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

Summary of revistas.iber.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

<table>
<thead>
<tr>
<th><strong>Issuer</strong></th>
<th>Let's Encrypt Authority X3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Common Name</strong></td>
<td>iberoamericana.metarevistas.org</td>
</tr>
<tr>
<td><strong>Key Type/Size</strong></td>
<td>RSA 2048 bits</td>
</tr>
<tr>
<td><strong>Signature Algorithm</strong></td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td><strong>Subject Alternative Names</strong></td>
<td>DNS:arete.ibero.edu.co, DNS:horizontespedagogicos.ibero.edu.co, DNS:iberoamericana.metarevistas.org, DNS:reviberopsicologia.ibero.edu.co, DNS:revistas.ibero.edu.co, DNS:revistas.iberoamericana.edu.co, DNS:revmovimientocientifico.ibero.edu.co</td>
</tr>
<tr>
<td><strong>Transparency</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Validation Level</strong></td>
<td>DV</td>
</tr>
<tr>
<td><strong>CRL</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>OCSP</strong></td>
<td><a href="http://ocsp.int-x3.letsencrypt.org">http://ocsp.int-x3.letsencrypt.org</a></td>
</tr>
<tr>
<td><strong>OCSP Must-Staple</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Valid From</strong></td>
<td>March 4th 2020, 04:58 CET</td>
</tr>
<tr>
<td><strong>Valid To</strong></td>
<td>June 2nd 2020, 05:58 CEST</td>
</tr>
</tbody>
</table>

#### CERTIFICATE CHAIN

**DST Root CA X3**

- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha1WithRSAEncryption
- **SHA256**: 0687260331a72403d909f105e69bcf0d32e1bd2493ff6d9206d11bcd6770739
- **PIN**: Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhlMN+eWys=
- **Expires in**: 485 days

**Let's Encrypt Authority X3**

- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
- **SHA256**: 25847d668eb4f04fd4d0b12b6b0740c567da7d024308eb6c2c96fe41d9de218d
- **PIN**: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgfFF2Uihg=
- **Expires in**: 288 days

**iberoamericana.metarevistas.org**

- **Key Type/Size**: RSA 2048 bits
- **Signature Algorithm**: sha256WithRSAEncryption
- **SHA256**: 
- **PIN**: 
- **Expires in**:
<table>
<thead>
<tr>
<th>Key Type/Size</th>
<th>RSA 2048 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Algorithm</td>
<td>sha256WithRSAEncryption</td>
</tr>
<tr>
<td>SHA256</td>
<td>a857df5ba1c51a4d1af7b5b4328953d65bf8781717d1d2e121303b3ad13cfa6d</td>
</tr>
<tr>
<td>PIN</td>
<td>PcJKolLrnKReGuMBadZ48nNf/Ual6ynDDEFiutm1ESA=</td>
</tr>
<tr>
<td>Expires in</td>
<td>0 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 config</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good config</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>Good config</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>Good config</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 config</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 config</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.

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

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

- **TLSv1.2**

### Supported Ciphers
List of all cipher suites supported by the server:

- **TLSv1.2**
  - 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

### Diffie-Hellman Parameter Size
Diffie-Hellman parameter size: **2048 bits**

### Supported Elliptic Curves
List of all elliptic curves supported by the server:

- **P-256 (prime256v1) (256 bits)**

### EC_POINT_FORMAT Extension
The server supports the EC_POINT_FORMAT TLS extension.
# 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:

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

## 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 | Good configuration |

**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.  

---