



**XVI JORNADAS  
STIC CCN-CERT**

**IV JORNADAS  
DE CIBER\_  
DEFENSA:  
ESPDEF-CERT**

# Evolucionando la Evaluación Criptográfica



**UN CIBERESCUDO  
ÚNICO PARA ESPAÑA**



## JOSÉ RUIZ GUALDA

*jtsec Beyond IT Security*

[jruiz@jtsec.es](mailto:jruiz@jtsec.es)

- Ingeniero en Informática (Universidad de Granada)
- Experto en Common Criteria, LINCE y FIPS 140-2 & FIPS 140-3
- Miembro del SCCG (Stakeholder Cybersecurity Certification Group) en la Comisión Europea
- Secretario del SC3 en CTN320
- Editor de LINCE como norma UNE
- Editor en JTC13 WG3 de la Metodología FITCEM
- Revisor de la Comisión Europea para el grupo ERNCIP "Certificación de Ciberseguridad IACS"



## JUAN MARTÍNEZ ROMERO

*jtsec Beyond IT Security*

[jmartinez@jtsec.es](mailto:jmartinez@jtsec.es)

- Ingeniero en Tecnologías de Telecomunicación (Universidad de Granada)
- Máster en Ciberseguridad (Universidad de Granada)
- Crypto Manager & Senior Cybersecurity Consultant
- Experto en FIPS 140-2, FIPS 140-3 y PCI-PTS, entre otras metodologías
- CriptoCert Certified Crypto Analyst

# ÍNDICE

01



Introducción

02



Historia de la Evaluación  
Criptográfica

03



Actualidad de la Evaluación  
Criptográfica

04



Metodología de Evaluación  
Criptográfica

05



Herramienta de Evaluación  
Criptográfica

06



Conclusiones

# INTRODUCCIÓN

## ¿Qué es la criptografía?

"Arte de escribir con clave secreta o de un modo enigmático."  
 La criptografía es el **ámbito de la criptología** encargado del estudio de los algoritmos, protocolos y sistemas empleados para **dotar de seguridad** a las comunicaciones, a la información y entidades que se comunican.

## Propiedades criptográficas

- Confidencialidad
- Integridad
- Autenticación
- No repudio

La criptografía es una **solución de ciberseguridad ideal para garantizar la seguridad de la información.**



# HISTORIA DE LA EVALUACIÓN CRIPTOGRÁFICA

USA

**NIST** (National Institute of Standards and Technology)

- Verificación de la Conformidad según FIPS 140-1, FIPS 140-2 y FIPS 140-3
  - CMVP - Diseñado para certificar módulos criptográficos
  - CAVP - Diseñado para certificar algoritmos criptográficos
- Publicación de múltiples "Special Publications" especificando algoritmos criptográficos y como probarlos.



ACVP

# HISTORIA DE LA EVALUACIÓN CRIPTOGRÁFICA

Internacional



# HISTORIA DE LA EVALUACIÓN CRIPTOGRÁFICA

España

Organismo de certificación de módulos criptográficos – OC-CCN (Centro Criptológico Nacional)

Organismo de Certificación / Centro Criptológico Nacional

**OC-CCN**

CRITERIOS Y METODOLOGÍAS

Criterios y metodologías de evaluación de los sistemas en uso del Organismo de Certificación

**Sistemas CCNets**

- OC-CCN v1.1 - Hoja de Ruta y Criterios de Evaluación de Seguridad
  - OC-CCN v1.1 - Hoja de Ruta - 1. Metodología de Evaluación de Seguridad v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 2. Seguridad de los Sistemas de Información v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 3. Seguridad de los Sistemas de Información v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 4. Seguridad de los Sistemas de Información v1.1 (2017-18)
- OC-CCN v1.1 - Hoja de Ruta
  - OC-CCN v1.1 - Hoja de Ruta - 1. Metodología de Evaluación de Seguridad v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 2. Seguridad de los Sistemas de Información v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 3. Seguridad de los Sistemas de Información v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 4. Seguridad de los Sistemas de Información v1.1 (2017-18)

**OC-CCN - Certificación Nacional de Seguridad**

- Certificación Nacional de Seguridad (CNS) versión 1.0
  - OC-CCN v1.1 - Hoja de Ruta - 1. Metodología de Evaluación de Seguridad v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 2. Seguridad de los Sistemas de Información v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 3. Seguridad de los Sistemas de Información v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 4. Seguridad de los Sistemas de Información v1.1 (2017-18)
- Certificación Nacional de Seguridad (CNS) versión 1.1
  - OC-CCN v1.1 - Hoja de Ruta - 1. Metodología de Evaluación de Seguridad v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 2. Seguridad de los Sistemas de Información v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 3. Seguridad de los Sistemas de Información v1.1 (2017-18)
  - OC-CCN v1.1 - Hoja de Ruta - 4. Seguridad de los Sistemas de Información v1.1 (2017-18)

La metodología CNS se orienta a la evaluación y certificación de productos de seguridad TIC de uso común en el ámbito OTIC, como productos certificados para sistemas operativos por el IEC con categoría media o alta y también se puede aplicar para la realización de Evaluaciones de Seguridad de Productos de Información y la certificación de los productos OTIC y OTIC de alta y media categoría.

