



**GUÍA DE SEGURIDAD
(CCN-STIC-800)**

**ESQUEMA NACIONAL DE SEGURIDAD
GLOSARIO DE TÉRMINOS
Y ABREVIATURAS**

Edita:



© Centro Criptológico Nacional, 2016

NIPO: 002-16-006-6

Fecha de Edición: febrero, 2016

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

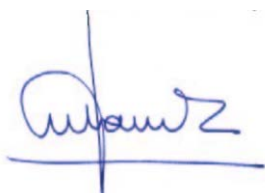
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Febrero 2016



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. TÉRMINOS.....	7
1.1. ACTIVO.....	7
1.2. ACREDITACIÓN	7
1.3. ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)	7
1.4. ALCANCE DE LA AUDITORÍA	7
1.5. AMENAZA	7
1.6. AMENAZA PERSISTENTE AVANZADA (APT)	7
1.7. ANÁLISIS O VALORACIÓN DE RIESGOS.....	8
1.8. AUDITOR.....	8
1.9. CRITERIOS DE RIESGO.....	8
1.10. AUDITOR INTERNO	8
1.11. AUDITOR EXTERNO.....	8
1.12. AUDITORIA.....	8
1.13. AUDITORÍA DE LA SEGURIDAD	8
1.14. AUDITORÍA DE SISTEMAS DE INFORMACIÓN	9
1.15. AUTENTICIDAD	9
1.16. AUTORIDAD DE ACREDITACIÓN.....	9
1.17. AUTORIDAD DELEGADA DE ACREDITACIÓN.....	9
1.18. ATAQUE POR FUERZA BRUTA O ATAQUE EXHAUSTIVO	9
1.19. CATEGORÍA DE UN SISTEMA.....	9
1.20. CERTIFICACIÓN DE LA SEGURIDAD	9
1.21. CIBERINCIDENTE	9
1.22. CLOUD APPLICATION PORTABILITY	10
1.23. CLOUD AUDITOR	10
1.24. CLOUD CAPABILITIES TYPE	10
1.25. CLOUD COMPUTING	10
1.26. CLOUD DATA PORTABILITY	10
1.27. CLOUD DEPLOYMENT MODEL	10
1.28. CLOUD SERVICE.....	10
1.29. CLOUD SERVICE CATEGORY	10
1.30. CLOUD SERVICE CUSTOMER	10
1.31. CLOUD SERVICE CUSTOMER DATA.....	11
1.32. CLOUD SERVICE PARTNER.....	11
1.33. CLOUD SERVICE PROVIDER.....	11
1.34. CLOUD SERVICE PROVIDER DATA.....	11
1.35. CLOUD SERVICE USER.....	11
1.36. CÓDIGO SEGURO DE VERIFICACIÓN (CSV).....	11
1.37. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	11
1.38. COMITÉ STIC	11
1.39. COMMON CRITERIA	12
1.40. COMMUNITY CLOUD	12
1.41. COMPROBACIÓN.....	12
1.42. COMPUTE AS A SERVICE (COMPAAS)	12
1.43. CONEXIÓN	12
1.44. CONFIDENCIALIDAD	12
1.45. CONTROL / CONTROLES	12
1.46. CORRELAR.....	12
1.47. CORREO BASURA (SPAM)	12
1.48. CRITERIOS COMUNES (COMMON CRITERIA).....	13
1.49. CRITERIOS DE AUDITORÍA	13
1.50. CUADRO DE MANDO.....	13

1.51.	CUMPLIMIENTO.....	13
1.52.	DATA PORTABILITY	13
1.53.	DATA STORAGE AS A SERVICE (DSAAS)	13
1.54.	DATOS.....	13
1.55.	DATOS DE CARÁCTER PERSONAL	14
1.56.	DECLARACIÓN DE REQUISITOS DE SEGURIDAD	14
1.57.	DECLARACIÓN DE REQUISITOS DE SEGURIDAD DE LA INTERCONEXIÓN	14
1.58.	DATOS DE CARÁCTER PERSONAL	14
1.59.	DECLARACIÓN DE CONFORMIDAD.....	14
1.60.	DENEGACIÓN [DISTRIBUIDA] DEL SERVICIO (DDOS)	14
1.61.	DICTAMEN	14
1.62.	DICTAMEN DE AUDITORÍA.....	14
1.63.	DISPONIBILIDAD	14
1.64.	DISPOSITIVO DE PROTECCIÓN DE PERÍMETRO.....	14
1.65.	EFFECTIVIDAD / EFICACIA	15
1.66.	EFICIENCIA	15
1.67.	ESCANER DE RED	15
1.68.	EVIDENCIA DE AUDITORÍA	15
1.69.	DESGUACIÓN O DESGUAR (DEFACE O DEFACEMENT).....	15
1.70.	DISPONIBILIDAD	15
1.71.	DUEÑO DEL RIESGO	15
1.72.	EVALUACIÓN DE LA SEGURIDAD.....	15
1.73.	EVENTO	16
1.74.	EVENTO DE SEGURIDAD.....	16
1.75.	FALSIFICACIÓN DE PETICIÓN EN SITIOS CRUZADOS (CSRF /XSRF)	16
1.76.	FIRMA ELECTRÓNICA	16
1.77.	GESTIÓN DE INCIDENTES.....	16
1.78.	GESTIÓN DE RIESGOS.....	16
1.79.	GUSANO.....	16
1.80.	HYBRID CLOUD.....	17
1.81.	IMPACTO	17
1.82.	INCIDENTE DE SEGURIDAD.....	17
1.83.	INDICADOR	17
1.84.	INFORMACIÓN	17
1.85.	INFORME DE AUDITORÍA	17
1.86.	INFRASTRUCTURE AS A SERVICE (IAAS)	17
1.87.	INFRASTRUCTURE CAPABILITIES TYPE	17
1.88.	INGENIERÍA SOCIAL	18
1.89.	INTEGRIDAD	18
1.90.	INTERCONEXIÓN	18
1.91.	INYECCIÓN DE FICHEROS REMOTA.....	18
1.92.	INYECCIÓN SQL (STRUCTURED QUERY LANGUAGE)	18
1.93.	LIMITACIONES AL ALCANCE	18
1.94.	MALWARE O CÓDIGO DAÑINO.....	19
1.95.	MANEJAR INFORMACIÓN	19
1.96.	MEASURED SERVICE	19
1.97.	MEDICIÓN	19
1.98.	MEDIDA	19
1.99.	MEDIDAS COMPENSATORIAS.....	19
1.100.	MEDIDAS DE SEGURIDAD	20
1.101.	MÉTRICA	20
1.102.	MÍNIMO PRIVILEGIO	20
1.103.	MULTI-TENANCY.....	20
1.104.	NECESIDAD DE CONOCER.....	20

1.105.	OBJETIVIDAD	20
1.106.	OBJETIVO DE LA AUDITORÍA	20
1.107.	OBSERVACIÓN	21
1.108.	OFUSCACIÓN	21
1.109.	ON-DEMAND SELF-SERVICE	21
1.110.	OPINIÓN INDEPENDIENTE Y OBJETIVA	21
1.111.	PHARMING (“FARM” GRANJA)	21
1.112.	PHISHING, SPEAR PHISHING	21
1.113.	PLAN DE AUDITORÍA	22
1.114.	PLAN DE RESPUESTA A CIBERINCIDENTES.....	22
1.115.	PLATFORM AS A SERVICE (PAAS)	22
1.116.	PLATFORM CAPABILITIES TYPE	22
1.117.	POLÍTICA DE FIRMA ELECTRÓNICA	22
1.118.	POLÍTICA DE SEGURIDAD	22
1.119.	PRINCIPIOS BÁSICOS DE SEGURIDAD	22
1.120.	PRINCIPIOS DE SEGREGACIÓN DE FUNCIONES.....	22
1.121.	PRIVATE CLOUD	22
1.122.	PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD	23
1.123.	PROCESO	23
1.124.	PROCESO DE SEGURIDAD	23
1.125.	PRODUCTO DE SEGURIDAD TIC	23
1.126.	PROGRAMAS ESPÍA	23
1.127.	PROGRAMA DE AUDITORÍA.....	23
1.128.	PROPIETARIO DEL RIESGO.....	24
1.129.	PROPIETARIO DEL SISTEMA	24
1.130.	PRUEBAS DE AUDITORÍA.....	24
1.131.	PRUEBAS DE CUMPLIMIENTO.....	24
1.132.	PRUEBAS SUSTANTIVAS	24
1.133.	PUBLIC CLOUD.....	24
1.134.	PUERTO SEGURO (SAFE HARBOR).....	24
1.135.	RANSOMWARE.	24
1.136.	RAT (REMOTE ACCESS TOOLS)	25
1.137.	RECOMENDACIONES.....	25
1.138.	REQUISITO	25
1.139.	REQUISITOS MÍNIMOS DE SEGURIDAD	25
1.140.	RESOURCE POOLING	25
1.141.	RESPONSABILIDAD	25
1.142.	RESPONSABLE DE LA INFORMACIÓN.....	26
1.143.	RESPONSABLE DE LA SEGURIDAD.....	26
1.144.	RESPONSABLE DEL SERVICIO	26
1.145.	RESPONSABLE DEL SISTEMA.....	26
1.146.	REVERSIBILITY	26
1.147.	RIESGO.....	26
1.148.	ROOTKIT.....	26
1.149.	SCANNER (SCANNING) ESCANER DE VULNERABILIDADES / ANÁLISIS DE SEGURIDAD DE LA RED	27
1.150.	SATISFACCIÓN DE AUDITORÍA	27
1.151.	SALVAGUARDAS (CONTRAMEDIDAS).....	27
1.152.	SECUENCIA DE COMANDOS EN SITIOS CRUZADO (XSS)	27
1.153.	SEGURIDAD DE LA INFORMACIÓN	27
1.154.	SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN.....	27
1.155.	SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	28
1.156.	SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.....	28
1.157.	SEGURIDAD POR DEFECTO.....	28
1.158.	SELECCIÓN DE MUESTRAS	28

