NORMATIVA DE GESTIÓN DE CLAVES CRIPTOGRÁFICAS

AYUNTAMIENTO DE MARTOS

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DEL

AYUNTAMIENTO DE MARTOS

Cuadro de Control

Título:	Normativa de Gestión de Claves Criptográficas		
Tipo de documento:	Normativa		
Nombre del Fichero:	NOS-011 Normativa de gestión de claves criptográficas.docx		
Clasificación:	Uso Interno		
Estado:	Documento		
Autor:	Consultor Externo		
Versión:	1.0	**Fecha:**	01-09-2016

Revisión y aprobación			
Revisado por:	Responsable de Seguridad		
Aprobado por:	Comité de Seguridad	**Fecha:**	22-03-2017

Lista de distribución	

Control de Cambios

Versión	Fecha	Autor	Descripción del Cambio

INDICE

1. OBJETO

El objeto del presente documento es la definición de la normativa aplicable a la Gestión de Claves Criptográficas empleadas de Ayuntamiento de Martos (en adelante, la Organización), dentro del alcance señalado en el Esquema Nacional de Seguridad.

Se ha implantado la presente normativa atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la Organización, que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

2. ALCANCE

Esta normativa es de aplicación a todo el ámbito de actuación de la Organización, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de la Organización.

La normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el la Organización, especialmente, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean Usuarios de los Sistemas de Información de la Organización.

3. LEGISLACIÓN Y NORMATIVA APLICABLE

Las referencias tenidas en cuenta para la redacción de este Procedimiento han sido:

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Ley 15/1999, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD.
- Documentos y Guías CCN-STIC.

4. CUERPO DEL DOCUMENTO

En la presente normativa se presentan los algoritmos criptográficos que han sido acreditados para el uso en los sistemas que forman parte del alcance del Esquema Nacional de Seguridad, cuando sus características y requerimientos se consideren necesarios.

La siguiente relación de algoritmos y protocolos criptográficos se consideran acreditados por el CCN para su uso dentro del ENS, siempre que se realice una implementación correcta de los mismos:

- Cifrado simétrico: AES, TDEA (3DES).

- Protocolos de acuerdo de clave: DH o DHKA, MQV, ECDH, ECMQV.
- Algoritmos asimétricos: RSA, DSA, ECDSA, ECIES.
- Funciones resumen: SHA (preferentemente SHA-2), HMAC.

4.1. Mecanismos de identificación

Concepto. Se entiende por identificación la comprobación de la identidad de una entidad, ya sea ésta una persona, un terminal, un proceso, una tarjeta, etc.

Con el fin de que toda entidad sea convenientemente identificada, cada una de ellas tendrá asignado un identificador único de modo que en cada momento se pueda tener conocimiento de quién ha hecho qué cosa.

Ejemplo. Pueden servir de identificadores únicos el número del DNI, el número del pasaporte, el carnet de conducir, una secuencia de caracteres numéricos o alfanuméricos, un certificado digital, tarjetas de identidad emitidas por el organismo que controle el acceso, etc. También se considerarán mecanismos válidos las tarjetas numeradas de visitantes, siempre que la persona poseedora de la misma haya pasado previamente por un control de acceso donde haya sido identificada mediante alguno de los mecanismos ya citados.

Elementos.

- Para la verificación de los derechos que posee la entidad, deberá existir una base de datos segura que permita validar en todo momento dichos derechos.
- Si se emplea un certificado digital, éste tendrá que utilizar en su firma digital una función resumen cuya seguridad sea mayor o igual a la función SHA-1 o, preferiblemente, cualquiera de la serie SHA-2.
- En el caso de que los caracteres numéricos o alfanuméricos a emplear sean obtenidos de forma aleatoria, éstos deberán ser generados con la suficiente seguridad como para evitar repeticiones o hipótesis acerca de su posible valor.

4.2. Mecanismos de autenticación

Concepto. Un mecanismo de autenticación es un proceso por el que una parte se asegura, mediante la obtención de una evidencia, de la identidad de una segunda parte que está implicada en un protocolo y en la que dicha segunda parte ha participado, es decir, la segunda parte participa activamente en el momento preciso o justo antes de que se adquiera la evidencia.