**ISO 15700**

- ISO 15700:2007 Security Requirements for Cryptographic Modules
- ISO 15700:2007 Security Requirements for Cryptographic Modules

**ISO**

- ISO 15700:2007 Security Requirements for Cryptographic Modules
- ISO 18045:2015 Test Requirements for Cryptographic Modules

**ISO**

- ISO 15700:2007 Security Requirements for Cryptographic Modules
- ISO 18045:2015 Test Requirements for Cryptographic Modules

# ACTUALIDAD DE LA EVALUACIÓN CRIPTOGRÁFICA

Europa

SOG-IS Crypto Evaluation Scheme  
Harmonised Cryptographic Evaluation  
Procedures v0.16 (Diciembre 2020)

- Primera metodología de evaluación de SOG-IS
  - Implementación de mecanismos criptográficos
  - Requisitos para Prevención de Pitfalls

SOG-IS HEP



SOG-IS Crypto Evaluation Scheme Agreed  
Cryptographic Mechanisms v1.2 (Enero  
2020)

- Mecanismos criptográficos acordados y recomendados por SOG-IS
  - Nivel de seguridad aceptable
  - Indicaciones de implementación

SOG-IS ACM



# ACTUALIDAD DE LA EVALUACIÓN CRIPTOGRÁFICA

España

## Guía CCN-STIC 130

Guía Requisitos Evaluación Criptológica (DL)  
(Octubre 2017)

- Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada
  - Enfoque similar a FIPS
  - Requisitos de seguridad



Guía CCN-STIC 130

## MEC – LINCE

Módulo de evaluación Criptográfica dentro  
la metodología LINCE

- Pruebas muy ligeras de conformidad criptográfica siguiendo la aproximación de los Perfiles de Protección del NIAP



## Botan-CCN Cryptographic Library

Implementación de referencia para  
evaluaciones criptográficas del CCN



# ACTUALIDAD DE LA EVALUACIÓN CRIPTOGRÁFICA

España

## Guía CCN-STIC 807

Criptología de empleo en el Esquema Nacional de Seguridad (Mayo 2022)

- Mecanismos criptográficos autorizados para su uso en el ENS
  - Fortaleza requerida según el nivel de seguridad
  - Protocolos Criptográficos
  - Requisitos para Prevención de Pitfalls



Guía CCN-STIC 807

## Guía CCN-STIC 221

Mecanismos Criptográficos Autorizados por el CCN (Pendiente de Publicación)