1.159.	SERVICE LEVEL AGREEMENT (SLA)	28
1.160.	SERVICIO	28
1.161.	SERVICIOS ACREDITADOS	29
1.162.	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)	29
1.163.	SISTEMA DE INFORMACIÓN	29
1.164.	SISTEMA DE PROTECCIÓN DE PERÍMETRO (SPP)	29
1.165.	SISTEMA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	29
1.166.	SISTEMA TIC	29
1.167.	SNIFFER/SNIFFING (MONITOR DE RED)	29
1.168.	SOFTWARE AS A SERVICE (SAAS)	30
1.169.	SPAM	30
1.170.	SPEAR PHISHING	30
1.171.	SPOOFING	30
1.172.	SPYWARE "SPY SOFTWARE"	30
1.173.	SUFICIENCIA DE LAS EVIDENCIAS	30
1.174.	SUPERVISIÓN	30
1.175.	SUPLANTACIÓN	30
1.176.	TENANT	31
1.177.	TIMESTAMP O SELLADO DE TIEMPOS	31
1.178.	TIPO DE INFORMACIÓN	31
1.179.	TRAZABILIDAD	31
1.180.	TROYANO O CABALLO DE TROYA	31
1.181.	VERIFICACIÓN	32
1.182.	VIRUS	32
1.183.	VULNERABILIDAD	32
1.184.	ZONA DESMILITARIZADA	32
2.	ABREVIATURAS	33
3.	REFERENCIAS	37

1. TÉRMINOS

1. A fin de conocer la seguridad que ofrece un sistema, necesitamos modelarlo, identificando y valorando los elementos que lo componen y las amenazas a las que están expuestos. Con estos datos podemos estimar los riesgos a los que el sistema está expuesto.

1.1. ACTIVO

2. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. ENS.

1.2. ACREDITACIÓN

3. Autorización otorgada por la Autoridad responsable de la acreditación, para manejar información de un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.

1.3. ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)

4. Responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema y de la redacción de los Procedimientos Operativos de Seguridad. OM 76/2002.
5. (en) Information System Security Officer. Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. CNSS Inst. 4009, Adapted

1.4. ALCANCE DE LA AUDITORÍA

6. Elementos a los que comprende la revisión de auditoría: los sistemas que estarán en revisión, el organismo responsable de estos sistemas, los elementos de la estructura tecnológica, personal vinculado a los elementos anteriores, periodos de tiempo. Dentro del contexto de esta guía tiene una relación directa con la Declaración de Aplicabilidad.

1.5. AMENAZA

7. Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

1.6. AMENAZA PERSISTENTE AVANZADA (APT)

8. (en)Advanced Persistent Threat (APT). Un ataque selectivo de ciberespionaje o ciber sabotaje, llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas. McAfee. Predicciones de amenazas para 2011.

1.7. ANÁLISIS O VALORACIÓN DE RIESGOS

9. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos. ENS.
10. Proceso sistemático para estimar la magnitud del riesgo sobre un Sistema (STIC 811)

1.8. AUDITOR

11. El profesional con formación y experiencia contrastable sobre las materias a auditar, que reúne las condiciones, además de las de conocimientos y competencia, de actuar de forma independiente. Realiza las tareas de auditoría.

1.9. CRITERIOS DE RIESGO

12. Términos de referencia respecto a los que se evalúa la importancia de un riesgo. [UNE Guía 73:2010]

1.10. AUDITOR INTERNO

13. Pertenece a una unidad independiente dentro del organismo al que pertenecen los elementos objeto de la auditoría, con funciones y autoridad claramente definidas, que no tiene responsabilidades operativas, directivas o de gestión de los procesos, sistemas o áreas auditados. Para favorecer su independencia esta unidad debe reportar al nivel jerárquico más alto dentro del organismo.

1.11. AUDITOR EXTERNO

14. Es independiente laboralmente al organismo donde realizará la auditoría. Para mantener su independencia, a título individual o como entidad, no debe haber realizado funciones (asesoría, consultoría), para los sistemas o procesos dentro del alcance de la auditoría a realizar.

1.12. AUDITORIA

15. Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.
 - Nota 1: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).
 - Nota 2: “Evidencia de auditoría” y “criterios de auditoría” se definen en la Norma ISO 19011.[ISO, Anexo SL]

1.13. AUDITORÍA DE LA SEGURIDAD

16. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. ENS.

1.14. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

17. La Auditoría de sistemas de información es el proceso metodológico, realizado con independencia de los elementos auditados y con objetividad, de recoger, agrupar y evaluar evidencias para determinar si los sistemas o tecnologías de la información salvaguardan los activos, mantienen la integridad de los datos, contribuyen al logro de los fines de la organización y utilizan eficientemente los recursos
18. La actividad de auditoría debe evaluar las exposiciones al riesgo referidas al gobierno, operaciones y sistema de información de la organización, con relación a la fiabilidad e integridad de la información, la eficacia y eficiencia de las operaciones, la protección de activos, y el cumplimiento de leyes, regulaciones y contratos

1.15. AUTENTICIDAD

19. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. ENS.

1.16. AUTORIDAD DE ACREDITACIÓN

20. Autoridad responsable de la definición y aplicación de la Política STIC.

1.17. AUTORIDAD DELEGADA DE ACREDITACIÓN

21. Autoridad responsable en su ámbito, de la aplicación de la Política STIC y de las competencias que delegue la Autoridad de Acreditación.

1.18. ATAQUE POR FUERZA BRUTA O ATAQUE EXHAUSTIVO

22. Caso particular de ataque sólo al texto cifrado en el que el criptoanalista, conociendo el algoritmo de cifra, intenta su descifrado probando con cada clave del espacio de claves. Si el cardinal de este último es un número muy grande, el tiempo invertido en recorrer el citado espacio es fabuloso, y las probabilidades de éxito escasísimas. [Ribagorda:1997]

1.19. CATEGORÍA DE UN SISTEMA

23. Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios. ENS.

1.20. CERTIFICACIÓN DE LA SEGURIDAD

24. Determinación positiva de que un producto o Sistema tiene capacidad para proteger la información según un nivel de seguridad, y de acuerdo a unos criterios establecidos en el procedimiento o metodología de evaluación correspondiente.

