GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 804

ENS. Guía de implantación

Junio 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.10.26 12:15:18 +02'00'

NIPO: 785-17-029-1

Fecha de Edición: junio de 2017
AENOR, AUDERTIS, BDO y NUNSYS han colaborado en la revisión del presente documento y sus anexos y José Antonio Mañas ha participado en su realización y modificación.
El Ministerio de Hacienda y Función Pública ha financiado el desarrollo del presente documento y sus anexos.

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

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 (CNI), 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 (CCN) 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.

El 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, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, 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 (STIC) 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.

Junio de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular.
2. El Esquema Nacional de Seguridad establece una serie de medidas de seguridad en su Anexo II que están condicionadas a la valoración (Anexo I) del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión.
3. Estas medidas constituyen un mínimo que se debe implementar, o justificar los motivos por los cuales no se implementan o se sustituyen por otras medidas de seguridad que alcancen los mismos efectos protectores sobre la información y los servicios.
4. Esta guía busca ayudar a los responsables de los sistemas para que puedan implantar rápida y efectivamente las medidas requeridas, sin perjuicio de que empleen recursos propios o recurran a proveedores y productos externos.
5. Para cada medida se proporciona:
   - una descripción más amplia que la proporcionada en el ENS,
   - referencias externas que ayuden a su comprensión y realización,
   - relación con medidas o controles en otros esquemas de seguridad,
   - relación con los principios básicos recogidos en el ENS,

2. NIVELES DE MADUREZ

6. Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez[1] permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.
7. Los niveles identificados son los siguientes:

Nivel	Descripción
L0	Inexistente. Esta medida no está siendo aplicada en este momento.

[1] *CMM - Capability Maturity Model*, Carnegie Mellon University, CMU.

Nivel	Descripción
L1	Inicial / ad hoc. En el nivel L1 de madurez, el proceso existe, pero no se gestiona. La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de alta calidad.
L2	Repetible, pero intuitivo. En el nivel L2 de madurez, la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
L3	Proceso definido. Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.
L4	Gestionado y medible. Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel L3, la confianza era solamente cualitativa.
L5	Optimizado. El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

Tabla 1. Niveles de madurez

8. Como regla general, se exigirá un nivel de madurez en las medidas de seguridad en proporción al nivel de las dimensiones afectadas o de la categoría del sistema:

Nivel de madurez medidas de seguridad	Categoría del sistema de las tecnologías de la información y la comunicación	Nivel de madurez mínimo exigido
Bajo	Básica	L2 - Repetible, pero intuitivo
Medio	Media	L3 - Proceso definido
Alto	Alta	L4 - Gestionado y medible

Tabla 2. Niveles de madurez exigidos en función de la categoría del sistema o nivel de la dimensión de seguridad

3. [ORG] MARCO ORGANIZATIVO

9. Toda organización necesita poder asegurar el alcance de sus objetivos, definiendo funciones y estableciendo responsabilidades y canales de coordinación. Esta estructura permite la gestión día a día de las actividades rutinarias y la resolución ordenada de los incidentes que puedan sobrevenir.
10. Toda estructura organizativa necesita una evaluación constante y un análisis de la respuesta a los incidentes de forma que se aprende de la experiencia, se corrigen defectos o debilidades y se busca la excelencia por medio de la mejora continua.
11. La organización en materia de seguridad no puede sino estar alineada y servir a la misión del organismo, ajustándose a las necesidades de los servicios que se prestan.
12. La carencia de una organización formal y efectiva se traduce en unas prestaciones inciertas, cuyo resultado depende de la fortuna y el buen tino de los miembros de la organización, sin poder asegurar que se vayan a alcanzar los objetivos propuestos, ni tan siquiera pueda decirse que la Organización está bajo control.

3.1 [ORG.1] POLÍTICA DE SEGURIDAD

13. Es un documento de alto nivel que define el significado de “seguridad de la información” en una organización. El documento debe estar accesible y ser conocido por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible. Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos.
14. Establece las autoridades dentro de la organización: roles y funciones. La política tiene carácter de obligado cumplimiento.
15. Guías CCN-STIC:
    - Guía CCN-STIC-801 - ENS Responsables y Funciones

- Guía CCN-STIC-805 – Política de Seguridad
- Guía CCN-STIC-402 - Organización y Gestión para la Seguridad de los Sistemas TIC
- Guía CCN-STIC-201 - Organización y Gestión para la Seguridad de las STIC

16. Son de especial relevancia los siguientes principios básicos:
    - Artículo 5. La seguridad como un proceso integral.
    - Artículo 9. Reevaluación periódica.