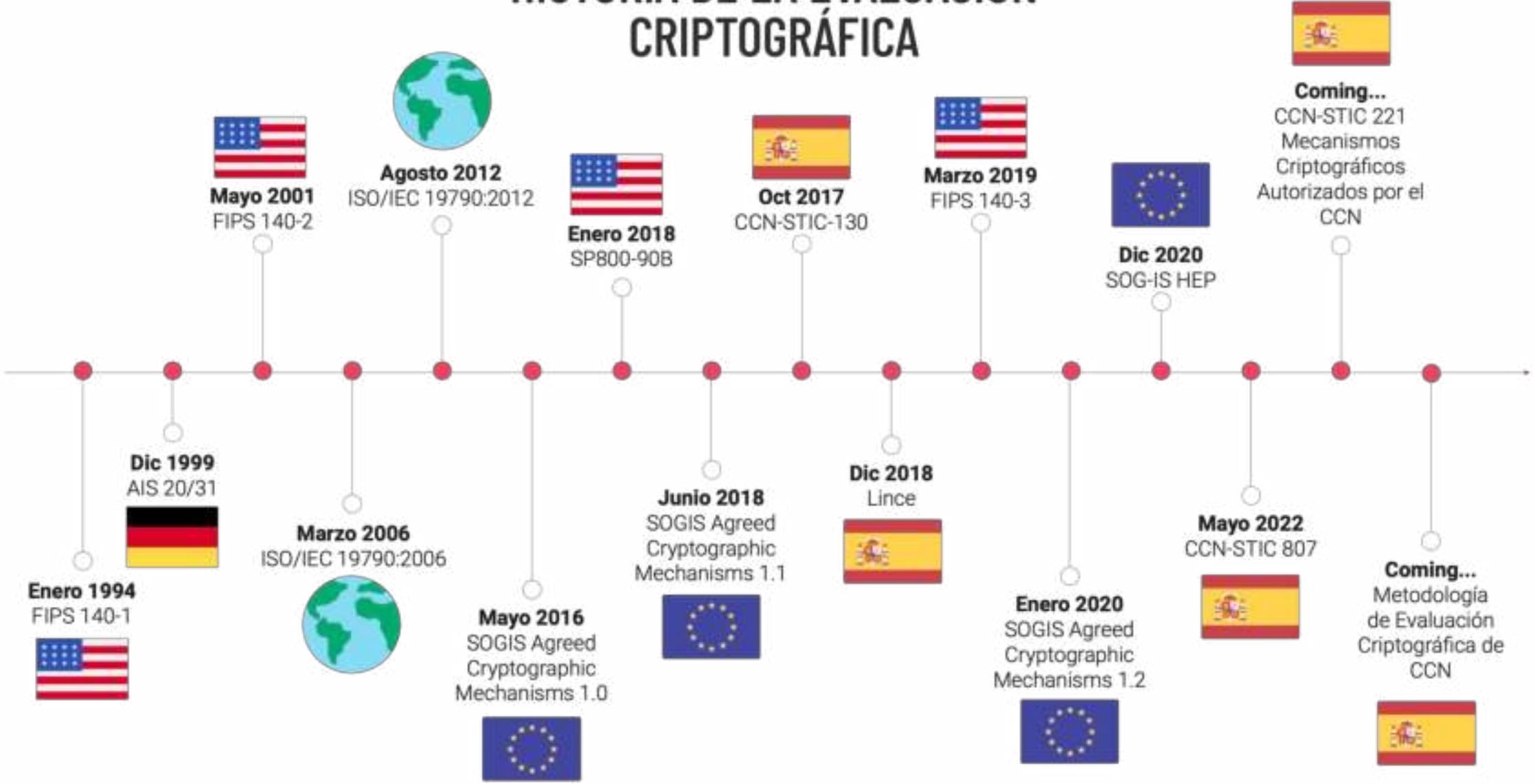
- Mecanismos criptográficos autorizados por CCN
  - Inclusión de nuevos algoritmos autorizados por CCN respecto al ACM europeo.
  - Guía de uso transversal no limitada al ENS

NUEVO



Guía CCN-STIC 221

# HISTORIA DE LA EVALUACIÓN CRIPTOGRÁFICA



# ACTUALIDAD DE LA EVALUACIÓN CRIPTOGRÁFICA

## ¿Problemática a nivel nacional?

Razones por las que es necesaria esta metodología criptográfica

### FIPS y/o ISO FIPS

- Solo funciona cuando el módulo se ha creado para cumplir los requisitos de FIPS.
- No funciona bien en productos que integran criptografía pero no usan un módulo criptográfico de un tercero.
- No se verifican errores de implementación que afecten a la seguridad ni valores límites. Es decir, las pruebas son muy de conformidad.



### STIC 130

- No incluye conformidad a nivel de algoritmos e incluye requisitos de implementación de producto,
- No está 100% focalizada en la implementación criptográfica.
- Aporta el punto de vista de seguridad



STIC 130

No tenemos una metodología que evalúe algoritmos y protocolos criptográficos.

# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Uso

Metodología de Evaluación Criptográfica de CCN

- Productos cuya funcionalidad principal requiera de criptografía (ej.- VPN, cifradores, comunicaciones seguras, etc...)
- Durante procesos de certificación CC, LINCE y STIC Complementaria



# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Definición

Metodología de Evaluación Criptográfica de CCN  
• Estructura del Documento

**DRAFT**



# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 1. Requisitos Criptográficos

**Objetivo:** Especificar los requisitos extraídos por CCN de la guía CCN-STIC 130 que aplican a la seguridad de los productos criptográficos en relación a los mecanismos y primitivas criptográficas implementadas en relación a:

- Implementación de algoritmos aprobados
- KATs (Know Answer Tests)
- Self-tests
- Gestión de parámetro críticos de la seguridad (PCS)

**Evaluación:** El evaluador deberá verificar que los el TOE cumple con los requisitos criptográficos recogidos en esta sección.



# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 2. Mecanismos Criptográficos Aprobados

Objetivo: Especificar los mecanismos criptográficos reconocidos y acordados por los participantes del Esquema de Evaluación Criptográfica de SOG-IS.

Evaluación: El evaluador deberá verificar que los mecanismos criptográficos implementados por el TOE cumplen con las directrices presentadas por el SOG-IS en la guía SOG-IS Agreed Cryptographic Mechanisms.