1.21. CIBERINCIDENTE

25. Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta. STIC 401 GLOSARIO.
26. Incidente relacionado con la seguridad de las Tecnologías de la Información y las Comunicaciones que se produce en el Ciberespacio. Este término engloba aspectos como

los ataques a sistemas TIC, el fraude electrónico, el robo de identidad, el abuso del Ciberespacio, etc. [ISDEFE-6:2009]

1.22. CLOUD APPLICATION PORTABILITY

27. (en) Ability to migrate an application from one cloud service to another cloud service [ISO/IEC 17788:2014]

1.23. CLOUD AUDITOR

28. (en) Cloud service partner with the responsibility to conduct an audit of the provision and use of cloud services [ISO/IEC 17788:2014]

1.24. CLOUD CAPABILITIES TYPE

29. (en) Classification of the functionality provided by a cloud service to the cloud service customer, based on resources used. NOTE–The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type.[ISO/IEC 17788:2014]

1.25. CLOUD COMPUTING

30. (en) Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. NOTE Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.[ISO/IEC 17788:2014]

1.26. CLOUD DATA PORTABILITY

31. (en) Data portability from one cloud service to another cloud service.[ISO/IEC 17788:2014]

1.27. CLOUD DEPLOYMENT MODEL

32. (en) Way in which cloud computing can be organized based on the control and sharing of physical or virtual resources NOTE–The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud.[ISO/IEC 17788:2014]

1.28. CLOUD SERVICE

33. (en) One or more capabilities offered via cloud computing invoked using a defined interface. [ISO/IEC 17788:2014]

1.29. CLOUD SERVICE CATEGORY

34. (en) Group of cloud services that possess some common set of qualities. NOTE–A cloud service category can include capabilities from one or more cloud capabilities types. [ISO/IEC 17788:2014]

1.30. CLOUD SERVICE CUSTOMER

35. (en) Party which is in a business relationship for the purpose of using cloud services. NOTE–A business relationship does not necessarily imply financial agreements. [ISO/IEC 17788:2014]

1.31. CLOUD SERVICE CUSTOMER DATA

36. (en) Class of data objects under the control, by legal or other reasons, of the cloud service customer that was in put to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service. NOTE 1 An example of legal controls is copyright. NOTE 2 It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers or obtained from another source, or it might be publicly available data. However, any out put data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary. [ISO/IEC 17788:2014]

1.32. CLOUD SERVICE PARTNER

37. (en) Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer , or both [ISO/IEC 17788:2014]

1.33. CLOUD SERVICE PROVIDER

38. (en) Party which makes cloud services available [ISO/IEC 17788:2014]

1.34. CLOUD SERVICE PROVIDER DATA

39. (en) Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider NOTE – Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.[ISO/IEC 17788:2014]

1.35. CLOUD SERVICE USER

40. (en) Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services NOTE– Examples of such entities include devices and applications. [ISO/IEC 17788:2014]

1.36. CÓDIGO SEGURO DE VERIFICACIÓN (CSV)

41. Herramienta de control de versiones de gran utilidad en entornos de desarrollo software y que garantiza la integridad del documento del que se trate.

1.37. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

42. Órgano colegiado que coordina las actividades de la organización en materia de seguridad de la información. En particular asume los roles de responsable de la información y responsable de los servicios. Guía CCN-STIC-801.

1.38. COMITÉ STIC

43. Comisión que reúne a los responsables de seguridad TIC y toma decisiones de coordinación. Guía CCN-STIC 402.

1.39. COMMON CRITERIA

44. Ver Criterios Comunes.

1.40. COMMUNITY CLOUD

45. (en) Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection. [ISO/IEC 17788:2014]

1.41. COMPROBACIÓN

46. 1) (DRAE) Verificar, confirmar la veracidad o exactitud de algo.
47. 2) Dentro del contexto de esta guía, son verificaciones de la realización de controles, del establecimiento de medidas de seguridad, y de documentación de políticas, entre otros, dentro de los requerimientos establecidos por la norma de referencia en la auditoría.

1.42. COMPUTE AS A SERVICE (COMPAAS)

48. (en) Cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software NOTE–To run some software, capabilities other than processing resources may be needed.[ISO/IEC 17788:2014]

1.43. CONEXIÓN

49. Se produce una conexión, cuando se proveen los medios físicos y lógicos de transmisión adecuados (por ejemplo enlace satélite, fibra óptica, etc.) susceptibles de ser empleados para el intercambio de información entre Sistemas.

1.44. CONFIDENCIALIDAD

50. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. ENS.

1.45. CONTROL / CONTROLES

51. 1) (DRAE) Regulación, manual o automática, sobre un sistema.
52. 2) Mecanismo o procedimiento que evita, previene, o detecta un riesgo.
53. 3) En el contexto de una auditoría, estos pueden ser clasificados en preventivos, detectivos, y correctivos.

1.46. CORRELAR

54. Proceso de comparar diferentes fuentes de información, obteniéndose de esta manera sentido a eventos que analizados por separado no la tendrían o pasaría desapercibida.

1.47. CORREO BASURA (SPAM)

55. Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es una extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de usuarios están expuestos a este correo basura que se confirma en encuestas que

muestran que más del 50% de todos los emails son correos basura. No es una amenaza directa, pero la cantidad de correos electrónicos (e-mails) generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.http://www.alerta-antivirus.es/seguiridad/ver_pag.html?tema=S

1.48. CRITERIOS COMUNES (COMMON CRITERIA)

56. Estándar internacional para la certificación de la seguridad en computadoras que pretende garantizar que el software se comporta conforme a las especificaciones.

1.49. CRITERIOS DE AUDITORÍA

57. 1) Normas y procesos metodológicos propios de la función de auditoría.
58. 2) Dentro de una auditoría, esta palabra se usa también para las razones o discernimientos de los auditores para la confección del plan de auditoría, o evaluar los resultados de las pruebas realizadas.

1.50. CUADRO DE MANDO

59. Conjunto de indicadores para resumir el desempeño de un sistema.
60. Scorecard. (1) A printed program or card enabling a spectator to identify players and record the progress of a game or competition. (2) A small card used to record one's own performance in sports such as golf.[Herrmann:2007]

1.51. CUMPLIMIENTO

61. Ver “prueba de cumplimiento”.

1.52. DATA PORTABILITY

62. (en) Ability to easily transfer data from one system to another without being required to reenter data. NOTE – It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system. But even if the formats do not match, the transformation between them may be simple and straightforward to achieve with commonly available tools. On the other hand, a process of printing out the data and rekeying it for the target system could not be described as "easy." [ISO/IEC 17788:2014]

1.53. DATA STORAGE AS A SERVICE (DSAAS)

63. (en) Cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities. NOTE–DSaaS can provide any of the three cloud capabilities types.[ISO/IEC 17788:201]

1.54. DATOS

64. Representación de la información usando algún formato que permita su comunicación, interpretación, almacenamiento y procesamiento automático.
65. (en) Data. (1) Representations of information or objects, in any form. (2) The representation of information in a manner suitable for the communication, interpretation, storage, or processing. [Herrmann:2007]

1.55. DATOS DE CARÁCTER PERSONAL

66. Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

1.56. DECLARACIÓN DE REQUISITOS DE SEGURIDAD

67. Es el documento base para la acreditación. Consiste en la exposición completa y detallada de los principios de seguridad que deben observarse y de los requisitos de seguridad que se han de implantar conforme al correspondiente análisis de riesgos realizado previamente.

1.57. DECLARACIÓN DE REQUISITOS DE SEGURIDAD DE LA INTERCONEXIÓN

68. Documento base para la acreditación de la interconexión de Sistemas. Consiste en la exposición completa y detallada de los principios de seguridad que deben observarse en la interconexión, y de los requisitos de seguridad que se han de implantar conforme al correspondiente análisis de riesgos realizado previamente.

1.58. DATOS DE CARÁCTER PERSONAL

69. Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.59. DECLARACIÓN DE CONFORMIDAD

70. Manifestación escrita de los órganos o entidades de derecho público, firmada por su responsable, mediante la que se da publicidad que los sistemas a que se refieren cumplen con las exigencias del Esquema Nacional de Seguridad aprobado por Real Decreto 3/2010, de 8 de enero.

1.60. DENEGACIÓN [DISTRIBUIDA] DEL SERVICIO (DDOS)

71. Denial of Service (DoS) Denial of Service Distributed (DDoS). Ataque de denegación de servicio que se realiza utilizando múltiples puntos de ataque simultáneamente. Denegación de Servicio Distribuida (DDoS). Ataque DoS en el que participan gran cantidad de máquinas atacantes.[CCN-STIC-612:2006]

1.61. DICTAMEN

72. (DRAE) Opinión y juicio que se forma o emite sobre algo.

1.62. DICTAMEN DE AUDITORÍA

73. Ver “informe de auditoría”.

1.63. DISPONIBILIDAD

74. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. ENS.

1.64. DISPOSITIVO DE PROTECCIÓN DE PERÍMETRO

75. Hardware y/o software, cuya finalidad es mediar en el tráfico de entrada y salida en los puntos de interconexión de los Sistemas.

1.65. EFECTIVIDAD / EFICACIA

76. (DRAE) Efectividad. Capacidad de lograr el efecto que se desea o se espera.
77. Eficacia. Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados. [UNE-ISO/IEC 27000:2014]

1.66. EFICIENCIA

78. Relación entre el resultado alcanzado y los recursos utilizados. [ISO-9000_es:2000]

1.67. ESCANER DE RED

79. Herramienta de seguridad cuyo objetivo es la detección de los sistemas conectados a la red, así como los servicios que estos puedan estar prestando.