17. ISO[2]/IEC 27000
    - 27001:2013
        - 4 – Contexto de la organización
        - 5.2 – Política
        - 5.3 – Roles, responsabilidades y autoridad
    - 27002:2013
        - 6.1.1 - Roles y responsabilidades relativas a la seguridad de la información
        - 18.1.1 - Identificación de legislación aplicable y requisitos contractuales

18. NIST SP 800-53 rev.4
    - [PM-2] Senior Information Security Officer
    - [PM-11] Mission/Business Process Definition

19. Otras referencias:
    - NIST SP 800-12 - An Introduction to Computer Security.

3.2 [ORG.2] NORMATIVA DE SEGURIDAD

20. Conjunto de documentos que, sin entrar en detalles, establecen la forma de afrontar un cierto tema en materia de seguridad. Definen la posición del organismo en aspectos concretos y sirven para indicar cómo se debe actuar en caso de que una cierta circunstancia no esté recogida en un procedimiento explícito o que el procedimiento pueda ser impreciso o contradictorio en sus términos.
21. A veces se denominan “policies” (en inglés).
22. A veces se denominan “standards” (en inglés).

[2] *International Organization for Standardization*. Organización internacional de normalización.

23. Las normas deben centrarse en los objetivos que se desean alcanzar, antes que en la forma de lograrlo. Los detalles los proporcionarán los procedimientos. Las normas ayudan a tomar la decisión correcta en caso de duda.
24. Las normas deben describir lo que se considera uso correcto, así como lo que se considera uso incorrecto.
25. La normativa tiene carácter de obligado cumplimiento. Esto debe destacarse, así como las consecuencias derivadas de su incumplimiento (medidas disciplinarias).
26. Cada norma debe indicar la forma de localizar los procedimientos que se han desarrollado en la materia tratada. Es difícil que la norma cubra todos los procedimientos desarrollados, pero los procedimientos deben indicar la norma o normas que desarrollan.
27. Las normas deben escribirlas personas expertas en la materia, conocedoras de la postura de la Dirección, de las posibilidades y limitaciones de la tecnología correspondiente y con experiencia en los incidentes o situaciones típicas que pueden encontrarse los usuarios. Las normas deben ser revisadas por el departamento de asesoría legal, tanto para evitar el incumplimiento de alguna norma de rango superior, como para introducir registros que puedan ser requeridos como evidencias en caso de conflicto.
28. Las normas deben ser realistas y viables. Deben ser concisas (sin perder precisión) y sin ambigüedades. Deben estar motivadas, ser descriptivas y definir puntos de contacto para su interpretación correcta.
29. Normativa típica:
    - control de acceso: protección de los elementos de autenticación y autorización (contraseñas, tarjetas, etc.)
    - puesto de trabajo despejado y equipos desatendidos
    - protección frente a software malicioso: virus, spyware, adware, etc.
    - desarrollo de aplicaciones (software)
    - instalación de aplicaciones (software)
    - acceso remoto
    - tele-trabajo
    - uso de portátiles
    - gestión de soportes de información removibles (tales como CD, llaves USB, etc.)
    - tratamiento de la información impresa: copias, almacenamiento y destrucción
    - uso del correo electrónico
    - uso de la web
    - problemas de ingeniería social
    - criterios de clasificación de la información
    - tratamiento de información de carácter personal
    - copias de respaldo (back ups)
    - uso de la criptografía

- gestión de claves
- manejo de dispositivos
- cifrado, firma y verificación

- seguridad física
  - uso de las instalaciones
- relaciones con terceros (proveedores externos)
  - acuerdos de confidencialidad
  - cooperación preventiva
  - resolución de incidencias

30. Guías CCN-STIC:
    - Guía CCN-STIC-821 - Normas de Seguridad
31. Son de especial relevancia los siguientes principios básicos:
    - Artículo 7. Prevención, reacción y recuperación.
    - Artículo 9. Reevaluación periódica.
32. ISO/IEC 27000
    - 27002:2013
      - 5.1 – Directrices de gestión de la seguridad de la información
      - 6.1.3 - Contacto con las autoridades
      - 6.1.4 - Contacto con grupos de interés especial
      - 18.1.2 - Derechos de propiedad intelectual (IPR)
      - 18.2.3 - Comprobación del cumplimiento técnico
33. NIST SP 800-53 rev.4
    - Todos los apartados, primer control (XX-1). Por ejemplo, AC-1 “Access Control Policy and Procedures”.
    - PM-15 - Contacts with Security Groups and Associations
34. Otras referencias:
    - The SANS Security Policy Project http://www.sans.org/resources/policies/
    - NIST SP800-12 - An Introduction to Computer Security
    - NSA - Manageable Network Plan

3.3 [ORG.3] PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD

35. Conjunto de documentos que describen paso a paso cómo realizar una cierta actividad. Facilitan las tareas rutinarias evitando que se olviden pasos importantes. Lo que nunca debe ocurrir es que una cierta actividad sólo sepa hacerla una determinada persona; debe estar escrito cómo se hace para que la persona pueda ser remplazada.

