Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.

**Summary of revistas.udca.edu.co:443 (HTTPS) SSL Security Test**

The server configuration supports only TLSv1.2 protocol, precluding users with older browsers from accessing your website.
## SSL Certificate Analysis

### RSA CERTIFICATE INFORMATION
- **Issuer**: Let's Encrypt Authority X3
- **Common Name**: revistas.udca.edu.co
- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
- **Subject Alternative Names**: DNS:revistas.udca.edu.co, DNS:udca.metarevistas.org
- **Validation Level**: DV
- **Valid From**: April 14th 2020, 01:00 CEST
- **Valid To**: July 13th 2020, 01:00 CEST

### CERTIFICATE CHAIN

#### DST Root CA X3
- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha1WithRSAEncryption
- **SHA256**: 0687260331a72403d909f105e69bcf0d32e1bd2493ff6d9206d11bcd6770739
- **PIN**: Vjs8r4z+80wjNcr1YKepWQboSIrI63WsWXhIMN+eWys=
- **Expires in**: 485 days

#### Let's Encrypt Authority X3
- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
- **SHA256**: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d
- **PIN**: YLh1dUR9y6Kja30RrAn7JKnbQQ/uEtLMkBF2Fu1hg=
- **Expires in**: 288 days

#### revistas.udca.edu.co
- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
<table>
<thead>
<tr>
<th>SHA256</th>
<th>aed059b8d949db514bd2a3af5e9ce0db2dcbff59772cca1cc5d51a2a61d1365d</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>ys7K5fwa0GxqaUnYs4TzLBw4kS5peO+PkXqChqLBQSM=</td>
</tr>
<tr>
<td>Expires in</td>
<td>40 days</td>
</tr>
</tbody>
</table>
## Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

### CERTIFICATES ARE TRUSTED

All the certificates provided by the server are trusted.  

**Good configuration**

### SUPPORTED CIPHERS

List of all cipher suites supported by the server:

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good configuration</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>

### SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLSv1.2</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>

### DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: **2048 bits**  

**Good configuration**

### SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

<table>
<thead>
<tr>
<th>Elliptic Curve</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-256 (prime256v1) (256 bits)</td>
<td>Good configuration</td>
</tr>
</tbody>
</table>

### POODLE OVER TLS

The server is not vulnerable to POODLE over TLS.  

**Not vulnerable**

### GOLDENDOODLE

The server is not vulnerable to GOLDENDOODLE.  

**Not vulnerable**

### ZOMBIE POODLE

The server is not vulnerable to Zombie POODLE.  

**Not vulnerable**

### SLEEPING POODLE

The server is not vulnerable to Sleeping POODLE.  

**Not vulnerable**

### 0-LENGTH OPENSSL

The server is not vulnerable 0-Length OpenSSL.  

**Not vulnerable**

### CVE-2016-2107

---
The server is not vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107).

**SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION**

The server does not support client-initiated insecure renegotiation.

**ROBOT**

The server is not vulnerable to ROBOT (Return Of Bleichenbacher's Oracle Threat) vulnerability.

**HEARTBLEED**

The server version of OpenSSL is not vulnerable to Heartbleed attack.

**CVE-2014-0224**

The server is not vulnerable to CVE-2014-0224 (OpenSSL CCS flaw).
## Test For Compliance With HIPAA Guidance

Reference: HIPAA of 1996. Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or IndecIPHERable to Unauthorized Individuals.

### X.509 Certificates Are in Version 3

All the X509 certificates provided by the server are in version 3.  

**Good configuration**

### Server Supports OCSP Stapling

The server supports OCSP stapling, which allows better verification of the certificate validation status.  

**Good configuration**

### Supported Protocols

List of all SSL/TLS protocols supported by the server:

**TLSv1.2**  

**Good configuration**

### Supported Ciphers

List of all cipher suites supported by the server:

**TLSv1.2**

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Good configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td></td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td></td>
</tr>
</tbody>
</table>

**Good configuration**

### Diffie-Hellman Parameter Size

Diffie-Hellman parameter size: **2048 bits**  

**Good configuration**

### Supported Elliptic Curves

List of all elliptic curves supported by the server:

<table>
<thead>
<tr>
<th>Elliptic Curve</th>
<th>Good configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-256 (prime256v1) (256 bits)</td>
<td></td>
</tr>
</tbody>
</table>

**Good configuration**

### EC_POINT_FORMAT Extension

The server supports the EC_POINT_FORMAT TLS extension.  

**Good configuration**
Test For Compliance With NIST Guidelines

Reference: NIST Special Publication 800-52 Revision 2 - Section 3

**X.509 CERTIFICATES ARE IN VERSION 3**

All the X509 certificates provided by the server are in version 3.  
Good configuration

**SERVER SUPPORTS OCSP STAPLING**

The server supports OCSP stapling, which allows better verification of the certificate validation status.  
Good configuration

**SUPPORTED CIPHERS**

List of all cipher suites supported by the server:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

**SUPPORTED PROTOCOLS**

List of all SSL/TLS protocols supported by the server:

- TLSv1.2

**DIFFIE-HELLMAN PARAMETER SIZE**

Diffie-Hellman parameter size: 2048 bits  
Good configuration

**SUPPORTED ELLIPTIC CURVES**

List of all elliptic curves supported by the server:

- P-256 (prime256v1) (256 bits)  
Good configuration

**SERVER DOES NOT SUPPORT OF TLSV1.3**

The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.  
Information

**SERVER DOES NOT SUPPORT EXTENDED MASTER SECRET**

The server does not support Extended Master Secret extension for TLS versions ≤ 1.2.  
Non-compliant with NIST guidelines

**EC_POINT_FORMAT EXTENSION**

The server supports the EC_POINT_FORMAT TLS extension.  
Good configuration
## Test For Industry Best-Practices

### DNSCAA
This domain does not have a Certification Authority Authorization (CAA) record.

### CERTIFICATES DO NOT PROVIDE EV
The RSA certificate provided is NOT an Extended Validation (EV) certificate.

### SERVER DOES NOT SUPPORT OF TLSV1.3
The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses.

### SERVER DOES NOT HAVE CIPHER PREFERENCE
The server does not prefer cipher suites. We advise to enable this feature in order to enforce usage of the best cipher suites selected.

### ALWAYS-ON SSL
The HTTP version of the website redirects to the HTTPS version.

### SERVER PROVIDES HSTS WITH LONG DURATION
The server provides HTTP Strict Transport Security for more than 6 months:

| 63072000 seconds |

### SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION
The server does not support client-initiated secure renegotiation.

### SERVER-INITIATED SECURE RENEGOTIATION
The server supports secure server-initiated renegotiation.

### SERVER DOES NOT SUPPORT TLS COMPRESSION
TLS compression is not supported by the server.