UNA-VD-CIRC-029-2022
UNA-DTIC-CIRC-008-2022

PARA: Comunidad universitaria

DE: Vicerrectoría de Docencia
Dirección de Tecnologías, Información y Comunicación

ASUNTO: Mejoras de seguridad implementadas en los servicios de Aula Virtual

FECHA: 12 de mayo de 2022

En atención al criterio técnico de la circular UNA-DTIC-CIRC-07-2022 de la Dirección de Tecnologías de la Información y Comunicación, enviado por correo el 28 de abril del 2022, referido a: INSTRUCCIONES PARA EL ASEGURAMIENTO DE SERVIDORES DE CÓMPUTO Y DE LA PLATAFORMA TECNOLÓGICA INSTITUCIONAL, me permito informarles que el equipo informático de la Vicerrectoría de Docencia, en acciones coordinadas con el equipo informático del Centro de Gestión Informática (CGI), han realizado una serie de acciones para robustecer la seguridad de los sistemas de Aula Virtual.

Algunas de las medidas de seguridad implementadas, pueden tener impacto en el acceso y uso de algunas actividades y recursos del Aula Virtual.

A continuación, se detallan las medidas implementadas y su posible impacto y soluciones:

1. **Actualizaciones de las plataformas de Aula Virtual:** Durante la semana del 28 de abril al 5 de mayo, se actualizaron los servidores y las versiones de Moodle de todas las plataformas de Aula Virtual, este evento no tiene implicaciones posteriores.

2. **Implementación de Firewall:** El martes 10 de mayo de 2022 se implementó un Firewall por parte del CGI y posteriormente se han reportado más de 43 mil intentos de acceso malicioso al Aula Virtual Institucional, como se observa en la siguiente imagen. Cabe mencionar que en esta imagen no se incluyen los accesos válidos de los profesores y estudiantes en la plataforma, por lo cual es evidente que el Aula Virtual Institucional recibe un tráfico alto, en los sistemas informáticos que la Universidad Nacional ofrece a la comunidad.

Requested filters:
Security Policy contains "/Common/POL_WAF_AULAVIRTUAL"

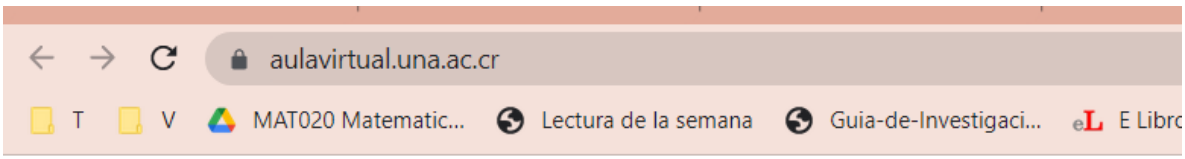
Violation	▼ Requests
Access from malicious IP address	43555
Illegal HTTP status in response	7567
Evasion technique detected	1112
HTTP protocol compliance failed	1103
Request length exceeds defined buffer size	656
Illegal file type	159
Illegal method	89
Malformed JSON data	17
Access from disallowed Geolocation	15

Total Entries: **9**

3. La implementación del Firewall trae consigo un tiempo en que el sistema debe adaptarse a la actividad normal de la plataforma y las acciones realizadas por sus usuarios, por lo que por el momento se pueden experimentar bloqueos en ciertas actividades, como en los casos que se describen a continuación:

CASO 1.

Problema: Al ingresar a la plataforma de Aula Virtual Institucional digitando de forma directa en el navegador la dirección https://www.aulavirtual.una.ac.cr, existe la posibilidad que se le muestre el siguiente error



La URL solicitada fue rechazada. Por favor consulte con su administrador.

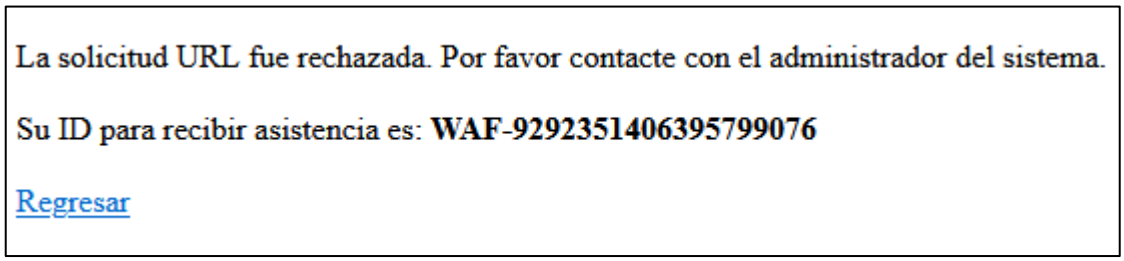
Su ID de soporte es: 9292351406396814925 [Volver]