36. Un procedimiento puede estar definido (es comunicado a los organismos implicadas, se comprende por su parte y se ejecuta regularmente conforme a lo definido) y un procedimiento puede estar documentado (además de lo anterior, consta en un documento escrito). No todos los procedimientos se requieren que estén documentados, pero sí deberían estarlo los más críticos para la organización.
37. A veces se denominan “guías” o “instrucciones”.
38. Cada procedimiento debe detallar:
    - en qué condiciones debe aplicarse
    - quién es el que debe llevarlo a cabo
    - qué es lo que hay que hacer en cada momento, incluyendo el registro de la actividad realizada
    - cómo identificar situaciones anómalas y cuál es mecanismo para escalar la situación
    - cómo se reportan deficiencias en los procedimientos
39. El conjunto de procedimientos debe cubrir un alto porcentaje (al menos el 80%) de las actividades rutinarias, así como aquellas tareas que se realizan con poca frecuencia, pero exigen seguir unos pasos determinados muy precisos.
40. Nunca se puede decir que hay demasiados procedimientos. Cuantos más, mejor.
41. No obstante, es mejor no tener un procedimiento que tener un procedimiento erróneo o anticuado.
42. Debe existir un mecanismo para que los usuarios accedan rápidamente a una versión actualizada de los procedimientos que les afectan. El uso de la intranet como repositorio de documentos es muy eficaz, aunque hay que prever algunas copias en papel para aquellas actividades que hay que realizar cuando exista un incidente o fallo en la intranet.
43. Debe existir un procedimiento para que los usuarios puedan informar de errores, inexactitudes o carencias en los procedimientos y se tenga en cuenta estas comunicaciones en el proceso de mejora continua.
44. Guías CCN-STIC:
    - Guía CCN-STIC-203 - Estructura y contenido de los procedimientos operativos de seguridad (POS)
    - Guía CCN-STIC-822 - Procedimientos Operativos de Seguridad
45. Son de especial relevancia los siguientes principios básicos:
    - Artículo 9. Reevaluación periódica.
46. ISO/IEC 27000
    - 27002:2013
        - 12.1.1 - Documentación de los procedimientos de operación

- 18.2.3 - Comprobación del cumplimiento técnico

47. NIST SP 800-53 rev.4
    - Todos los apartados, primer control (XX-1). Por ejemplo, AC-1 “Access Control Policy and Procedures”.
    - PM-15 - Contacts with Security Groups and Associations

3.4 [ORG.4] PROCESO DE AUTORIZACIÓN

48. Ningún sistema de información con responsabilidades sobre la información que maneja o los servicios que presta debería admitir elementos no autorizados por cuanto la libre incorporación de elementos socavaría de raíz la confianza en el sistema, al modificar la superficie de ataque y dar pie a nuevas vulnerabilidades susceptibles de ser explotadas.
49. El ENS singulariza una serie de elementos, sin perjuicio de que se aplique siempre la regla de ‘se requiere autorización previa’ con carácter general a todos los componentes durante todo su ciclo de vida:
    a. Utilización de instalaciones, habituales y alternativas.
    b. Entrada de equipos en producción, en particular, equipos que involucren criptografía.
    c. Entrada de aplicaciones en producción.
    d. Establecimiento de enlaces de comunicaciones con otros sistemas.
    e. Utilización de medios de comunicación, habituales y alternativos.
    f. Utilización de soportes de información.
    g. Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA[3], u otros de naturaleza análoga.
    h. Utilización de servicios de terceros, bajo contrato o Convenio.
    i. Utilización de equipos propiedad del usuario (BYOD – *Bring Your Own Device*).
50. El proceso de autorización requiere:
    - que esté definido en la normativa de seguridad la persona o punto de contacto para autorizar un determinado componente o actuación,
    - que exista un mecanismo (por ejemplo, un formulario) para solicitar la autorización, indicando lo que se desea y la motivación; esta solicitud deberá incorporar los siguientes elementos:

[3] *Personal Digital Assistant*. Asistente digital personal

- descripción precisa del elemento o actuación para el que se solicita autorización,
- descripción precisa de las actividades para las que se requiere el nuevo componente,
- justificación de que nuevo componente no afecta a otras funcionalidades del sistema,
- si el nuevo componente introduce posibles vulnerabilidades (es decir, si expone al sistema a nuevas o renovadas amenazas), deberá anexarse un análisis de riesgos y las medidas que se toman para gestionarlo; este análisis de riesgos tendrá la intensidad proporcionada a la categoría del sistema, como se establece en [op.pl.1],
- justificación de que no se viola ninguna normativa de seguridad,
- información de los procedimientos de seguridad que son aplicables al caso o, si fuere necesario, la necesidad de desarrollar algún nuevo procedimiento específico

  - que se requiera la aprobación formal de la petición (o sea, la firma del responsable) antes de la actuación

51. Si se requieren nuevos procedimientos, la autorización puede ser temporal con un plazo límite para desarrollar los nuevos procedimientos y formalizar la autorización definitiva.
52. La autorización sólo cubrirá la utilización de los nuevos recursos para los objetivos explícitamente aprobados.
53. Son de especial relevancia los siguientes principios básicos:
    - Artículo 9. Reevaluación periódica.
54. ISO/IEC 27000
    - 27002:2013
      - 6.1.1 - Roles y responsabilidades relativas a la seguridad de la información
55. NIST SP 800-53 rev.4
    - [PM-10] Security Authorization Process
56. Otras referencias:
    - NIST SP800-12 - An Introduction to Computer Security
    - Manageable Network Plan

4. MARCO OPERACIONAL

57. Medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 [OP.PL] PLANIFICACIÓN

58. Actividades previas a la puesta en explotación.
59. Son de especial relevancia los siguientes principios básicos:
    - Artículo 5. La seguridad como un proceso integral.
    - Artículo 6. Gestión de la seguridad basada en los riesgos.