En general, los mecanismos de autenticación se basan en el uso de tres posibles propiedades o características de la parte que ha de ser autenticada:

- algo que sabe (por ejemplo, una clave),
- algo que se tiene (una tarjeta inteligente o un dispositivo físico son ejemplos de esta característica)
- algo que se es (un rasgo o propiedad biométrica, fisonomía facial, la huella digital, el patrón de iris, etc.).

Niveles. Para los mecanismos de autenticación se consideran tres niveles de seguridad: bajo, medio y alto.

Nivel bajo

Para el nivel bajo se admite cualquier mecanismo de autenticación, ya sean claves concertadas (se entiende por clave concertada una ristra de bits que no hay forma de memorizar), contraseñas (se entiende por contraseña números de identificación personal –PIN– de al menos 4 dígitos o caracteres), dispositivos físicos (en inglés, tokens, dongles), dispositivos software como certificados digitales y procesos basados en biometría.

Con el fin de evitar posibles ataques por fuerza bruta, se recomienda la utilización de políticas de bloqueo de contraseñas, de modo que después de determinado número de intentos fallidos (se recomiendan hasta tres intentos) el acceso mediante contraseña quede bloqueado o métodos de retardo de solicitud de contraseña. Para ello, las claves deben ser suficientemente complejas y seguras para resistir ataques de fuerza bruta:

Nivel medio

Los mecanismos de autenticación admitidos para el nivel medio son, también, dispositivos físicos, dispositivos software como certificados digitales y procesos basados en biometría. No está aconsejado el uso de claves concertadas, en el caso de utilización se permitirán aquellas que estén formadas de al menos 8 caracteres alfanuméricos. Si estos últimos son generados de forma aleatoria o pseudoaleatoria, deberán poseer la suficiente seguridad como para evitar repeticiones o hipótesis acerca de su posible valor.

De nuevo, para evitar posibles ataques por fuerza bruta, se recomienda la utilización de políticas de bloqueo de contraseñas, de modo que después de determinado número de intentos fallidos (se recomiendan hasta tres intentos) el acceso mediante contraseña quede bloqueado o métodos de retardo de solicitud de contraseña.

Nivel alto

Para el nivel alto, los mecanismos de autenticación se basarán en dispositivos físicos personalizados o mediante dispositivos que hagan uso de patrones biométricos. En el caso de utilizar un patrón biométrico se requerirá la utilización de un segundo factor de autenticación token o clave segura (generada de forma aleatoria y con una longitud de al menos 8 caracteres alfanuméricos).

En caso de utilizar claves concertadas, deberán implantarse las medidas de seguridad más restrictivas en cuanto a robustez y longitud.

Son aceptables los siguientes sistemas de autenticación: RADIUS, TLS, EAP, WPA, KERBEROS.

A fin de evitar posibles ataques por fuerza bruta, se recomienda la utilización de políticas de bloqueo de contraseñas, de modo que después de determinado número de intentos fallidos (se recomiendan hasta tres intentos) el acceso mediante contraseña quede bloqueado o métodos de retardo de solicitud de contraseña.

	NIVEL BAJO	NIVEL MEDIO	NIVEL ALTO
Con número limitado de intentos	≥ 4 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~24 bits	≥ 5 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~30 bits	≥ 6 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~36 bits
sin límite en el número de intentos	≥ 8 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~48 bits	≥ 10 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~60 bits	≥ 12 caracteres alfanuméricos del conjunto A-Z a-z 0-9 ~72 bits
	< 1 año de validez	< 180 días de validez	< 90 días de validez

4.3. Mecanismos de protección de la confidencialidad

La confidencialidad de una información consiste en mantener dicha información secreta para todos salvo para los autorizados a conocerla.

Nivel bajo

No aplica.

Nivel medio

Para mantener la confidencialidad de la información en el nivel medio se utilizarán redes privadas virtuales, en particular se hará uso de IPsec, SSL v3 y TLS.

IPsec es un protocolo, que posibilita proteger las comunicaciones sobre una red IP, de modo que cada uno de los paquetes de datos que se transmite es cifrado y autenticado. Dado que IPsec incluye protocolos para el establecimiento de claves de cifrado, éstas deberán garantizar, para este nivel medio, una seguridad equivalente a 112 bits.

