Cifrado Seguro NGINX

Para activar el Cifrado Seguro en servidores Nginx (sea Windows o Linux), tendremos que acceder al archivo de configuración del Server 443, el cual puede estar en una de estas ubicaciones:

- En el archivo /etc/nginx/nginx.conf
- En un archivo dentro de la carpeta /etc/nginx/conf.d
- En un archivo dentro de la carpeta /etc/nginx/sites-enabled

```
server {
    listen       443 ssl http2 default_server;
    listen       [::]:443 ssl http2 default_server;
    server_name  _;
    root         /usr/share/nginx/html;

    ssl_certificate "/etc/nginx/ssl/Certificate.crt";
    ssl_certificate_key "/etc/nginx/ssl/private.key";
    ssl_session_cache shared:SSL:1m;
    ssl_session_timeout  10m;
    ssl_ciphers HIGH:!aNULL:!MD5;
    #ssl_prefer_server_ciphers on;
```

En este archivo, deberemos hacer 3 configuraciones:

1. Agregar el atributo ssl_protocols de la siguiente manera: ssl_protocols TLSv1.2;
2. Buscar el atributo ssl_prefer_server_ciphers y descomentarlo o agregarlo: ssl_prefer_server_ciphers on;
3. Buscar el atributo ssl_ciphers y editarlo de la siguiente manera:

ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4"

Debe quedar de la siguiente manera:

```
    server {
        listen       443 ssl http2 default_server;
        listen       [::]:443 ssl http2 default_server;
        server_name  _;
        root         /usr/share/nginx/html;

        ssl_certificate "/etc/httpd/ssl/Certificate.crt";
        ssl_certificate_key "/etc/httpd/ssl/private.key";
        ssl_session_cache shared:SSL:1m;
        ssl_session_timeout  10m;
        ssl_ciphers "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4";
        ssl_prefer_server_ciphers on;
        ssl_protocols TLSv1.2;
```

Los cambios realizados se aplicarán después de reiniciar el servicio Nginx.

Nota: Si quieres un cifrado más seguro, reemplazar los Cipher Suites por:

ssl_ciphers ALL:!RSA:!CAMELLIA:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!SHA1:!SHA256:!SHA384

Tener en cuenta que, si el cliente no es compatible con alguno de los Cipher Suites seguros, no se podrá establecer la comunicación.

HSTS en Servidores Nginx

Si quieres activar HSTS para obtener un A+ en la prueba de SSLQualys, se debe agregar la siguiente cabecera al Server 443:

add_header Strict-Transport-Security "max-age=63072000; includeSubDomains" always;

```
        add_header Strict-Transport-Security "max-age=31536000; includeSubDomain
s; preload" always;
```

Luego de un reinicio del servicio Nginx, el subdominio incluirá las cabeceras de HSTS en los paquetes que viajen desde el servidor.