4.1.1 [OP.PL.1] ANÁLISIS DE RIESGOS

60. Empleamos la expresión “análisis de riesgos” en el sentido de “risk assessment”[4] en la terminología de ISO.
61. El análisis de riesgos permite:
    - validar el conjunto de medidas de seguridad implantado,
    - detectar la necesidad de medidas adicionales y
    - justificar el uso de medidas de protección alternativas.
62. Todo análisis de riesgos debe identificar y priorizar los riesgos más significativos a fin de conocer los riesgos a los que estamos sometidos y tomar las medidas oportunas, técnicas o de otro tipo.
63. El análisis de riesgos debe ser una actividad recurrente; es decir, se debe mantener actualizado.
64. El aspecto formal exige que el análisis esté documentado y aprobado. La documentación debe incluir los criterios utilizados para seleccionar y valorar activos, amenazas y salvaguardas.
65. Un análisis de riesgos debe ser realizado:
    - durante la especificación de un nuevo sistema, para determinar los requisitos de seguridad que deben incorporarse a la solución,
    - durante el desarrollo de un nuevo sistema, para analizar opciones,
    - durante la operación del sistema, para ajustar a nuevos activos, nuevas amenazas, nuevas vulnerabilidades y nuevas salvaguardas.

[4] "Risk Assessment", que incluye la identificación, análisis y evaluación de riesgos, conforme a UNE-ISO 31000.

66. Todo sistema opera bajo una situación de cierto riesgo residual. El riesgo residual debe estar documentado y aprobado por el responsable de la información y del servicio correspondiente(s).

67. Guías CCN-STIC:

    - 470H1 – Manual de usuario PILAR. Análisis y gestión de riesgos
    - 470H2 – Manual de usuario PILAR. Análisis de impacto y continuidad del negocio
    - 472F – Manual de usuario PILAR BASIC
    - 473E – Manual de usuario µPILAR

68. Son de especial relevancia los siguientes principios básicos:

    - Artículo 5. La seguridad como un proceso integral.
    - Artículo 6. Gestión de la seguridad basada en los riesgos.

69. ISO/IEC 27000

    - 27001:2013
        - 6.1 – Acciones para abordar riesgos y oportunidades
        - 6.1.1 - General
        - 6.1.2 – Evaluación de riesgos
        - 6.1.3 – Tratamiento de los riesgos
        - 8.2 - Evaluación de riesgos
        - 8.3 – Tratamiento de los riesgos

70. NIST SP 800-53 rev.4

    - [RA] Risk Assessment
    - [PM-9] Risk Management Strategy

71. Otras referencias:

    - Magerit v3:2012 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información; Ministerio de Administraciones Públicas; Consejo Superior de Administración Electrónica. http:// administracionelectronica.gob.es/
    - UNE 71504 - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información; AENOR Agencia Española de Normalización
    - NIST SP 800-30 - Risk Management Guide for Information Technology Systems
    - NIST SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
    - NIST SP 800-39 - Managing Risk from Information Systems: An Organizational Perspective
    - ISO/IEC 27005 - Information security risk management
    - ISO/IEC 31000 – Gestión del riesgo – Principios y directrices

4.1.2 [OP.PL.2] ARQUITECTURA DE SEGURIDAD

72. Lo que se busca con esta medida de seguridad es tener una visión global, íntegra e integradora de cómo es el sistema de información, cómo se gestiona y cómo se defiende. Esta medida es básicamente documental y descriptiva.

73. La arquitectura de seguridad es elaborada bajo la dirección del Responsable del Sistema, y es aprobada por el Responsable de la Seguridad.

74. Son de especial relevancia los siguientes principios básicos:

    - Artículo 7. Prevención, reacción y recuperación.
    - Artículo 8. Líneas de defensa.

75. ISO 27000

    - 27002:2013
        - 8.1.1 - Inventario de activos
        - 8.1.2 - Propiedad de los activos
        - 13.1.1 - Controles de red
        - 14.2.5 - Principios para la ingeniería de sistemas seguros

76. NIST 800-53 rev.4

    - [CM-8] Information system Component Inventory
    - [PM-5] Information Systems Inventory
    - [PM-7] Enterprise Architecture
    - [PM-8] Critical Infrastucture Plan
    - [SA-5] Information System Documentation
    - [SA-8] Security Engineering Principles
    - [PL-8] Information Security Architecture

77. Otras referencias:

    - Manageable Network Plan

4.1.3 [OP.PL.3] ADQUISICIÓN DE NUEVOS COMPONENTES

78. La adquisición de nuevos componentes debe:

    - tener en cuenta el análisis de riesgos [op.pl.1]
    - ajustarse a la arquitectura de seguridad [op.pl.2]
    - prever los recursos necesarios, esfuerzo y medios económicos para:
        - la implantación inicial.
        - el mantenimiento a lo largo de su vida útil.
        - atender a la evolución de la tecnología.
    - en todo momento se atenderá tanto a las necesidades técnicas como a la necesaria concienciación y formación de las personas que van a trabajar con los componentes.