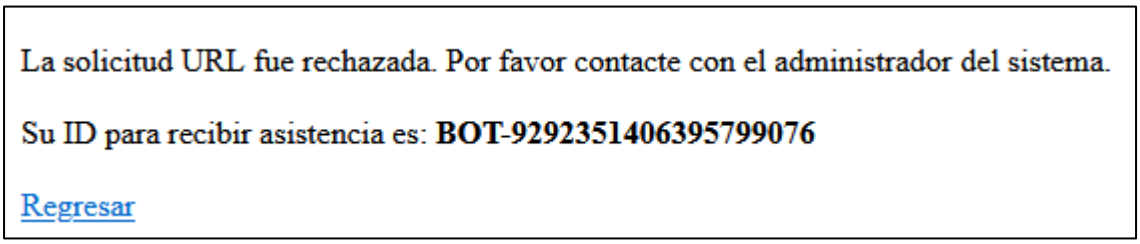
Causa: El firewall tiene una base de datos con una lista negra de IP`s y la IP de su modem, se encuentra en esa lista negra, por lo cual es bloqueada. Es importante destacar que esto se debe a que las IP de los hogares no son fijas, y cada vez que se reinicia el módem, su IP cambia, de esta forma puede, que en algún momento la IP que usted fuese usada por otro usuario en actividades maliciosas, por eso aparece en la lista negra.

Solución: Reinicie el modem de su hogar. Si esto no funciona envié un correo a ticdocencia@una.cr con la imagen del bloqueo.

CASO 2.

Problema. Se puede presentar al ingresar a una actividad o un recurso, por tiempo de finalización de la sesión, o por tipo de archivo. El sistema les bloquea y les aparece las siguientes leyendas ya sean de tipo WAF o BOT, como se observa en las imágenes.





Causa: Dentro del Firewall la actividad o recurso que usted está intentando utilizar, no se encuentra contempladas las reglas de exclusión asignadas a la plataforma, esto a pesar de realizar un mapeo por parte del personal de equipo de informáticos de Docencia, para ingresar todas las excepciones posibles.

Solución: Enviar un correo a ticdocencia@una.cr con la imagen, para evaluar si procede a agregarse la excepción para que sea permitido dentro del aula virtual dicha actividad.

4. **Deshabilitación para subir archivos ejecutables:** A partir del próximo lunes 16 de mayo, se deshabilitará la posibilidad de subir archivos de tipo .msi, .exe y cualquier otro ejecutable, esto como medida de seguridad para evitar la inserción de software malicioso dentro de los servidores que albergan el aula virtual.
   Como medida de contingencia para las personas docentes, que dentro de sus proyectos académicos solicitan este tipo de archivos a las personas estudiantes, se recomienda que se habiliten espacios en One Drive o Teams, y en Aula Virtual se solicite solo el enlace compartido.

5. **Reducción de tamaño de subida de archivos:** A partir del próximo lunes 16 de mayo, se reducirá la subida de archivos en el Aula Virtual Institucional a 250MB. Como medida de contingencia, se recomienda a las personas docentes y estudiantes utilizar otras plataformas institucionales, como One Drive para la subida de archivos de gran tamaño. En este video se explica, por ejemplo, como subir un video a One Drive para vincularlo al Aula Virtual https://youtu.be/FmjkovKsnQ0

   Es importante destacar que, en periodos de inicio de ciclos, trimestre y cuatrimestre, se contempla la necesidad de realizar un incremento en el tamaño de subido a 1GB, esto para que se pueda realizar el proceso de restauración de copias de seguridad de cursos.

6. **Mejoras en seguridad:** Se implementaron mejoras en seguridad para evitar los accesos maliciosos, debido a que se ha detectado una posible suplantación de identidad por medio de un BOT. Por lo tanto, en algunos casos, el sistema verificará por medio del CAPTCHA si es un humano el cual va a realizar la solicitud de ingreso. Esto será normal en dispositivos de la marca Apple (Mac/IPhone/IPad).

7. **Consejos de seguridad adicionales:** Adicional a las mejoras implementadas, se recuerda la responsabilidad de cada persona usuaria, de hacer un uso responsable de sus credenciales institucionales, no compartir sus claves con nadie, realizar cambios periódicos de las mismas, crear contraseñas seguras (no use su fecha de cumpleaños, nombre, nombre de sus familiares, etc.; procure combinar letras y números). Además, recuerde siempre cerrar su sesión al terminar de usar la plataforma, principalmente si está en una computadora pública.

Dada la importancia y las implicaciones académicas del contenido de esta circular, **se solicita a las personas directoras y subdirectoras, instruir a las personas académicas para que, en la semana del 16 al 20 de mayo de 2022, abran un espacio en su horario de clase, para dar lectura a este documento**.

Debido a que estas acciones de seguridad se implementan en un ambiente en que el país está bajo una serie de ataques a la seguridad informática, **se solicita NO divulgar en redes sociales el contenido de esta circular**.

Las consultas acerca de este tema se pueden dirigir al correo ticdocencia@una.cr, el cual se está atendiendo en horario de 7:00 a.m. a 6:00 p.m.

Atentamente,

Firmado por AXEL ARMANDO HERNANDEZ VARGAS (FIRMA)
PERSONA FISICA, CPF-01-0968-0694.
Fecha declarada: 13/05/2022 04:46 PM
Lugar: DTIC

M.Sc. Axel Hernández Vargas
Director de DTIC
Universidad Nacional

RANDALL HIDALGO MORA (FIRMA)
PERSONA FISICA, CPF-04-0168-0374.
Fecha declarada: 12/05/2022 04:20:08 PM

M.Sc. Randall Hidalgo Mora
Vicerrector de Docencia
Universidad Nacional