Guía CCN-STIC 221

# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 3. Pruebas de Conformidad de Algoritmos

**Objetivo:** Especificar los requisitos necesarios para la realización de las pruebas de conformidad de los mecanismos y primitivas criptográficas implementadas por el TOE. Estas pruebas determinarán si los mecanismos y primitivas criptográficas empleados por el TOE se han implementado de forma adecuada, de manera similar a lo realizado por el NIST, pero verificando además, parametrizaciones y valores límite que suelen inducir a error.

**Evaluación:** El proceso de evaluación se divide en cuatro fases:

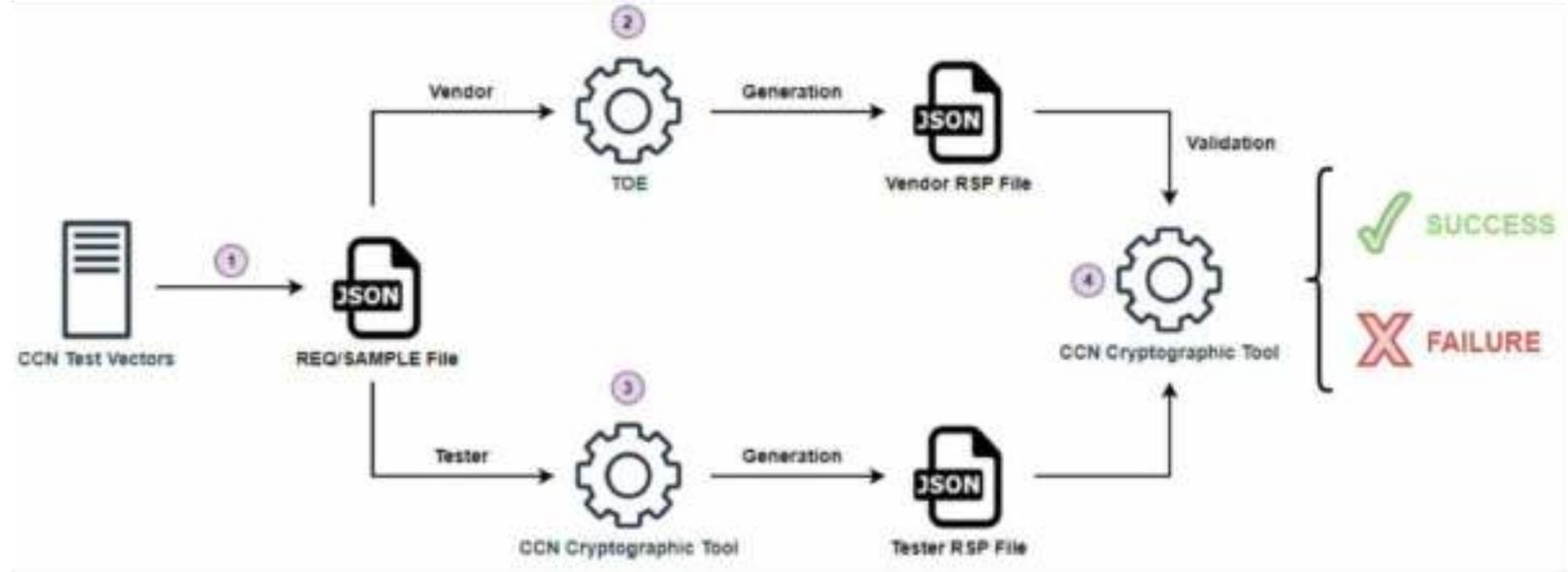
1. Generación de Vectores de Prueba: Ficheros Request y Sample
2. Generación de Resultados por parte del Fabricante: Fichero Response
3. Generación de Resultados por parte del Evaluador: Fichero Response
4. Validación de Resultados por parte del Evaluador



# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 3. Pruebas de Conformidad de Algoritmos

Diagrama del Proceso de Evaluación de las Pruebas de Conformidad



# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 3. Pruebas de Conformidad de Algoritmos

### Generación de Vectores de Prueba

- El evaluador deberá generar un fichero 'REQUEST' (en formato JSON) para cada mecanismo criptográfico implementado por el TOE que contendrá los vectores de test asociados a la parametrización soportada.
- Adicionalmente, el evaluador generará el fichero 'SAMPLE' (en formato JSON) para cada mecanismo criptográfico implementado por el TOE que contendrá una solución de ejemplo para indicar el formato del resultado esperado.

El evaluador deberá enviar al fabricante un paquete de archivos que contenga los ficheros 'REQUEST' y 'SAMPLE' asociados a todos los mecanismos criptográficos implementados por el TOE.