79. Son de especial relevancia los siguientes principios básicos:
    - Artículo 9. Reevaluación periódica.

80. ISO/IEC 27000
    - 27002:2013
        - 14.1.1 - Análisis de requisitos y especificaciones de seguridad de la información

81. NIST 800-53 rev.4
    - [PL-1] Security Planning Policy and Procedures
    - [PL-2] System Security Plan
    - [PL-7] Security Concept of Operations
    - [PL-8] Information Security Architecture
    - [SA-1] System and Services Acquisition Policy and Procedures
    - [SA-3] System Development Life Cycle
    - [SA-4] Acquisition Process
    - [SA-8] Security Engineering Principles
    - [SA-12] Supply Chain Protection

82. Otras referencias:
    - NIST SP 800-18 - Guide for Developing Security Plans for Federal Information Systems
    - NIST SP 800-65 - Integrating IT Security into the Capital Planning and Investment Control Process

4.1.4 [OP.PL.4] DIMENSIONAMIENTO / GESTIÓN DE CAPACIDADES

83. Conviene destacar que esta medida de seguridad no es meramente técnica, sino que tiene implicaciones presupuestarias y por ello debe gestionarse con tiempo para que las necesidades queden debidamente recogidas en los presupuestos. Si en todas las medidas de seguridad hay que huir de la improvisación, en esta con mayor razón.

84. Nótese que en entornos flexibles como es el empleo de recursos en la nube, el dimensionado efectivo del sistema puede ser dinámico, adecuándose a las necesidades del servicio.

85. ISO/IEC 27000
    - 27002:2013
        - 12.1.3 - Gestión de capacidades

86. NIST SP 800-53 rev.4
    - [SA-2] Allocation of Resources
    - [AU-4] Audit Storage Capacity

4.1.5 [OP.PL.5] COMPONENTES CERTIFICADOS

87. Todas las palabras se quedan cortas para insistir en la necesidad de recurrir a componentes probados, evaluados y certificados. Desarrollar los propios componentes exige un apreciable nivel de formación, un considerable esfuerzo y una capacidad de mantenimiento de la seguridad frente a vulnerabilidades, defectos y nuevas amenazas. Todo esto se simplifica notablemente recurriendo a componentes de terceras partes siempre y cuando dichos componentes estén asegurados para protegernos de acuerdo a nuestras necesidades y frente a nuestras amenazas. Esto quiere decir que antes de adquirir un producto, por muy acreditado que esté, hay que cerciorarse de que cubre nuestras necesidades específicas.

88. El empleo de componentes certificados requiere:

- un esfuerzo preliminar de validación: idoneidad para el caso
- un esfuerzo de implantación: adquisición y formación
- y un esfuerzo continuo de actualizaciones para no perder las garantías iniciales

89. Cuando se evalúan productos, es frecuente establecer una escala de niveles. En el caso de Criterios Comunes (ISO 15408), esta es la escala:

EAL[5]1 – Probado funcionalmente

EAL1 es aplicable cuando se necesita alguna confianza en el funcionamiento correcto pero las amenazas a la seguridad no son importantes. Será útil cuando se necesite garantía independiente en la controversia entre el debido cuidado que se ha ejercido y la protección de la información personal o similar.

EAL1 proporciona una evaluación del TOE[6] disponible para el cliente, incluyendo pruebas independientes sobre una especificación y un examen de los manuales proporcionados. Se piensa que una evaluación EAL1 pueda ser realizada con éxito sin la ayuda del fabricante del TOE y con un gasto mínimo.

Una evaluación a este nivel debe proporcionar evidencia de que el TOE funciona de una manera consistente con su documentación y que proporciona protección útil contra las amenazas identificadas.

EAL2 – Probado estructuralmente

EAL2 necesita la cooperación del fabricante por lo que se refiere a entregar información de diseño y resultados de pruebas, pero no debe exigir más esfuerzo por parte del fabricante de lo que supone una práctica comercial buena. Por tanto, no debe requerir una inversión substancialmente mayor en costes o tiempo.

EAL2 es, por consiguiente, aplicable en aquellas circunstancias en las que fabricantes o usuarios necesitan un nivel de seguridad, entre bajo y moderado, garantizado

[5] *EAL Evaluaton Assurance Level*. Niveles de confianza en la evaluación.
[6] *TOE.Target of Evaluation*. Objetivo de evaluación.

independientemente ante la falta de disponibilidad inmediata del registro de desarrollo completo. Esta situación puede surgir al dar seguridad a sistemas heredados o en los que el acceso al fabricante puede estar limitado.