Por su parte, SSL y su sucesor TLS, son protocolos criptográficos que proporcionan autenticidad y privacidad en una red, es decir, comunicaciones seguras, haciendo uso de métodos criptográficos. En general, en estos protocolos únicamente se autentica el servidor, quedando el cliente sin autenticar. Al igual que con IPsec, las claves que se utilicen en estos protocolos deberán tener un nivel de seguridad de 112 bits.

Un nivel de seguridad de 112 bits se traduce en claves de 112 bits (o superiores) para los sistemas de cifrado simétrico TDEA y AES, en claves de longitud 2048 bits (o superiores) para el criptosistema RSA y en claves de longitudes comprendidas entre los 224 y 255 bits para criptosistemas basados en curvas elípticas.

Nivel alto

En el nivel alto de protección de la información se emplearán, preferentemente, dispositivos hardware para el establecimiento y uso de la red privada virtual. Además, en este caso las claves a utilizar tienen que garantizar un nivel de seguridad de 128 bits.

Un nivel de seguridad de 128 bits supone el uso de claves de 128 bits (o superiores) para el sistema de cifrado simétrico AES y de claves de entre 256 y 283 bits para los sistemas basados en curvas elípticas.

Para el caso particular del criptosistema RSA, se permiten claves de 2048 bits, si bien se recomienda que la longitud de las claves sea mayor.

Resumen de protocolos aceptados:

Tipo	Nivel BAJO (opcional)	Nivel MEDIO	Nivel ALTO
secreto compartido TDEA AES	≥ 112 bits 112 o 168 128, 192 o 256	≥ 112 bits 112 o 168 128, 192 o 256	≥ 128 bits no 128, 192 o 256
clave pública RSA curvas elípticas	≥ 2.048 bits ≥ 224 bits	≥ 2.048 bits ≥ 224 bits	≥ 2.048 bits ≥ 256 bits

4.4. Mecanismos de protección de la autenticidad e integridad

Concepto.

Se entiende por autenticidad de una información la corroboración de la fuente de la información, es decir, la verificación de que quien la elaboró o quien dice ser el remitente de la misma es quien dice ser.

Por su parte, la integridad de una información hace referencia a la comprobación de que la información recibida no ha sido alterada por entidades no autorizadas o por medios no conocidos.

Es frecuente que autenticidad, integridad y confidencialidad se traten de forma conjunta negociando los protocolos, los parámetros y las claves en la fase de establecimiento.

Nivel bajo

En el nivel bajo, se asegurará, al menos, la autenticidad del otro extremo de la comunicación antes de proceder al intercambio de información, de modo que se prevengan posibles ataques activos, que serán, como mínimo, detectados.

Se consideran ataques activos (por contraposición a los ataques pasivos en los que sólo se monitoriza la comunicación con el fin de obtener información de la misma o de lo intercambiado en ella) a aquellos ataques en los que se altere la información transmitida, se inserte información engañosa, o se secuestre la comunicación.

Para la protección de la integridad se podrán usar funciones HMAC cuya función de hash sea SHA-1 o preferiblemente SHA-2.

Nivel medio

En el nivel medio se emplearán, al igual que en la protección de la confidencialidad, redes privadas virtuales que proporcionen una seguridad equivalente a 112 bits. Esto es, se utilizarán claves cuya longitud sea de 112 bits (o superiores) para los sistemas de cifrado simétrico TDEA y AES, claves de 2048 bits (o superiores) para el criptosistema RSA y claves de longitudes comprendidas entre los 224 y 255 bits para criptosistemas basados en curvas elípticas.

Nivel alto

En este nivel se emplearán redes privadas virtuales que garanticen una seguridad equivalente a 128 bit, con la salvedad ya señalada del criptosistema RSA. Además, se recomienda el uso de dispositivos hardware para el establecimiento y uso de las redes privadas virtuales.

Es decir, se emplearán claves de 128 bits (o mayores) para los criptosistemas de cifrado simétrico TDEA y AES y claves de entre 256 y 283 bits para los criptosistemas basados en curvas elípticas. Para el criptosistema RSA, se permiten claves de 2048 bits, si bien se recomienda que la longitud de las claves sea mayor.