1.68. EVIDENCIA DE AUDITORÍA

80. Las evidencias consisten, principalmente, en las demostraciones y testimonios (documentales, automatizadas, etc.) de los resultados de la aplicación de los procedimientos de auditoría (pruebas). Éstas deben ser suficientes para soportar las conclusiones del auditor. Para ello deben acreditar determinadas situaciones o hechos irrefutables en cuanto a los hechos a los que se refieren. La evaluación de estas evidencias corresponde al auditor para emitir su opinión.

1.69. DESFIGURACIÓN O DESFIGURAR (DEFACE O DEFACEMENT)

81. Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia. El cambio de imagen puede ser a beneficio del atacante, o por mera propaganda (a beneficio del atacante o para causar una situación embarazosa al propietario de las páginas). STIC 401 GLOSARIO.
82. **Deface o Defacement** (desfigurar o desfiguración) deformación o cambio producido de manera intencionada en una página web legítima a través de algún tipo de acceso de código dañino. Informe de Amenazas 2015.

1.70. DISPONIBILIDAD

83. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. ENS.

1.71. DUEÑO DEL RIESGO

84. Persona o entidad que tiene la responsabilidad y la autoridad para gestionar los riesgos. ISO Guía 73.
85. **(en) Risk owner.** Person or entity with the accountability and authority to manage the risk. ISO Guide 73.

1.72. EVALUACIÓN DE LA SEGURIDAD

86. Proceso de comprobación de que un producto o Sistema satisface las características de seguridad que proclama tener. Dicho proceso consiste en el examen detallado con el fin de encontrar una posible vulnerabilidad y confirmar el nivel de seguridad establecido. El

examen se realiza de acuerdo a un procedimiento o metodología determinado y siguiendo unos criterios de evaluación perfectamente definidos y establecidos.

1.73. EVENTO

87. (Operación del Servicio) Un cambio de estado significativo para la cuestión de un Elemento de Configuración o un Servicio de TI. El término Evento también se usa como Alerta o notificación creada por un Servicio de TI, Elemento de Configuración o herramienta de Monitorización. Los Eventos requieren normalmente que el personal de Operaciones de TI tome acciones, y a menudo conllevan el registro de Incidencias.[ITIL:2007]

1.74. EVENTO DE SEGURIDAD

88. Suceso de seguridad de la información. Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.[UNE-ISO/IEC 27000:2014]

1.75. FALSIFICACIÓN DE PETICIÓN EN SITIOS CRUZADOS (CSRF /XSRF)

89. **Cross Site Request Forgery (CSRF /XSRF)**. Es un tipo de *exploit* o programa malicioso que aprovecha un fallo o vulnerabilidad de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un clic, cabalgamiento de sesión, y ataque automático.

1.76. FIRMA ELECTRÓNICA

90. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante. ENS.

1.77. GESTIÓN DE INCIDENTES

91. Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas. RD. 951/2015, de 23 de octubre ENS.

1.78. GESTIÓN DE RIESGOS

92. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. ENS.

1.79. GUSANO

93. **Worm**. Programa que está diseñado para copiarse y propagarse por sí mismo mediante mecanismos de red. No realizan infecciones a otros programas o ficheros. [CCN-STIC-430:2006]. Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de ellos mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.http://www.alerta-antivirus.es/seguiridad/ver_pag.html?tema=S

1.80. HYBRID CLOUD

94. (en) cloud deployment model using at least two different cloud deployment models [ISO/IEC 17788:2014]

1.81. IMPACTO

95. Consecuencia que sobre un activo tiene la materialización de una amenaza.

1.82. INCIDENTE DE SEGURIDAD

96. Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información. ENS. Ver Ciberincidente.

1.83. INDICADOR

97. (1) Instrumento que se utiliza para monitorizar la operación de un ingenio, en sentido general. (2) Química. Un elemento que cambia de color o estructura cuando se dan ciertas circunstancias, sirviendo como mecanismo de detección. (3) Economía. Conjunto de estadísticos que sirven para saber cómo está y a dónde se encamina la economía.
98. **(en) Indicator.** (1) An instrument used to monitor the operation or condition of an engine, furnace, electrical network, reservoir, or other physical system; a meter or gauge. (2) Chemistry. A chemical compound that changes color and structure when exposed to certain conditions and is therefore useful for chemical tests. (3) Ecology: A plant or animal whose existence in an area is strongly indicative of specific environmental conditions. (4) Any of various statistical values that together provide an indication of the condition or direction of the economy. [Herrmann:2007]

1.84. INFORMACIÓN

99. Caso concreto de un cierto tipo de información.
100. **(en) Information.** An instance of an information type. FIPS 199.

1.85. INFORME DE AUDITORÍA

101. Es el producto final de las tareas realizadas en una auditoría. En el informe el auditor comunica, a quien corresponda, los resultados de las tareas realizadas, con los resultados obtenidos.

1.86. INFRASTRUCTURE AS A SERVICE (IAAS)

102. (en) cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type NOTE–The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls).[ISO/IEC 17788:2014]

1.87. INFRASTRUCTURE CAPABILITIES TYPE

103. (en) cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources [ISO/IEC 17788:2014]

1.88. INGENIERÍA SOCIAL

104. Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S
105. Eufemismo empleado para referirse a medios no técnicos o de baja complejidad tecnológica utilizados para atacar a sistemas de información, tales como mentiras, suplantaciones, engaños, sobornos y chantajes. [CCN-STIC-403:2006]

1.89. INTEGRIDAD

106. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. ENS.

1.90. INTERCONEXIÓN

107. Se produce una interconexión entre Sistemas, cuando existe una conexión y se habilitan flujos de información entre los mismos, con diferentes políticas de seguridad, diferentes niveles de confianza, diferentes Responsables o una combinación de las anteriores.

1.91. INYECCIÓN DE FICHEROS REMOTA

108. Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web. En esta clase de vulnerabilidades se incluye la inyección *SQL* (*Structured Query Language*), la inyección *LDAP* (*Lighthweight Directory Access Protocol*) y la inyección *XPath*. <http://es.pcisecuritystandards.org>

1.92. INYECCIÓN SQL (STRUCTURED QUERY LANGUAGE)

109. Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos *SQL* (*Structured Query Language*) no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos. <http://es.pcisecuritystandards.org>
110. Técnica de ataque, cuyo objetivo es hacer uso de alguna vulnerabilidad en la validación de entradas en una aplicación para pasar código SQL no autorizado a una base de datos no accesible a priori para el atacante.[CCN-STIC-818]

1.93. LIMITACIONES AL ALCANCE

111. Son aquellos registros o documentos, o elementos del alcance de la auditoría, a los que, aunque previstos en las revisiones planificadas, para lograr los objetivos de la auditoría, el auditor no ha podido tener acceso, por distintas razones, y cuya restricción de acceso puede impactar en las conclusiones de la auditoría. Deben estar reflejadas en el informe de auditoría. Dentro del contexto de esta guía de auditoría, aunque podrían surgir en la definición del alcance, esta situación debería ser excepcional. Si las restricciones surgen en la fase inicial de delimitación del alcance, el auditor debe indicarlo, además de en el

informe final, en la planificación. Asimismo, si surge en la fase inicial, debe indicarse el posible impacto en la realización de la auditoría, y la obtención de las conclusiones en relación al objetivo de la auditoría. Es conveniente que en todos los casos, el auditor requiera que se comunique por escrito, la restricción de acceso a registros, documentos o elementos auditables, y justificados por el objetivo de la auditoría

1.94. MALWARE O CÓDIGO DAÑINO

112. Software de carácter malicioso cuyo objetivo principal es dañar o infiltrarse en un sistema.

1.95. MANEJAR INFORMACIÓN

113. Presentar, elaborar, almacenar, procesar, transportar o destruir información.

1.96. MEASURED SERVICE

114. (en) metered delivery of cloud services such that usage can be monitored, controlled, reported and billed

1.97. MEDICIÓN

115. (1) Proceso consistente en la asignación de números o símbolos a entidades de la realidad de forma que nos permitan describir dichas entidades de acuerdo a unas reglas claramente definidas. (2) Comparación de una propiedad de un objeto con una propiedad similar en otro objeto que se usa de referencia.

116. **(en) Measurement.** (1) The process by which numbers or symbols are assigned to entities in the real world in such a way as to describe them according to clearly defined rules. (2) A process that is a repeated application of a test method using a measuring system. (3) The comparison of a property of an object to a similar property of a standard reference. Measurements are effective when they are used either to orient decisions, to define corrective actions, or to get a better understanding of casual relationships between intended expectations and observed facts. [Herrmann:2007]

1.98. MEDIDA

117. El número o símbolo asignado a una entidad como resultado de un proceso de medición. La medida sirve para caracterizar un atributo de la entidad.