EAL3 – Probado y verificado metódicamente

EAL3 permite a un fabricante concienzudo obtener garantía máxima de la ingeniería de seguridad en la fase de diseño sin la alteración sustancial de las prácticas de desarrollo válidas existentes.

EAL3 es aplicable en aquellas circunstancias en las que fabricantes o usuarios necesitan un nivel moderado de seguridad garantizado independientemente y una completa investigación del TOE y su desarrollo sin necesidad de reingeniería sustancial.

EAL4 – Diseñado, probado y revisado metódicamente

EAL4 permite a un fabricante obtener garantía máxima de la ingeniería de seguridad basada en correctas prácticas de desarrollo comercial que, aun siendo riguroso, no requiere un conocimiento o destreza especializados sustanciales ni otros recursos. EAL4 es el nivel más alto que permite que sea económicamente factible aplicar CC a una línea de producto ya existente.

EAL4 es, por consiguiente, aplicable en aquellas circunstancias en las que fabricantes o usuarios necesitan un nivel de seguridad, entre moderado y alto, garantizado independientemente de TOEs convencionales y están dispuestos a costear gastos adicionales de ingeniería específica de seguridad.

EAL5 – Diseñado y probado semiformalmente

EAL5 permite a un fabricante obtener garantía máxima de la ingeniería de seguridad basada en prácticas de desarrollo comercial rigurosas apoyadas por una moderada aplicación de técnicas específicas de ingeniería de seguridad. En este caso el TOE probablemente se diseñe y desarrolle con la intención de lograr el nivel de garantía EAL5. Es probable que el coste adicional atribuible a los requisitos de EAL5, comparado al coste que supone un desarrollo riguroso sin la aplicación de técnicas especializadas, no sea grande.

EAL5 es, por consiguiente, aplicable en aquellas circunstancias en las que fabricantes o usuarios necesiten un nivel alto de seguridad, garantizado independientemente, en un desarrollo previsto y requiere un enfoque de desarrollo riguroso sin incurrir en gastos no razonables atribuibles a las técnicas de ingeniería específica de seguridad.

EAL6 – Diseñado, probado y revisado semiformalmente

EAL6 permite a los fabricantes obtener alta garantía de la aplicación de técnicas de ingeniería de seguridad en un entorno de desarrollo riguroso para producir un TOE específico para proteger los recursos de alto valor contra riesgos significativos.

EAL6 es, por consiguiente, aplicable al desarrollo de TOEs de seguridad para su aplicación en situaciones de alto riesgo donde el valor de los recursos protegidos justifica el coste adicional.

EAL7 – Diseñado, probado y revisado formalmente

EAL7 es aplicable al desarrollo de TOEs de seguridad para su aplicación en situaciones de riesgo extremadamente alto y/o donde el alto valor de los recursos justifica el mayor coste. La aplicación práctica de EAL7 se limita actualmente a TOEs con una funcionalidad estrictamente dirigida a la seguridad que permite un extenso análisis formal.

90. El ENS solo requiere la consideración de productos certificados para sistemas de categoría ALTA. No obstante, cabe hacer las siguientes indicaciones:

- Un nivel EAL1 sería recomendable para cualquier sistema.
- Un nivel EAL2 sería aconsejable para sistemas de categoría MEDIA o ALTA.
- Un nivel EAL3 sería interesante para sistemas de categoría ALTA, concretamente para elementos críticos del sistema como puede ser la frontera exterior hacia redes públicas.
- Niveles por encima de EAL3 son siempre interesantes, pero probablemente desproporcionados para sistemas adscritos al ENS, salvo frente a amenazas extremas.

91. Guías CCN-STIC:

- Guía CCN-STIC-813 - Componentes Certificados en el ENS
- Guía CCN-STIC-103 – Catálogo de Productos con certificación criptologica

92. ISO/IEC 27000

93. NIST SP 800-53 rev. 4

94. Otras referencias:

- NIST SP 800-23 - Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- NIST SP 800-36 – Guide to Selecting Information Technology Security Products
- Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
  http://www.oc.ccn.cni.es
- Orden PRE/2740/2007 de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

- ISO/IEC 15408-1:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
- ISO/IEC 15408-2:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- ISO/IEC 15408-3:2005 – Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

- ISO/IEC 18045:2005 - Information technology – Security techniques – Methodology for IT security evaluation
- ISO/IEC TR 19791:2006 - Information technology – Security techniques – Security assessment of operational systems

4.2 [OP.ACC] CONTROL DE ACCESO

95. El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

96. Con el cumplimiento de todas estas medidas se garantiza que nadie accederá a recursos sin autorización. Además, debe quedar registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

97. El control de acceso que se implanta en un sistema real es un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de categoría básica, se prima la comodidad, mientras que en sistemas de categoría alta se prima la protección.