Resumen de protocolos permitidos:

Tipo	Nivel BAJO (opcional)	Nivel MEDIO	Nivel ALTO
secreto compartido TDEA AES	≥ 112 bits 112 o 168 128, 192 o 256	≥ 112 bits 112 o 168 128, 192 o 256	≥ 128 bits no 128, 192 o 256
clave pública RSA curvas elípticas	≥ 2.048 bits ≥ 224 bits	≥ 2.048 bits ≥ 224 bits	≥ 2.048 bits ≥ 256 bits
funciones hash SHA-1 (160) RIPEMD-160 SHA-2 SHA-3	 PCP PCP ≥ 256 bits ≥ 256 bits	 PCP PCP ≥ 256 bits ≥ 256 bits	 PCP PCP ≥ 256 bits ≥ 256 bits

PCP: Permitido a Corto Plazo

4.5. Cifrado de la información

Concepto. Cifrar una información consiste en transformarla de modo que pase a ser ilegible para todos salvo para las entidades autorizadas a acceder a dicha información. En general, el acceso a la información original a partir de su versión cifrada se lleva a cabo mediante el uso de claves y algoritmos.

El cifrado será aplicable a la información cuya confidencialidad sea considerada de nivel alto. Así, no se hará distinción acerca del soporte en el que la misma esté almacenada. En este sentido, se incluyen tanto los dispositivos fijos (disco duro, etc.), como los dispositivos removibles, es decir, CDs, DVDs, discos duros externos, pendrives, cintas de backup, etc., así como las bases de datos que contengan información de nivel alto.

Para el cifrado de información considerada de nivel alto en confidencialidad, ya sea en tránsito o mientras esté almacenada, se utilizarán sistemas de cifrado seguros. Se entienden por sistemas de cifrado seguros los que garantizan una seguridad de, al menos, 128 bits. Es decir, se emplearán claves para el cifrado/descifrado de información de 128 bits (o mayores) para los criptosistemas de cifrado simétrico TDEA y AES y claves de entre 256 y 283 bits para los criptosistemas basados en curvas elípticas. Para el caso particular del criptosistema RSA se permiten claves de 2048 bits, si bien se recomienda que dicha longitud sea mayor en la medida de lo posible.

Resumen:

Tipo	Nivel BAJO (opcional)	Nivel MEDIO (opcional)	Nivel ALTO
secreto compartido TDEA AES	≥ 112 bits 112 o 168 128, 192 o 256	≥ 128 bits no 128, 192 o 256	≥ 128 bits no 128, 192 o 256
clave pública RSA curvas elípticas	 ≥ 2.048 bits ≥ 224 bits	 ≥ 2.048 bits ≥ 224 bits	 ≥ 2.048 bits ≥ 256 bits

4.6. Protección de las claves criptográficas

Las claves criptográficas, independientemente de la seguridad que ofrezcan, estarán protegidas durante todo su ciclo de vida. Ello significa que se deberán arbitrar las medidas de seguridad necesarias tanto en el proceso de generación de las claves, como en su transporte al punto de explotación, en su custodia durante el tiempo que estén en uso, y en su posterior almacenamiento después de su vida activa hasta su destrucción final.

En la medida de lo posible, se velará porque los dispositivos portátiles no almacenen claves de acceso remoto a los diferentes organismos. Se entienden por claves de acceso remoto aquellas que permiten acceder a los equipos del organismo del que se depende o de otros organismos de naturaleza similar.

Se recomienda que, en caso de que sea necesario almacenar claves en ordenadores portátiles u otros dispositivos removibles, éstas estén a su vez cifradas por otras claves que sólo el propietario del hardware que las tiene almacenadas sea capaz de generar y utilizar.

Nivel bajo

Para proteger las claves en el nivel bajo, los procesos de generación de las mismas deberán estar aislados y no conectados a ninguna red. De igual modo, las claves archivadas por haber

sido retiradas y en espera de ser destruidas, también deberán estar almacenadas en dispositivos aislados.

Además, el acceso a los procesos tanto de generación de claves, como de transporte, custodia y almacenamiento estarán protegidos con una seguridad equivalente a 112 bits.

Nivel medio y alto

Para el nivel medio y alto, se considerarán las mismas protecciones que las señaladas en el punto anterior, si bien, en este caso las claves proporcionarán una seguridad equivalente a 128 bits.