118. **(en) Measure.** The number or symbol assigned to an entity by the measurement process in order to characterize an attribute. [Herrmann:2007]

1.99. MEDIDAS COMPENSATORIAS

119. Medidas de seguridad que se aplican en lugar de otras de las prescritas en el Anexo II. Deben satisfacer los siguientes requisitos:

- Cumplir con el propósito de las medidas a las que sustituye.
- Reducir el riesgo igual o más que las medidas originales.
- Estar aprobadas formalmente por el Responsable de la Seguridad.

120. **(en) compensating security control.** A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended

security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. [CNSSI_4009:2010]

1.100. MEDIDAS DE SEGURIDAD

121. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación. ENS.

1.101. MÉTRICA

122. Por una parte es una unidad de medida (como lo es, por ejemplo, el sistema métrico decimal). Por otra parte, suele tener una finalidad, entendiéndose como una herramienta para entender la realidad y tomar decisiones al respecto.
123. **(en) Metric.** (1) A proposed measure or unit of measure. (2) Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. [Herrmann:2007]

1.102. MÍNIMO PRIVILEGIO

124. Principio según el cual los sujetos deben acceder exclusivamente a aquellos objetos que precisen inexcusablemente para ejecutar sus trabajos o procesos. Es término sinónimo de "necesidad de saber". [Ribagorda 2007]
125. **(en) Least privilege.** The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. [CNSSI_4009:2010]

1.103. MULTI-TENANCY

126. **(en)** allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another [ISO/IEC 17788:2014]

1.104. NECESIDAD DE CONOCER

127. Determinación positiva por la que se confirma que un posible destinatario requiere el acceso a, el conocimiento de, o la posesión de la información para desempeñar servicios, tareas o cometidos oficiales.
128. **(en) Need-to-know.** A method of isolating information resources based on a user's need to have access to that re-source in order to perform their job but no more. The terms 'need-to-know' and 'least privilege' express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. [CNSSI_4009:2010]

1.105. OBJETIVIDAD

129. Ver "opinión independiente y objetiva".

1.106. OBJETIVO DE LA AUDITORÍA

130. 1) Las metas específicas que debe lograr la auditoría.

131. 2) En el contexto de esta guía, llegar con concluir si se cumple con lo requeridos por las normas de referencia.

1.107. OBSERVACIÓN

132. Ver “pruebas de auditoría”.

1.108. OFUSCACIÓN

133. Proceso de ocultar o dificultar el acceso a la información mediante técnicas de camuflaje, encriptación, compresión, etc.

1.109. ON-DEMAND SELF-SERVICE

134. (en) feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider [ISO/IEC 17788:2014]

1.110. OPINIÓN INDEPENDIENTE Y OBJETIVA

135. 1) Independiente: (DRAE) que no tiene dependencia, que no depende de otro.
136. 2) Objetiva: (DRAE) Perteneciente o relativo al objeto en sí mismo, con independencia de la propia manera de pensar o de sentir.
137. 3) La auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que está siendo auditada para permitir completar de manera objetiva la auditoría.
138. 4) El auditor debe juzgar y opinar sobre los resultados de la auditoría, en función del objetivo y alcance de la misma, libre de toda parcialidad o sesgo que pueda afectar de forma negativa en los resultados de la auditoría, y que pueda conducir a una interpretación errónea de los hechos identificados.

1.111. PHARMING (“FARM” GRANJA)

139. Deriva del término en inglés "farm" (granja). Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP (*Internet Protocol*) legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP donde se aloja una web (página) falsa que suplantarán la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad. <http://www.inteco.es/glossary/Formacion/Glosario/>

1.112. PHISHING, SPEAR PHISHING

140. Similar a “*fishing*” pescando. *Spear phishing* (“lanza”). Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.
141. Delito informático consistente en obtener información confidencial de forma fraudulenta y haciendo uso de la ingeniería social.

1.113. PLAN DE AUDITORÍA

142. Ver “programa de auditoría”

1.114. PLAN DE RESPUESTA A CIBERINCIDENTES

143. Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, responder y limitar las consecuencias de un ciberincidente

1.115. PLATFORM AS A SERVICE (PAAS)

144. (en) Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type [ISO/IEC 17788:2014]

1.116. PLATFORM CAPABILITIES TYPE

145. (en) Cloud capabilities type in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider [ISO/IEC 17788:2014]

1.117. POLÍTICA DE FIRMA ELECTRÓNICA

146. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma. ENS.

1.118. POLÍTICA DE SEGURIDAD

147. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos. ENS.

1.119. PRINCIPIOS BÁSICOS DE SEGURIDAD

148. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios. ENS.

1.120. PRINCIPIOS DE SEGREGACIÓN DE FUNCIONES

149. 1) (DRAE) Principio: Norma o idea fundamental que rige el pensamiento o la conducta.

150. 2) La separación o segregación de funciones es una regla básica en los controles: evitar que una persona pueda dominar todo un proceso, de tal forma que errores u omisiones, o incumplimientos de controles no puedan ser identificados. Por lo tanto, el auditor debe identificar donde no se cumple con esta norma fundamental, para evaluar el impacto en la efectividad de los controles.

1.121. PRIVATE CLOUD

151. (en)cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer [ISO/IEC 17788:2014]

1.122. PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD

152. Descripción precisa de la aplicación de los requisitos de seguridad, detallando las responsabilidades y todas las acciones y procedimientos de seguridad a seguir, con el objetivo de garantizar y mantener la seguridad del Sistema. En su caso será la descripción de la aplicación de la Declaración de Requisitos de un Sistema (DRS) correspondiente.
153. Los POS definen los principios que deberán adoptarse en materia de seguridad, los procedimientos operativos que deberán seguirse y las responsabilidades del personal. Los POS se elaborarán bajo la responsabilidad del Responsable del Sistema. Adaptada de 2001/264/CE.

1.123. PROCESO

154. Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado. ENS.

1.124. PROCESO DE SEGURIDAD

155. Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad. ENS.

1.125. PRODUCTO DE SEGURIDAD TIC

156. Conjunto de componentes *software*, *firmware* y/o *hardware*, que proporcionan funcionalidad de seguridad, diseñado para su uso o para su incorporación en un sistema o en un entorno operativo definido específicamente y con una utilidad particular.

1.126. PROGRAMAS ESPÍA

157. *Spyware "spy software"*. Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último. <http://es.pcisecuritystandards.org>
158. *Spyware*. Código malicioso diseñado habitualmente para utilizar la estación del usuario infectado con objetivos comerciales o fraudulentos como puede ser mostrar publicidad o robo de información personal del usuario. [CCN-STIC-400:2006]
159. Software espía. Cualquier forma de tecnología que se usa para recoger información sobre una persona o empresa, o información referente a equipos o a redes, sin su conocimiento o consentimiento. También puede venir implementado en su hardware. Puede capturar hábitos de navegación, mensajes de correo, contraseñas y datos bancarios para transmitirlos a otro destino en Internet. Al igual que los virus puede ser instalado al abrir un adjunto de correo infectado, pulsando en una ventana de publicidad o camuflado junto a otros programas que instalemos. http://www.alertaantivirus.es/seguridad/ver_pag.html?tema=S

1.127. PROGRAMA DE AUDITORÍA

160. Descripción detallada (paso a paso) de los procedimientos de auditoría (documentación, pruebas, etc.) que se deben realizar durante la ejecución del trabajo de auditoría para alcanzar el objetivo de la misma. En el programa de la auditoría también se incluyen la

asignación de tareas, fechas de realización de las tareas, y recursos necesarios para desarrollar la auditoría.

1.128. PROPIETARIO DEL RIESGO

161. Ver 'dueño del riesgo'.

1.129. PROPIETARIO DEL SISTEMA

162. Ver 'responsable del sistema'.

1.130. PRUEBAS DE AUDITORÍA

163. 1) Permiten obtener evidencia y verificar la consistencia de los controles existentes y también medir el riesgo por deficiencia de estos o por su ausencia.

164. 2) Se diseñan y planifican para asegurar que los controles se diseñan adecuadamente y funcionan de forma efectiva y continuada.

1.131. PRUEBAS DE CUMPLIMIENTO

165. Permiten determinar si un control se está realizando de la forma prevista en la normas y políticas de seguridad establecidas por el organismo responsable del SI. Su objetivo principal es determinar si el control se realiza y si sus resultados son efectivos.