98. Estas medidas suelen venir recogidas en la literatura de seguridad bajo los epígrafes

- I&A – Identificación y Autenticación
- Control de Acceso

4.2.1 [OP.ACC.1] IDENTIFICACIÓN

99. Se debe asignar un identificador singular para cada entidad (usuario o proceso) que accede al sistema y para cada rol de cada entidad frente al sistema (administrador, usuario, etc.).

100. De esta manera:

- se puede saber quién recibe qué derechos de acceso,
- se puede saber quién ha hecho qué, y qué ha hecho para corregir o para perseguir.

101. La identificación de usuarios suele ir asociada a una "cuenta de usuario". A menudo se habla de "derechos de una cuenta" para referirse a los derechos del titular de la cuenta. Se dice que los derechos de un usuario son los de su cuenta en el sistema.

102. Se deben gestionar las cuentas de usuario:

- Las cuentas deben ser inhabilitadas cuando:
  - el usuario deja la organización o
  - cesa en la función para la cual se requería la cuenta de usuario o

- la persona que lo autorizó da orden en contra.

- Las cuentas inhabilitadas deben ser retenidas durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a una cuenta (periodo de retención).
- No deben existir 2 cuentas con el mismo identificador, de forma que no se puedan confundir dos usuarios ni se puedan imputar actividades a usuarios diferentes.

103. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 9.2.1 - Registro y baja de usuario
104. NIST SP 800-53 rev. 4
    - [AC-2] Account Management
    - [AC-14] Permitted Actions without Identification or Authentication
    - [IA-2] Identification and Authentication (Organizational Users)
    - [IA-3] Device Identification and Authentication
    - [IA-4] Identifier Management
    - [IA-5] Authenticator Management
    - [IA-8] Identification and Authentication (Non-Organizational Users)

4.2.2 [OP.ACC.2] REQUISITOS DE ACCESO

105. Es necesario que tanto los sistemas en producción como los previos a su puesta en explotación cuenten con un mecanismo de control de acceso, basado en el identificador asignado a cada entidad (usuario o proceso) y un mecanismo de autenticación.
106. Para definir este control de accesos, debe definirse un documento o matriz donde se especifique cuáles son los componentes del sistema y sus ficheros o registros de configuración y se relacionen con los diferentes permisos de usuario, de manera que únicamente puedan acceder a los recursos los usuarios autorizados.
107. Será el responsable de cada información o servicio, quien especifique los derechos de acceso a los mismos, responsabilizándose de la asignación de autorización y nivel de acceso al mismo.
108. Guías CCN-STIC:
    - Serie CCN-STIC-500 - Guías para Entornos Windows
    - Serie CCN-STIC-600 - Guías para otros Entornos
    - Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles
109. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 9.1.1 - Política de control de acceso

- 9.1.2 - Acceso a redes y servicios en red
- 9.4.1 - Restricción del acceso a la información
- 9.4.4 - Uso de los recursos del sistema con privilegios especiales
- 9.4.5 - Control de acceso al código fuente de los programas

110. NIST SP 800-53 rev. 4
    - [AC-3] Access Enforcement
    - [AC-4] Information Flow Enforcement
    - [AC-6] Least Privilege
    - [AC-24] Access Control Decisions
    - [CM-5] Access Restrictions for Change
    - [MP-2] Media Access
111. Otras referencias:
    - Manageable Network Plan
        - Milestone 5: Control Your Network (User Access)

4.2.3 [OP.ACC.3] SEGREGACIÓN DE FUNCIONES Y TAREAS

112. La segregación de funciones tiene dos objetivos:
    - prevenir errores
    - impedir el abuso de privilegios por parte de los usuarios autorizados

113. Debe documentarse un esquema de funciones y tareas en el que se contemplan las que son incompatibles en una misma persona. La incompatibilidad debe garantizar que para llevar a cabo un proceso o actividad crítica siempre se requieren al menos 2 personas.
114. Debe establecerse un procedimiento de asignación de personas a funciones y tareas a personas que garantice que no se viola el esquema anterior, ni cuando se asignan responsabilidades inicialmente, ni cuando se actualizan.
115. Hay que evitar que las personas que trabajan en la operación diaria del sistema participen en el desarrollo de aplicaciones (desarrolladores) o en su configuración (administradores).
    - nadie puede autorizarse a sí mismo
    - los desarrolladores no pueden modificar datos de explotación
    - los desarrolladores no pueden pasar software a explotación
    - los desarrolladores no pueden configurar software en explotación
    - los operadores ni desarrollan software ni pueden modificar los desarrollos
    - los usuarios ni desarrollan ni pueden modificar los desarrollos
    - los usuarios ni configuran ni pueden modificar la configuración