REQUEST



SAMPLE

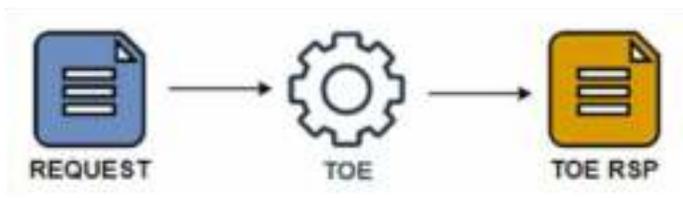
# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 3. Pruebas de Conformidad de Algoritmos

### Generación de Resultados por parte del Fabricante

- El fabricante deberá generar un fichero 'RESPONSE' asociado a cada mecanismo criptográfico implementado, que contendrá la salida proporcionada por el TOE para cada uno de los vectores de test proporcionados en el fichero 'REQUEST'.
- El fabricante deberá conservar el formato JSON presentado en los ficheros 'REQUEST' y 'SAMPLE' para la generación del fichero 'RESPONSE'.

El fabricante deberá enviar al evaluador un paquete de archivos que contenga los ficheros 'RESPONSE' asociados a todos los mecanismos criptográficos implementados por el TOE.



# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 3. Pruebas de Conformidad de Algoritmos

### Generación de Resultados por parte del Evaluador

- El evaluador deberá generar el fichero 'RESPONSE' asociado a cada mecanismo criptográfico implementado por el TOE, empleando la librería Botan-CCN como implementación criptográfica de referencia.
- El evaluador deberá conservar el formato JSON presentado en los ficheros 'REQUEST' y 'SAMPLE' para la generación del fichero 'RESPONSE'.

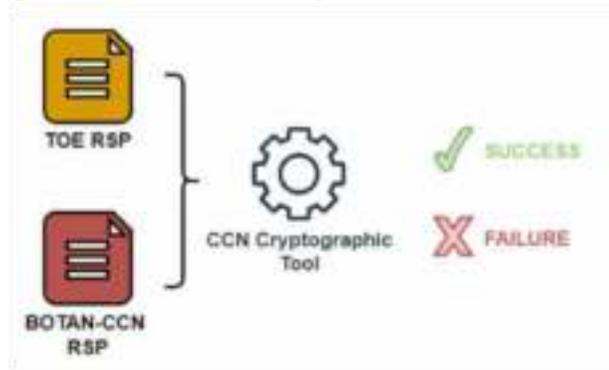


# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 3. Pruebas de Conformidad de Algoritmos

### Validación de Resultados por parte del Evaluador

- El evaluador deberá validar los ficheros 'RESPONSE' proporcionados por el fabricante para cada mecanismo criptográfico implementado por el TOE, comparando los resultados proporcionados con los obtenidos en la fase anterior empleando la librería criptográfica Botan-CCN.
- El evaluador determinará si el TOE implementa correctamente los mecanismos y primitivas criptográficas empleadas y declaradas.





# METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

## Estructura / 4. Errores Comunes de Implementación

**Objetivo:** Especificar los requisitos necesarios para evitar errores de implementación en los mecanismos y primitivas criptográficas implementados por el TOE.

**Evaluación:** El evaluador deberá verificar que los mecanismos criptográficos implementados por el TOE cumplen con las directrices para evitar errores de implementación presentadas por el SOG-IS en la guía SOG-IS Harmonised Cryptographic Evaluation Procedures.

### EJEMPLO:

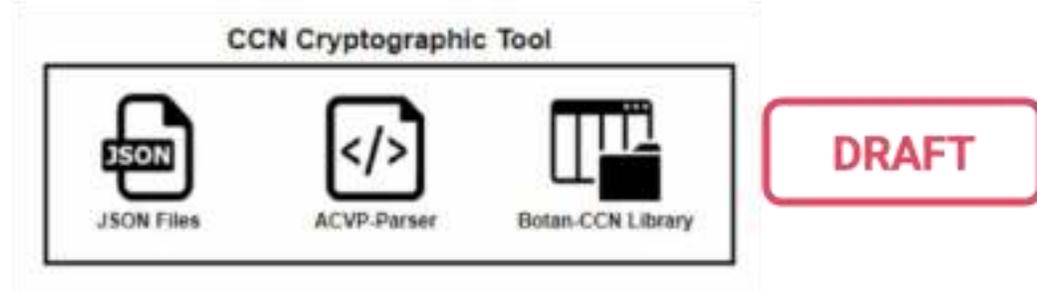
El evaluador deberá verificar que un IV nunca puede ser reutilizado en el cifrado con la misma clave para diferentes entradas

# HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

## Definición

### Herramienta de Evaluación Criptográfica de CCN

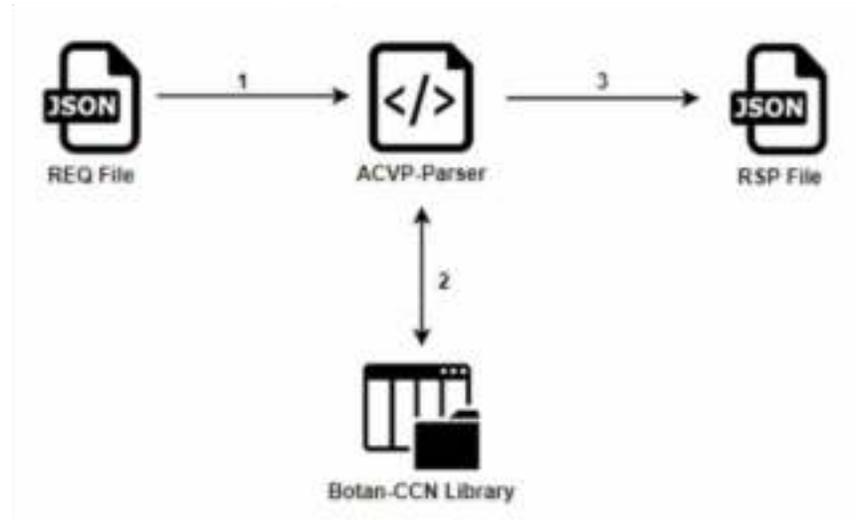
- Realización de Pruebas de Conformidad
- Estructura de la Herramienta
  - Ficheros de test JSON: vectores de test en formato hexadecimal de acuerdo a la metodología de SOG-IS.
  - ACVP-Parser: procesamiento de ficheros JSON y extracción de parámetros necesarios para invocar a la implementación criptográfica de referencia.
  - Botan-CCN Cryptographic Library: implementación criptográfica de referencia empleada para la generación de resultados de los vectores de test y la validación de la correcta implementación criptográfica del TOE.



# HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

## Diagrama de Flujo

1. Procesado de los vectores de tests para extraer los parámetros empleando el ACVP-Parser.
2. Invocación de la librería criptográfica Botan-CCN para realizar la generación de resultados de los vectores de tests haciendo uso del fichero 'REQUEST' asociado.
3. Generación de fichero 'RESPONSE' asociado a un mecanismos criptográfico empleando el fichero 'REQUEST' asociado y los resultados obtenidos empleando la librería criptográfica Botan-CCN.



# HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

## Ejemplo de Uso: SHA-256

```

1 CCN-SHA256_KAT.req.json X
2
3 {
4   "Version": "1.0"
5 }
6 {
7   "vsId": 0,
8   "algorithm": "SHA2-256",
9   "revision": "1.0",
10  "isSample": false,
11  "testGroups": [
12    {
13      "tgId": 1,
14      "testType": "KAT",
15      "tests": [
16        {
17          "tcId": 1,
18          "msgLen": 256,
19          "msg": "89fc1acc238a285e4a208e04a8f204291f581a12756353da4b8c0cf5ef82b95"
20        },
21        {
22          "tcId": 2,
23          "msgLen": 256,
24          "msg": "32f4b27186c38ba9e9359a3c41475207a98ade99569e5bb72f06161e989798b"
25        }
26      ]
27    }
28  ]
29 }

```

Fichero 'REQUEST'

```

1 CCN-SHA256_KAT.rsp.json X
2
3 {
4   "Version": "1.0"
5 }
6 {
7   "vsId": 0,
8   "algorithm": "SHA2-256",
9   "revision": "1.0",
10  "isSample": false,
11  "testGroups": [
12    {
13      "tgId": 1,
14      "testType": "KAT",
15      "tests": [
16        {
17          "tcId": 1,
18          "msgLen": 256,
19          "msg": "89fc1acc238a285e4a208e04a8f204291f581a12756353da4b8c0cf5ef82b95",
20          "wd": "4f44c1c7fb6bb6f9681829f3897bfd950c56fa07844be76489676356ac1888a4"
21        },
22        {
23          "tcId": 2,
24          "msgLen": 256,
25          "msg": "32f4b27186c38ba9e9359a3c41475207a98ade99569e5bb72f06161e989798b",
26          "wd": "b48289998871561d7ffda28a955f296e3e237800d6dffe3a8de94d8ba757c743"
27        }
28      ]
29    }
30  ]
31 }