1.132. PRUEBAS SUSTANTIVAS

166. Permiten confirmar la exactitud de determinadas situaciones o hechos, pero fundamentalmente permiten sustanciar el impacto y alcance de una deficiencia, o incidencia de seguridad, con proyección sobre la integridad de determinada información o de un proceso. Ejemplo: en la revisión de un inventario de copias de respaldo, una prueba de cumplimiento puede determinar si los controles previstos se están cumpliendo o no, pero con una prueba sustantiva, se podría determinar cuántos, y /o cuáles elementos no están incluidos en el inventario.

1.133. PUBLIC CLOUD

167. (en) cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider [ISO/IEC 17788:2014]

1.134. PUERTO SEGURO (SAFE HARBOR)

168. Marco de actuación establecido por Estados Unidos y la Unión Europea para salvar las diferencias entre ambos en tratamiento de la privacidad y la protección de datos. Este marco regula el tratamiento de datos personales de ciudadanos europeos por parte de empresas estadounidenses.

1.135. RANSOMWARE.

169. ("Secuestro" informático). El *ransomware* es un código dañino para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado. El *ransomware* se propaga a través de archivos adjuntos de correo

electrónico, programas infectados y sitios web comprometidos. Un programa de malware *ransomware* también puede ser llamado criptovirus, criptotroyano o criptogusano.

170. Consiste en el secuestro del ordenador (imposibilidad de usarlo) o el cifrado de sus archivos (*Cryptoware*) y la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.

1.136. RAT (REMOTE ACCESS TOOLS)

171. *Remote Access Tools*. Herramientas para acceso remoto. Pieza de software que permite a un "operador" controlar a distancia un sistema como si se tuviera acceso físico al mismo. Aunque tiene usos perfectamente legales, el software RAT se asocia habitualmente con ciberataques o actividades criminales o dañinas. En estos casos, el malware suele instalarse sin el conocimiento de la víctima, ocultando frecuentemente un troyano.

1.137. RECOMENDACIONES

172. Pueden ser parte del informe de auditoría, donde además de incluir las conclusiones de las tareas de auditoría realizadas, e identificar las deficiencias observadas, se pueden incluir sugerencias concretas para la solución de los fallos identificados.

1.138. REQUISITO

173. 1) (DRAE) Circunstancia o condición necesaria para algo.
174. 2) Dentro del contexto de esta guía, son las condiciones, en ocasiones mínimas, a cumplir por los auditores, o en cuanto a la aplicación de una norma.
175. 3) En auditoría se suele indicar que existen "requisitos" o mandatos mínimos que debe cumplir el proceso de auditoría, tales como establecer el alcance y objetivo de la auditoría, realizar un programa de auditoría, y las pruebas relacionadas, así como la emisión de un informe, entre otros.

1.139. REQUISITOS MÍNIMOS DE SEGURIDAD

176. Exigencias necesarias para asegurar la información y los servicios. ENS.

1.140. RESOURCE POOLING

177. (en) Aggregation of a cloud service provider's physical or virtual resources to serve one or more cloud service customers [ISO/IEC 17788:2014]

1.141. RESPONSABILIDAD

178. 1) Obligación o deber de realizar alguna acción.
179. 2) Dentro del contexto de una auditoría, se deben establecer, por ejemplo, responsabilidades mínimas para la función de auditoría interna, responsabilidades del cumplimiento de la metodología de auditoría, y sus requisitos mínimos.
180. 3) El auditor es responsable por la opinión y las conclusiones vertidas en el informe de auditoría.

1.142. RESPONSABLE DE LA INFORMACIÓN

181. Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.
182. **(en) Information Owner.** Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. CNSS Inst. 4009.

1.143. RESPONSABLE DE LA SEGURIDAD

183. El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Persona encargada de velar por la seguridad de la información de la organización. Su labor consiste en estar al día de la evolución tecnológica en la medida en que afecta a la seguridad de la información, estableciendo puentes entre el responsable de seguridad corporativa y los responsables de tecnología.
184. **(en) The Computer Security Program Manager** (and support staff) directs the organization's day-to-day management of its computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the computer security program as well as those external to the organization. NIST Special Publication 800-12.

1.144. RESPONSABLE DEL SERVICIO

185. Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

1.145. RESPONSABLE DEL SISTEMA

186. Persona que se encarga de la explotación del sistema de información.
187. **(en) Information System Owner (or Program Manager).** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. CNSS Inst. 4009, Adapted

1.146. REVERSIBILITY

188. **(en)** process for cloud service customers to retrieve their cloud service customer data and application artefacts and for the cloud service provider to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period [ISO/IEC 17788:2014]

1.147. RIESGO

189. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. ENS.

1.148. ROOTKIT

190. Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos. http://www.alerta-antivirus.es /seguridad/ ver_pag.html?tema=S

191. Tipo de software malicioso que, al instalarse sin autorización, es capaz de pasar desapercibido y tomar el control administrativo de un sistema informático. <http://es.pcisecuritystandards.org>

1.149. SCANNER (SCANNING) ESCANER DE VULNERABILIDADES / ANÁLISIS DE SEGURIDAD DE LA RED

192. Escáner de vulnerabilidades. Programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no.
193. Análisis de seguridad de la red. Proceso mediante el cual se buscan vulnerabilidades en los sistemas de una entidad de manera remota a través del uso de herramientas manuales o automatizadas. Análisis de seguridad que incluyen la exploración de sistemas internos y externos, así como la generación de informes sobre los servicios expuestos a la red. Los análisis pueden identificar vulnerabilidades en sistemas operativos, servicios y dispositivos que pudieran utilizar personas malintencionadas. <http://es.pcisecuritystandards.org>

1.150. SATISFACCIÓN DE AUDITORÍA

194. 1) (DRAE) Satisfacer: Cumplir, llenar ciertos requisitos o exigencias.
195. 2) Dentro del contexto de la auditoría, se refiere a que el programa o plan de auditoría, debe cumplir con los objetivos de auditoría, y las tareas realizadas con éste.

1.151. SALVAGUARDAS (CONTRAMEDIDAS)

196. Procedimiento o mecanismo tecnológico que reduce el riesgo.

1.152. SECUENCIA DE COMANDOS EN SITIOS CRUZADO (XSS)

197. **Cross Site Scripting (XSS)** Esta falla permite a un atacante introducir en el campo de un formulario o código embebido en una página, un "script" (perl, php, javascript, asp) que tanto al almacenarse como al mostrarse en el navegador, puede provocar la ejecución de un código no deseado. <http://www.vsantivirus.com/vul-webcamxp.htm>

1.153. SEGURIDAD DE LA INFORMACIÓN

198. Es la protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas, con el fin de proporcionar confidencialidad, integridad y disponibilidad.
199. Information Security. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]

1.154. SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN

200. Es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. ENS

1.155. SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

201. (en) Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. CNSS Int. 4009.

1.156. SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

202. Capacidad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (Sistema) para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometan la disponibilidad, integridad y/o confidencialidad de los datos almacenados o transmitidos y de los servicios que dichos Sistemas ofrecen o hacen accesibles.

1.157. SEGURIDAD POR DEFECTO

203. El uso ordinario del sistema es sencillo y seguro, de forma que una utilización insegura requiere de un acto consciente por parte del usuario.[RD 3/2010 ENS artículo 19.d]
204. (en) **Security by default**, in software, means that the default configuration settings are the most secure settings possible, which are not necessarily the most user friendly settings. In many cases, security and user friendliness are evaluated based on both risk analysis and usability tests. This leads to the discussion of what the most secure settings actually are. As a result, the precise meaning of "secure by default" remains undefined.[https://en.wikipedia.org/wiki/Secure_by_default]

1.158. SELECCIÓN DE MUESTRAS

205. Se pueden aplicar criterios de muestreo estadístico o no, para seleccionar elementos a revisar en una determinada prueba. La calidad de la muestra y de la selección de los elementos de la muestra puede facilitar el análisis de los resultados de una prueba y también la sustentación de una conclusión de auditoría. Se utiliza fundamentalmente cuando existe una población homogénea de elementos a seleccionar, por ejemplo: cuentas de usuarios.

1.159. SERVICE LEVEL AGREEMENT (SLA)

206. (en) Documented agreement between the service provider and customer that identifies services and service targets NOTE 1—A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier. NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.[ISO/IEC 20000 -1:2011]

1.160. SERVICIO

207. Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

1.161. SERVICIOS ACREDITADOS

208. Servicios prestados por un sistema con autorización concedida por la autoridad responsable, para tratar un tipo de información determinada, en unas condiciones precisas de las dimensiones de seguridad, con arreglo a su concepto de operación. ENS

1.162. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

209. Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. ENS

1.163. SISTEMA DE INFORMACIÓN

210. Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. ENS.
211. (en) Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III.