4.7. Firma electrónica

Concepto. Una firma electrónica o digital es la simulación de una firma manuscrita pero en formato electrónico y tiene como fin enlazar de forma robusta una información con una entidad, esto es, el firmante de la información. De este modo, la firma electrónica previene el hecho de que un firmante pueda repudiar ser el autor de la información firmada, además de que la misma permite garantizar la integridad del contenido firmado.

Nivel bajo

Se podrá utilizar cualquier medio de firma electrónica de los reconocidos por la legislación vigente. En este sentido, los protocolos de firma electrónica harán uso de certificados digitales reconocidos1 (por ejemplo, los emitidos por la Fábrica Nacional de Moneda y Timbre o por la Dirección General de la Policía y Guardia Civil - DNIe) con claves RSA (del firmante) de, al menos, 1024 bits, o claves de 224-255 bits si se emplean curvas elípticas.

No se admitirá el uso de certificados cuya función resumen (en inglés, hash) sea la función MD5 u otra de seguridad inferior. Esto es, la función resumen deberá tener una seguridad mínima equiparable a la de la función SHA-1 o la RIPEMD-160.

Nivel medio

Se podrá utilizar cualquier medio de firma electrónica de los reconocidos por la legislación vigente. En este sentido, los protocolos de firma electrónica harán uso de certificados digitales reconocidos con claves RSA (del firmante) de, al menos, 1024 bits, o claves de 224-255 bits si se emplean curvas elípticas.

No se admitirá el uso de certificados cuya función resumen (en inglés, hash) sea la función MD5 u otra de seguridad inferior. Esto es, la función resumen deberá tener una seguridad mínima equiparable a la de la función SHA-1 o la RIPEMD-160.

En cualquier caso, se debe implantar el uso de certificados digitales reconocidos cuya clave pública RSA sea de 2048 bits (o superior), o si se emplean curvas elípticas, las claves deberían

tener una clave cuya longitud esté comprendida entre 255 y 283 bits. La función resumen a utilizar debe ser, preferiblemente, cualquiera de la serie SHA-2.

Además, las firmas se protegerán con sellos de tiempo.

Nivel alto

Al igual que en el caso del nivel medio, se podrá utilizar cualquier medio de firma electrónica de los reconocidos por la legislación vigente siempre que su clave RSA sea de, al menos, 2048 bits y utilice como función resumen la función SHA-1, la RIPEMD-160 u otra de seguridad equivalente, aunque se recomienda el uso de cualquier función resumen de las incluidas en la serie SHA-2.

Se recomienda el uso de certificados digitales reconocidos cuya clave pública RSA sea mayor de 2048 bits y cuya función resumen sea SHA-1, RIPEMD-160 o, preferiblemente, cualquiera de la serie SHA-2.

94. Si se emplean certificados digitales reconocidos basados en criptosistemas de clave pública que empleen curvas elípticas, deberán tener una clave cuya longitud esté entre los 256 y los 283 bits y deberán hacer uso de la función SHA-1, RIPEMD-160 o, preferiblemente, de cualquiera de las funciones incluidas en la serie SHA-2.

También en este nivel, las firmas se protegerán con sellos de tiempo.

Resumen de algoritmos permitidos:

Tipo	Nivel BAJO	Nivel MEDIO	Nivel ALTO
clave pública RSA DSA curvas elípticas	≥ 1.024 bits ≥ 1.024 bits ≥ 224 bits	≥ 1.024 bits (PCP) ≥ 1.024 bits (PCP) ≥ 224 bits	≥ 2.048 bits ≥ 2.048 bits ≥ 256 bits
funciones hash MD5 SHA-1 (160) RIPEMD-160 SHA-2 SHA-3	no corto plazo corto plazo ≥ 256 bits ≥ 256 bits	no corto plazo corto plazo ≥ 256 bits ≥ 256 bits	no corto plazo corto plazo ≥ 256 bits ≥ 256 bits

4.8. Sellos de tiempo

Concepto. Se entiende por sellado la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Nivel bajo y medio

No aplica.

Nivel alto

Se fecharán electrónicamente los documentos cuya fecha y hora de entrada debe acreditarse fehacientemente.

Se fecharán electrónicamente los documentos cuya fecha y hora de salida debe acreditarse fehacientemente.

