesgo** |
| **Amenaza** | ***R*** | ***E*** | ***DI*** | ***D*** | ***A*** | ***(R+E+DI)*** | ***(D+A)*** | ***PxI*** |
| Inyección de comandos SQL | 3 | 2 | 2 | 3 | 3 | 7 | 6 | 42 |
| Rastreo del flujo de datos | 3 | 1 | 1 | 2 | 2 | 5 | 4 | 20 |
| Suplantación del proceso web del servidor | 3 | 3 | 2 | 3 | 3 | 8 | 6 | 48 |
| Almacén de datos inaccesible | 2 | 2 | 1 | 2 | 3 | 5 | 5 | 25 |
| almacenamiento de credenciales débiles | 3 | 3 | 3 | 3 | 3 | 9 | 6 | 54 |
| Falsificación de petición en sitios cruzados | 3 | 3 | 2 | 3 | 3 | 8 | 6 | 48 |

Tabla 2. Calculo el riesgo

1. Mitigación.

|  |  |
| --- | --- |
| **Descripción de la amenaza** | Rastreo del flujo de datos |
| **Medidas mitigación** | Cifrar datos, utilizar una red privada virtual, utilizar un navegador web que proteja la privacidad. |

|  |  |
| --- | --- |
| **Descripción de la amenaza** | Suplantación del proceso web del servidor |
| **Medidas mitigación** | Utilizar HTTPS, implementar HSTS, utilizar un firewall de aplicaciones web, mantener el software actualizado, educar a los usuarios o empleados. |

|  |  |
| --- | --- |
| **Descripción de la amenaza** | Almacén de datos inaccesible |
| **Medidas mitigación** | Realizar copias de seguridad, implementar controles de acceso estrictos, segmentar la red, implementar firewalls y sistema de detención de intrusos, mantener el software actualizado, capacitar a los empleados en seguridad de la información. |

|  |  |
| --- | --- |
| **Descripción de la amenaza** | almacenamiento de credenciales débiles |
| **Medidas mitigación** | Utilizar contraseñas robustas, habilitar la autenticación de dos factores, almacenar las credenciales de forma segura. |

|  |  |
| --- | --- |
| **Descripción de la amenaza** | Falsificación de petición en sitios cruzados |
| **Medidas mitigación** | Validación de entrada, escapar las salidas, utilizar un marco de trabajo web seguro, utilizar escáneres de vulnerabilidades. |

Tabla 3. Salvaguardas

**Referencias Bibliográficas**

Marmolejo, P.A. (2021). Principios de la seguridad de la información y Propiedades del Software seguro. <https://repository.unad.edu.co/handle/10596/41638>

Chris Bronk. (2016). Cyber Threat: The Rise of Information Geopolitics in U.S. National Security. Praeger. <https://bibliotecavirtual.unad.edu.co/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1140402&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp_41>

Death, D. (2017). Information Security Risk Management. En S. Editing (Eds), Information Security Handbook (p.p 66 – 83). Packt Publishing. https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1655557&lang=es&site=eds-live&scope=site&ebv=EB&ppid=pp\_183