1.164. SISTEMA DE PROTECCIÓN DE PERÍMETRO (SPP)

212. Combinación de hardware y/o software, denominado Dispositivo de Protección de Perímetro (DPP), cuya finalidad es mediar en el tráfico de entrada y salida en los puntos de interconexión de los Sistemas.

1.165. SISTEMA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

213. Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información que está bajo responsabilidad de una única autoridad.

1.166. SISTEMA TIC

214. Sistema de información que emplea tecnologías de la información y de las comunicaciones.

1.167. SNIFFER/SNIFFING (MONITOR DE RED)

215. (“husmeador”, monitor de red). Programas que monitorizan la información que circula por la red con el objeto de capturar información. Las placas de red tienen un sistema de verificación de direcciones mediante el cual saben si la información que pasa por ella está dirigida o no a su sistema. Si no es así, la rechaza. Un *Sniffer* consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el *Sniffer*). Existen *Sniffers* para capturar cualquier tipo de información específica. Por ejemplo contraseñas de acceso a cuentas, aprovechándose de que generalmente no son cifradas por el usuario. También son utilizados para capturar números de tarjetas de crédito o direcciones de correo. El análisis de tráfico puede ser

utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto). Los buenos *Sniffers* no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo *TCP/IP* (*Transmission Control Protocol*), si pueden ser detectados con algunos trucos. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

1.168. SOFTWARE AS A SERVICE (SAAS)

216. (en) Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type [ISO/IEC 17788:2014]

1.169. SPAM

217. Ver Correo basura.

1.170. SPEAR PHISHING

218. *Spear* (“lanza”) *Phishing* (*fishing* “pescando”) dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniería social sobre la víctima). Ver *Phishing*

1.171. SPOOFING

219. Ver suplantación.

1.172. SPYWARE "SPY SOFTWARE"

220. Ver Programas espía.

1.173. SUFICIENCIA DE LAS EVIDENCIAS

221. Las evidencias que soportan una conclusión deben ser suficientes (bastantes), y relevantes (significativos), para soportar las conclusiones y opinión del auditor.

1.174. SUPERVISIÓN

222. 1) (DRAE) Ejercer la inspección superior en trabajos realizados por otros.

223. 2) Las tareas del equipo de auditoría deben ser supervisadas por el Jefe del equipo de auditoría para asegurar que se ha cumplido con el objetivo de la auditoría dentro del alcance previsto.

1.175. SUPLANTACIÓN

224. (En inglés *Spoofing*), Técnica basada en la creación de tramas *TCP/IP* (*Transmission Control Protocol / Internet Protocol*) utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado

225. http://www.alerta-antivirus.es/seguridad/ver_pag.html?tema=S

226. *Spoofing*. En materia de seguridad de redes, el término *spoofing* es una técnica de suplantación de identidad a través de la Red, llevada a cabo por un intruso generalmente

con usos de código dañino (*malware*) o de investigación. Los ataques de seguridad en las redes a través de técnicas de *spoofing* ponen en riesgo la privacidad de los usuarios que navegan por Internet, así como la integridad de sus datos. De acuerdo a la tecnología utilizada se pueden diferenciar varios tipos de *spoofing*:

- IP spoofing:** Consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
- ARP spoofing:** Es la suplantación de identidad por falsificación de tabla ARP. Las tablas ARP (*Address Resolution Protocol*) son un protocolo de nivel de red que relaciona una dirección de hardware con la dirección IP del ordenador. Por lo tanto, al falsear la tabla ARP de la víctima, todo lo que ésta envíe, será direccionado al atacante.
- DNS spoofing:** Es una suplantación de identidad por nombre de dominio (*Domain Name System*), la cual consiste en una relación falsa entre IP y nombre de dominio.
- Web spoofing:** Con esta técnica el atacante crea una falsa página web, muy similar a la que suele utilizar el afectado con el objetivo de obtener información de dicha víctima como contraseñas, información personal, datos facilitados, páginas que visita con frecuencia, perfil del usuario, etc.
- Mail spoofing:** Suplantación de correo electrónico bien sea de personas o de entidades con el objetivo de llevar a cabo envío masivo de *phishing* o *spam*.
<http://www.inteco.es/glossary/Formacion/Glosario/Spoofing>.

1.176. TENANT

227. (en) One or more cloud service users sharing access to a set of physical and virtual resources [ISO/IEC 17788:2014]

1.177. TIMESTAMP O SELLADO DE TIEMPOS

228. Técnica consistente en marcar con un “sello” la información. El sello identificará el momento en el que se produjo dicha marca.

1.178. TIPO DE INFORMACIÓN

229. Una categoría específica de información (por ejemplo, datos de carácter personal, médicos, financieros, investigaciones, contratos, información delicada, ...). Estos tipos los define una organización y, en algunos casos, vienen definidos por alguna normativa de carácter legal.
230. (en) **Information type.** A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. FIPS 199.

1.179. TRAZABILIDAD

231. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. ENS.

1.180. TROYANO O CABALLO DE TROYA

232. Introducción subrepticia en un medio no propicio, con el fin de lograr un determinado objetivo. DRAE. Diccionario de la Lengua Española.

233. Caballo de Troya o troyano, es un código dañino con apariencia de un programa inofensivo que al ejecutarlo brinda al atacante acceso remoto al equipo infectado, normalmente instalando una puerta trasera (*backdoor*). CCN-CERT IA_09-15 Informe de Amenazas .

1.181. VERIFICACIÓN

234. Cualquiera de las acciones de auditoría encaminadas a la comprobación el cotejo, el contraste y el examen de evidencias, registros y documentos.

1.182. VIRUS

235. Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros. [CCN-STIC-430:2006]

1.183. VULNERABILIDAD

236. Una debilidad que puede ser aprovechada por una amenaza. ENS
237. Error de programación o diseño que permite explotar el sistema de una manera diferente a la original.

1.184. ZONA DESMILITARIZADA

238. *Demilitarized Zone* o *DMZ* Se refiere a una zona o segmento de la red, con requisitos específicos de seguridad, de tal manera que está “aislada” o protegida del resto de sistemas y usuarios de la red. El nombre lo toma de las zonas reservadas entre las líneas de frontera de dos países, en las cuales no se permite presencia militar.

2. ABREVIATURAS

AA	Autoridad de Acreditación
ACL	Access Control List
ADA	Autoridad Delegada de Acreditación
AEPD	Agencia Española de Protección de Datos
AJAX	Asynchronous JavaScript and XML
ANS	Acuerdo de Nivel de Servicio (en inglés, SLA)
ARCO	Conjunto de derechos (Acceso, Rectificación, Cancelación y Oposición), a través de los cuales una persona puede ejercer el control sobre sus datos personales.
ASP	Active Server Pages
ASS	Administrador de Seguridad del Sistema
BD	Base de datos
BIA	Business Impact Analysis. Análisis de impacto en el negocio.
BYOD	Bring Your Own Device
CA	Certification Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CC	Common Criteria for Information Technology Security Evaluation. Criterios Comunes
CCM	Cloud Controls Matrix
CCN	Centro Criptológico Nacional
CCN-CERT	Centro Criptológico Nacional – Computer Emergency Response Team
CERT	Computer Emergency Response Team. Equipo de Respuesta a Incidentes Informáticos o ciberincidentes.
CIO	Chief Information Officer
CIRC	Computer Incident Response Capability. Capacidad de Respuesta a Incidentes Informáticos
CIRT	Computer Incident Response Team. Equipo de Respuesta a Incidentes Informáticos
CISO	Chief Information Security Officer
CLASP	Comprehensive, Lightweight Application Security Process
CMS	Content Management Systems
CR	Carriage Return
CSA	Cloud Security Alliance
CSI	Comité de Seguridad de la Información
CSP	Cloud Service Provider
CSRF /XSRF	Cross Site Request Forgery o falsificación de petición en sitios cruzados
CSV	Código Seguro de Verificación
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone. Zona desmilitarizada
DNS	Domain Name Service (o System)
DoS	Denial of Service
DPP	Dispositivo de Protección de Perímetro