Se fecharán electrónicamente las firmas cuya validez deba extenderse por largos periodos o así lo exija la normativa aplicable; alternativamente se pueden utilizar formatos de firma avanzada que incluyan fechado.

Se hará uso de sistemas de sellado de tiempo que utilicen una Autoridad de Sellado de Tiempo (TSA) siendo de los denominados esquemas simples o esquemas enlazados.

En los esquemas simples la TSA recibe el documento a sellar, le añade el tiempo actual y lleva a cabo un proceso de firma electrónica mediante un criptosistema asimétrico.

La firma electrónica de la TSA para el sellado de tiempo se hará mediante una clave RSA de, al menos, 3072 bits, o curvas elípticas con claves de, al menos, 284 bits, y una función resumen de las incluidas en la serie SHA-2 con una seguridad mayor o igual que la SHA-256. Es decir, no se aceptarán sellados de tiempo con firmas electrónicas realizadas por la TSA con longitudes de claves RSA menores a 3072 bits, o con claves de menos de 284 bits para ECC, ni con funciones resumen cuya seguridad sea menor que la ofrecida por la función SHA-256 de la serie SHA-2.

Para los esquemas enlazados, la seguridad recae en la función resumen empleada, por tanto, se empleará cualquiera de las funciones de la serie SHA-2 con una seguridad mayor o igual que la SHA-256.

	nivel ALTO	
tipo	**firma electrónica**	**listas enlazadas**
clave pública RSA curvas elípticas	 ≥ 3.072 bits ≥ 284 bits	 n.a. n.a.
funciones hash MD5 SHA-1 (160) RIPEMD-160 SHA-2 SHA-3	 no no no ≥ 256 bits ≥ 256 bits	 no no no ≥ 256 bits ≥ 256 bits

4.9. Mecanismos de cifrado utilizados en la organización

4.9.1. Conexiones VPN

Los accesos remotos a los sistemas de la organización se basan en tecnología DMVPN (Dynamic Multipoint Virtual Private Network).

En esencia, estas redes utilizan conexiones a Internet de distintos tipos y niveles de servicio, sobre las que establecen Túneles encriptados mediante el estándar IPSEC.

En los túneles, los procedimientos y formato de paquetes necesarios para establecer, negociar, modificar y eliminar las asociaciones de seguridad o SA de IPSEC son gestionados por ISAKMP. La configuración utilizada es la siguiente:

Algoritmo de encriptación:	AES - Advanced Encryption Standard (192 bit)
Algoritmo HASH:	Secure Hash Standard (SHA-1)
Método de autenticación:	Rivest-Shamir-Adleman Signature
Grupo Diffie-Hellman:	#5 (1536 bit)
Tiempo de renegociación:	86400 segs, sin límite de volumen de bytes

Los parámetros utilizados en IPSEC para efectuar las asociaciones de seguridad son:

Transform-set:	AES 192 con ESP
Modo del túnel:	Transporte
Tiempo de renegociación:	3600 segs, 4,6GB

4.9.1. Conexiones SSL

Las conexiones a los sitios web públicos donde la organización ofrece sus servicios, están protegidas con certificados emitidos por (Ej: Verisign (Symantec) de 2048 bit RSA) y algoritmo de firma (Ej: SHA1).

Los certificados instalados en todos los servidores públicos son de tipo ‘Extended Validation’ o EV.

4.9.2. Cifrado de dispositivos móviles

Todos aquellos dispositivos móviles que puedan transportar información clasificada como confidencial, deben disponer de un nivel de seguridad adicional mediante técnicas de cifrado.

La herramienta utilizada para el cifrado de dispositivos de almacenamiento extraíbles (pendrives, discos duros externos, etc.) y equipos portátiles es (Ej: “TrueCrypt”).

El algoritmo de encriptación utilizado es AES con claves de 256 bits. El algoritmo Hash empleado es SHA-512.

4.9.3. Cifrado de copias de respaldo

La herramienta utilizada para el cifrado es (Ej: Symantec Backup Exec), basada en algoritmos estándares de cifrado RSA y AES 256.

Las copias se efectúan en un servidor de backup.

5. ANEXOS/FORMATOS

N/A

6. REFERENCIAS

N/A