SISTEMA DE SEGURIDAD EN INFRAESTRUCTURA

REV. DD/MM/AAAA

Padre Sarmiento 19, bajo
36204 Vigo. Pontevedra
+ 34 986 415 241

ÍNDICE

Padre Sarmiento 19, bajo
36204 Vigo. Pontevedra
+ 34 986 415 241

1. Introducción.

A continuación, describiremos los distintos sistemas de seguridad integrados en la plataforma.

2. Sistemas de Seguridad.

2.1. Sistema de copias de Seguridad.

Copia de seguridad diaria de base de datos y de sistema de ficheros, ejecutada automáticamente por AWS y con un periodo de retención de 30 días

2.2. Actuaciones de mitigación frentes a los principales ataques y/o vulnerabilidades a los que está expuesta la plataforma

Se realiza la actualización periódica del código de la plataforma y configuración de seguridad según las recomendaciones de Moodle y las mejores prácticas.

2.3. Actuaciones en materia de Ciberseguridad frente a las principales vulnerabilidades.

- **Todos los interfaces de frontent están protegidos**

En todos los interfaces tanto de acceso al servicio como de gestión, la comunicación se realiza a través de protocolos seguros (HTTPS y SSH) respectivamente.

Con respecto al acceso externo a la base de datos que en la actualidad se realiza a través de mysql, se utiliza exclusivamente conexión SSL y el acceso a las tablas está limitado únicamente a las tablas necesarias.

- **Denegación de servicio.**

Todos los elementos de la infraestructura están protegidos por AWS Shield standard que protege frente a los ataques DDoS más comunes y frecuentes que tienen lugar en la capa de red y transporte y que están dirigidos las aplicaciones o sitios web

- **Fuga de información.**

Padre Sarmiento 19, bajo
36204 Vigo. Pontevedra
+ 34 986 415 241

Comunicación en todos los interfaces a través de protocolos seguros y restricciones de privilegios de acceso. El acceso a los frontend solo es posible mediante certificado público-privado validado previamente en el servidor y con restricción de ip del equipo desde el que se accede.

- **Manejo inadecuado de errores.**

Se realizan copias de seguridad diarias.

- **Inyecciones en el código.**

Disponemos de WAF instalado en el load balancer para proteger frente a los ataques web más comunes.

El WAF es un servicio de firewall de aplicaciones web que le permite monitorear las solicitudes web que se reenvían a una API de Amazon. Puede proteger esos recursos en función de las condiciones que especifique, como las direcciones IP desde las que se originan las solicitudes.

2.4. Servidores de alta disponibilidad y redimensionables, protegidos por firewalls y mecanismos de protección anti-DOS y DDOS

Los servidores están desplegados en una configuración de alta disponibilidad y alojados tras un load balancer que actúa de barrera frente ataques DoS.

2.5. Comunicación protegida segura (cifrada) entre los usuarios y el servidor

En todos los interfaces tanto de acceso al servicio como de gestión, la comunicación se realiza a través de protocolos seguros (HTTPS y SSH) respectivamente.

2.6. Actualizaciones de seguridad (mantenimiento): Instalación periódica de parches de seguridad.

A nivel de sistema operativo y de código de plataforma, de modo periódico mediante el despliegue de nuevas imágenes que contienen las últimas actualizaciones de seguridad.