DRS	Declaración de Requisitos de un Sistema
EAL	Evaluation Assurance Level
ENI	Esquema Nacional de Interoperabilidad
ENS	Esquema Nacional de Seguridad
ERI	Equipo de Respuesta a Incidentes
ESMTP	Extended SMTP. Extensiones al protocolo SMTP.
FAQ	Frequently Asked Questions
FIPS	Federal Information Processing Standards
FIREWALL	Cortafuegos
GPG	Gnu PG. Versión libre " open source" de PGP.
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol. Protocolo de transferencia de hipertexto, utilizado habitualmente en navegación web.
HTTPS	Secure Hyper Text Transfer Protocol
IaaS	Infrastructure as a Service
IDPS	Sistema con capacidades de IDS e IPS.
IDS	Intrusion Detection System. Sistema de Detección de Intrusiones. Sistema cuya finalidad es detectar las intrusiones que se han realizado o que están en curso
IIS	Internet Information Server
IMAP	Internet Message Access Protocol. Protocolo de acceso al correo electrónico que mantiene la estructura de carpetas en un servidor centralizado.
IPS	Intrusion Prevention System. Sistema de Prevención de Intrusiones. Su función es prevenir los incidentes antes de que se produzcan
IRT	Incident Response Team. Equipo de Respuesta a Incidentes
ISO	International Organization for standardization
ISSM	Information Systems Security Manager
ISSO	Information System Security Offices
J2EE	Java 2 Enterprise Edition
JSP	Java Server Pages
KRI	Key Risk Indicator. Indicadores críticos de riesgo.
LAMP	Linux, Apache, MySQL y PHP
LDAP	Lightweight Directory Access Protocol . Protocolo de acceso a directorio
LF	Line Feed
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de información
MTA	Mail Transfer Agent. Agente de Transferencia de correo, ubicado en el servidor.
MUA	Mail User Agent. Cliente de correo, ubicado habitualmente en equipos de usuario.
NAT	Network Address Translation. Conversión de una dirección IP de origen y / destino
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PCAP	Packet Capture
PGP	Pretty Good Privacy. Software de cifra y firma de datos ampliamente utilizado para reforzar la integridad y confidencialidad de los datos enviados a través de correo electrónico.

PHPBB	PHP Bulletin Board
POP3	Post Office Protocol v3. Protocolo de descarga de correo desde el MTA hasta el MUA.
POS	Procedimientos Operativos de Seguridad
PPT	Pliego de Prescripciones Técnicas
QoS	Quality of Service. Calidad del servicio.
RAT	Remote Access Tools. Herramientas para acceso remoto
RFI	Remote File Inclusion
RINFO	Responsable de la Información
ROUTER	Enrutador
RPV	Red Privada Virtual
RSEG	Responsable de la Seguridad
RSERV	Responsable del Servicio
RSIS	Responsable del Sistema
RTO	Recovery Time Objective (en español, TRS). Tiempo en el que es necesario restaurar un determinado servicio tras una parada para que ésta no impacte significativamente en el negocio.
SaaS	Software as a Service
SDLC	Software Development Life Cycle
SERT	Security Emergency Response Team. Equipo de Respuesta a Emergencias de Seguridad
SHTTP	Secure HyperText Transfer Protocol. Protocolo de transferencia segura de hiper texto utilizado habitualmente en navegación web en la que intervenga información confidencial (credenciales de usuario, mensajes de correo electrónico, datos bancarios...).
SIEM	Security Information and Event Management. Sistema que permite almacenar los registros (logs) de distintas fuentes de manera segura y correlarlos extrayendo información que podría pasar desapercibida si se analizan los distintos orígenes de información por separado.
SLA	Service Level Agreement (en español, ANS)
SMTP	Simple Mail Transfer Protocol. Protocolo simple de transferencia de correo, utilizado para el envío de correo electrónico.
SNMP	Single Network Management Protocol. Protocolo estándar de Gestión de Red
SOAP	Simple Object Access Protocol. Es un protocolo para acceso a servicios web que define como dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML (eXtensible Markup Language).
SPAM	Correo basura. Información no solicitada, normalmente de carácter publicitario, que se puede recibir por diferentes medios como correo electrónico, foros etc.
SPP	Sistema de Protección de Perímetro
SQL	Structured Query Language
SSL	Secure Sockets Layer. Protocolo de cifra que permite el intercambio seguro de información entre dos extremos, predecesor de TLS.
SSO	Single Sign On
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
SWITCH	Conmutador
TCP/IP	Transmission Control Protocol / Internet Protocol
TERENA	Trans-European Research and Education Networking Associations

TIC	Tecnologías de la Información y las Comunicaciones
TLS	Transport Layer Security. Protocolo de cifra que permite el intercambio seguro de información entre dos extremos
TRS	Tiempo de Recuperación del Sistema (en inglés, RTO)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VoIP	Voz sobre IP
WAF	Web Application Firewall
WASC	Web Application Security Consortium
WASS	Web Application Security Scanner
Webmail	Correo electrónico accesible vía Web
WHID	Web Hacking Incidents Database
XML	eXtended Markup Language
XSS	Cross Site Scripting Secuencia de comandos en sitios cruzado

3. REFERENCIAS

2001/264/CE

Decisión del Consejo de 19 de marzo de 2001 por la que se adoptan las normas de seguridad del Consejo.

CCN-STIC-201

Organización y Gestión para la Seguridad de las TIC

CCN-STIC-402

Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.

CCN-STIC-801

ENS - Responsables y Funciones. 2010.

CCN-STIC-201

Organización y Gestión para la Seguridad de las TIC

CCN-STIC-402

Organización y Gestión para la Seguridad de los Sistemas TIC. Diciembre 2006.

CCN-STIC-801

ENS - Responsables y Funciones. 2011.

CCN-STIC-802

ENS - Guía de Auditoría. Junio 2010.

CCN-STIC-803

ENS - Valoración de los Sistemas. 2011.

CCN-STIC-804

ENS - Guía de Implantación. 2013.

CCN-STIC-805

ENS - Política de Seguridad. 2011.

CCN-STIC-806

ENS - Plan de Adecuación. 2011.

CCN-STIC-807

ENS – Criptología de Empleo. 2015.

CCN-STIC-808

ENS – Verificación del cumplimiento de las medidas. 2011

CCN-STIC-809

ENS -Declaración y certificación de conformidad. 2015.

CCN-STIC-810

ENS - Guía de Creación de un CERT/CSIRT. 2011.

CCN-STIC-811

ENS - Interconexión en el ENS. 2012.

CCN-STIC-812

ENS - Seguridad en entornos y aplicaciones Web. 2011.

CCN-STIC-813

ENS - Componentes Certificados en el ENS. 2012.

CCN-STIC-814

ENS - Seguridad en correo electrónico. 2011.

CCN-STIC-815

ENS - Métricas e indicadores. 2014.

CCN-STIC-817

ENS - Gestión de ciberincidentes. 2015.

CCN-STIC-818

ENS - Herramientas de seguridad en el ENS. 2012.

CCN-STIC-823

ENS - Utilización de servicios en la nube. 2014.

CCN-STIC-825

ENS - Certificaciones 27001. 2013.

CNSS Inst. 4009

National Information Assurance (IA) Glossary. April 2010.

FIPS 200

Minimum Security Requirements for Federal Information and Information Systems. March 2006.

ISO Guide 73

Risk management — Vocabulary. 2009.

ISO/IEC 13335-1:2004

Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

ISO/IEC 27000

Information technology — Security techniques — Information security management system — Overview and vocabulary. 2009.

ISO/IEC 27001

Information technology — Security techniques — Information security management system — Requirements. 2005.

ISO/IEC 27002

Information technology — Security techniques — Code of practice for information security management. 2005.

ISO/IEC 27003

Information technology — Security techniques — Information security management system implementation guidance. 2010.

ISO/IEC 27004

Information technology — Security techniques — Information security management — Measurement. 2009.

ISO/IEC 27005

Information technology — Security techniques — Information security risk management. 2008.

ISO/IEC 27006

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems. 2007.

Ley 11/2007

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Publicado en: BOE número 150 de 23/6/2007, páginas 27150 a 27166 (17 págs.)

Ley 15/1999

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Publicado en: BOE número 298 de 14/12/1999, páginas 43088 a 43099 (12 págs.)

Magerit

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio para las Administraciones Públicas. Versión 3. 2012.

<http://administracionelectronica.gob.es/ctt/magerit>

OM 76/2002

Orden Ministerial número 76/2002, de 18 de abril, por la que se establece la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones. BOE de 29 de abril de 2002.

RD 1720/2007

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE de 19 de enero de 2008.

RD 3/2010

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. BOE de 29 de enero de 2010, modificado por el Real Decreto 951/2015, de 23 de octubre.

RD 4/2010

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010.

SP 800-12

An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. October 1995.

SP 800-30

Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30. July 2002.

SP 800-53

Recommended Security Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 Revision 3. August 2009.

SP 800-100

Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100. October 2006.