```

Fichero 'RESPONSE' generado por la Herramienta

# HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

Ejemplo de Uso: SHA-256

```

Vendor_CCN-SHA256_KAT.rsp.json
Vendor_CCN-SHA256_KAT.rsp.json | testgroups | | | | tests | | | | md
1
2
3   "Version": "1.0"
4
5
6   "vsId": 0,
7   "algorithm": "SHA-256",
8   "revision": "1.0",
9   "isSample": false,
10  "testgroups":
11
12    "tgId": 1,
13    "testType": "KAT",
14    "tests":
15
16      "tcId": 1,
17      "msgLen": 256,
18      "msg": "99f31acc238205c40708d4872847911501e11726357da96c075e07099",
19      "md": "4f44c1c7fb6b6f961829f3897b70056c50f6078440e70489870350ac1886a4"
20
21      PASS
22
23      "tcId": 2,
24      "msgLen": 256,
25      "msg": "32f4b27186c30ba6ea9359a2c414f5787a98ed9569e56b72f09181e997980",
26      "md": "b4d29999071501d17182ba957298c52237896d6d1fcaab8e94d0ea757c743"
27
28      PASS
29
30
31

```

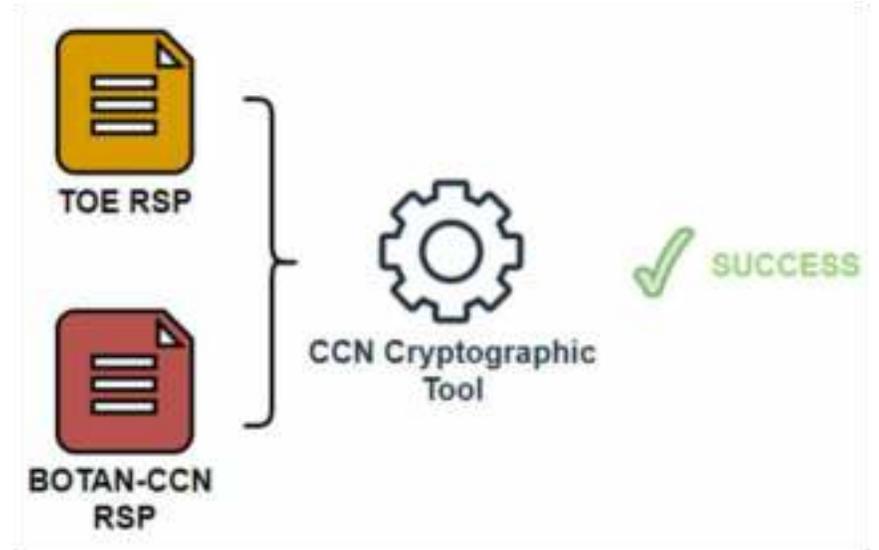
Fichero 'RESPONSE' generado por el TOE

```

~/Desktop/acvpparser-master
./acvp-parser -e CCN-SHA256_KAT.rsp.json Vendor_CCN-SHA256_KAT.rsp.json -x
[PASSED] compare CCN-SHA256_KAT.rsp.json with Vendor_CCN-SHA256_KAT.rsp.json

```

Validación de resultados



# HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

Ejemplo de Uso: SHA-256

```

Vendor_CCN-SHA256_KAT.rsp.json X
{} Vendor_CCN-SHA256_KAT.rsp.json 7 ...
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
  
```

```

{
  "Version": "1.0",
  "valid": 0,
  "algorithm": "SHA2-256",
  "revision": "1.0",
  "isSample": false,
  "testGroups": [
    {
      "tgId": 1,
      "testType": "KAT",
      "tests": [
        {
          "tcId": 1,
          "msgLen": 256,
          "msg": "89f1acc0c378a705e4a208ed4a87204291f981a12756392de466c0cf3ef02b95",
          "md": "4744c1e77hebb67he0107970937ef9030c96fab7044be76489076356c1880a4"
        }
      ]
    },
    {
      "tcId": 2,
      "msgLen": 256,
      "msg": "32f4b27106c300a90ea9359a2c414f5267a06adoe950e5be72f00161e909790b",
      "md": "048209990071501d7ff8a28a935f29de3e237006d6d7fe3a1de94de0a757c743"
    }
  ]
}
  
```

PASS

FAIL

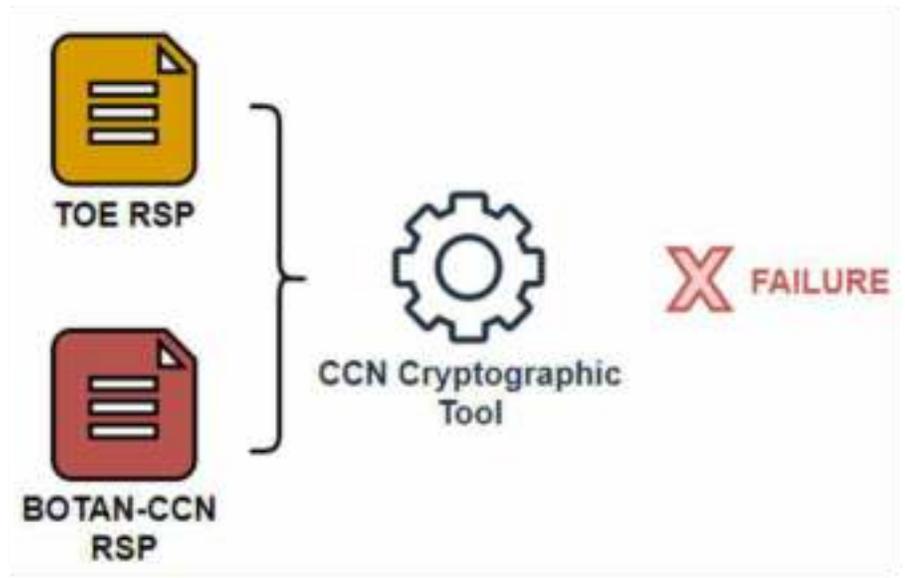
ERROR

Fichero 'RESPONSE' generado por el TOE

```

[~/Desktop/acvpparser-master]
$ ./acvp-parser -o CCN-SHA256_KAT.rsp.json Vendor_CCN-SHA256_KAT.rsp.json
[FAILURE] compare CCN-SHA256_KAT.rsp.json with Vendor_CCN-SHA256_KAT.rsp.json
  
```

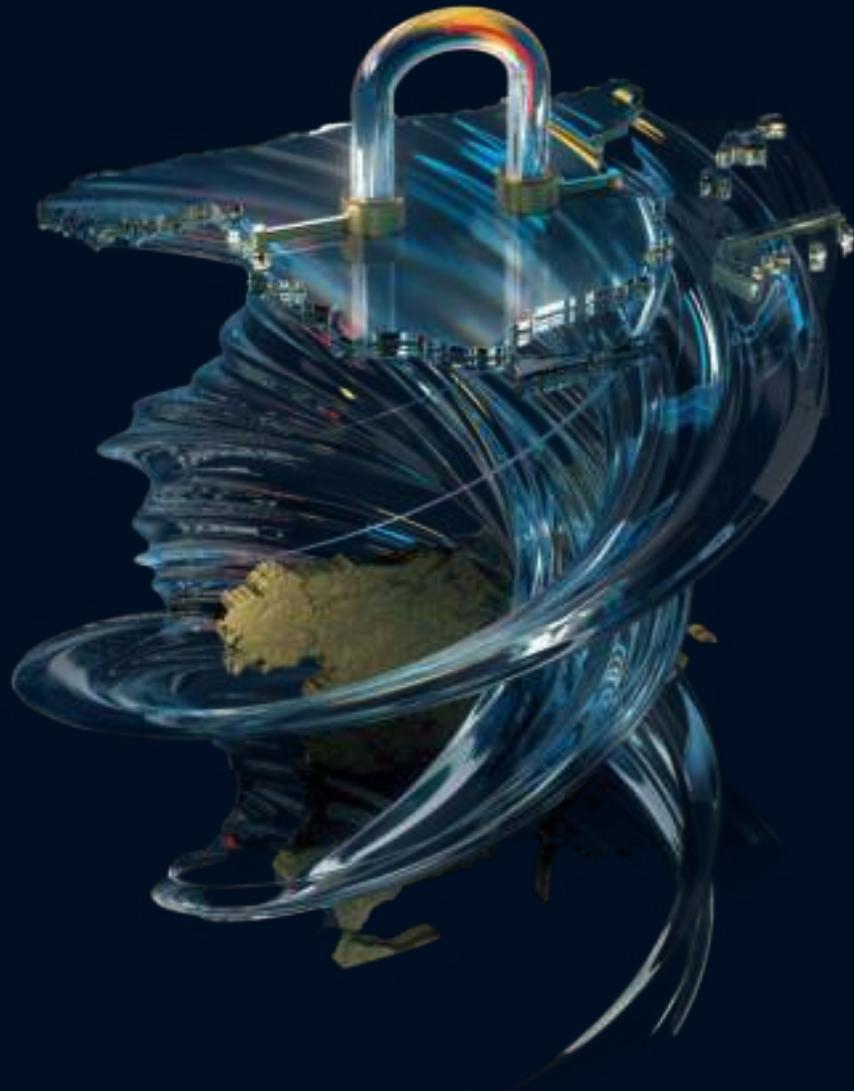
Validación de resultados



## CONCLUSIONES

- España es pionera en:
  - La creación de una metodología de evaluación criptográfica
  - La creación de una herramienta de validación de la conformidad de los algoritmos
- Contribución para complementar los esfuerzos europeos
- Resulta necesario y lógico unificar criterios en el sector para facilitar la vida a laboratorios y fabricantes.





# MUCHAS GRACIAS



UN CIBERESCUDO  
ÚNICO PARA ESPAÑA