116. Hay que evitar que las personas que trabajan en la auditoría o supervisión participen en cualquier otra función.
117. Deberá prestarse una especial atención a los roles asociados a cuentas de administración del sistema (administración de equipos, de aplicaciones, de comunicaciones, de seguridad), fragmentando las funciones administrativas entre varias personas cuando la categoría del sistema lo requiera. En todo caso el número de personas con derechos de administración debe ser lo más reducido posible sin menoscabo de la usabilidad del sistema.
118. Guías CCN-STIC:
    - Guía CCN-STIC-801 - ENS Responsables y funciones
119. ISO/IEC 27000
    - 27002:2013:
        - 6.1.2 - Segregación de tareas
120. NIST SP 800-53 rev4:
    - [AC-5] Separation of Duties

4.2.4 [OP.ACC.4] PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

121. En la estructuración de los derechos de acceso se deben en cuenta las necesidades de cada usuario según su función en la organización y las tareas que tiene encomendadas.
122. La necesidad de acceso debe venir por escrito de parte del responsable de la información o proceso al que va a concedérsele acceso.
123. El reconocimiento de la necesidad de acceso debe ser reasegurado periódicamente, extinguiéndose cuando no se demuestre positivamente que la necesidad perdura.
124. Deberá prestarse una especial atención a las cuentas de administración del sistema (administración de equipos, de aplicaciones, de comunicaciones, de seguridad), estableciendo procedimientos ágiles de cancelación y mecanismos de monitorización del uso que se hace de ellas.
125. ISO/IEC 27000
    - 27002:2013:
        - 9.2.2 - Provisión de acceso de usuario
        - 9.2.3 - Gestión de privilegios de acceso
        - 9.2.5 - Revisión de los derechos de acceso de usuario
        - 9.2.6 - Retirada o reasignación de los derechos de acceso
        - 9.4.1 - Restricción del acceso a la información
126. NIST SP 800-53 rev4:

- [AC-3] Access Enforcement
- [AC-24] Access Control Decisions
- [CM-5] Access Restrictions for Change

127. Otras referencias:

- Manageable Network Plan
  - Milestone 5: Control Your Network (User Access)

4.2.5 [OP.ACC.5] MECANISMO DE AUTENTICACIÓN

128. Es el mecanismo que permite validar la identidad de un usuario. Es crítico por cuanto la identificación del usuario es, en general, fácilmente accesible.

129. Típicamente los mecanismos de autenticación recurren:

- a algo que se conoce (un secreto, por ejemplo, una contraseña)
- a algo que se tiene (un objeto, por ejemplo, una tarjeta o una llave)
- a algo que es propio del usuario (características biométricas)

130. A veces estos mecanismos se emplean por pares para dificultar la falsificación y ganar tiempo frente a la pérdida de alguno de los mecanismos. Como, por ejemplo:

- una tarjeta + un PIN[7]
- una tarjeta + una característica biométrica
- una característica biométrica + una contraseña

131. Cada mecanismo tiene sus puntos débiles que deben atajarse por medio de normativa y procedimientos que regulen su uso, periodo de validez y gestión de incidencias tales como la pérdida por parte del usuario legítimo.

Nivel de las dimensiones de seguridad		nivel en I C A T		
		Bajo	Medio	Alto
Factores de autenticación		Un sólo factor	Doble factor de autenticación	
algo que se sabe	contraseñas claves concertadas PIN	ok	con cautela	con cautela

[7] *Personal Identification Number* es un número de identificación personal utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema. Es un tipo de contraseña.

algo que se tiene	*tokens*[8] tarjetas	ok	ok	criptográficos
algo que se es	biometría	ok	ok	ok

Tabla 3. Mecanismos de autenticación según nivel de dimensiones de seguridad

132. Las credenciales deberán activarse una vez estén bajo control efectivo del usuario (por ejemplo, contraseña temporal de un solo uso) y serán única y exclusivamente para dicho usuario, prohibiéndose su divulgación o uso compartido. Es decir, el usuario deberá reconocer que ha recibido las credenciales y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.

133. Las credenciales caducarán con una periodicidad marcada por la política de la organización, aunque la entidad (persona, equipo o proceso) haga uso habitual de ellas.

134. Las credenciales se retirarán y serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican:

- Termina su relación con el sistema
- Tras un periodo definido de no utilización

135. Además, debe contemplarse la posibilidad de que las aplicaciones y otros elementos tecnológicos de seguridad de los que se haga uso, sobre todo si se usan productos comerciales, no tengan la capacidad para permitir una adecuada configuración de los mecanismos de autenticación atendiendo al Esquema Nacional de Seguridad y a la categoría del sistema. Por ello deberán tenerse en cuenta las siguientes opciones:

- Adquirir productos con la capacidad de cumplir los requisitos exigidos.
- Disponer de otros elementos o medidas previas que suplan las carencias de los requisitos exigidos (por ejemplo, autenticación contra LDAP o Directorio Activo, máquinas de salto para autenticarse en elementos de seguridad con configuración limitada, etc.).
- Reemplazar las medidas de seguridad por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos y sea aprobado formalmente por el Responsable de la Seguridad, tal como se indica en el Artículo 27 del Real Decreto 3/2010, de 8 de Enero.

[8]Tarjeta o dispositivo electrónico que utiliza un usuario autorizado para acceder a un sistema informático

Contraseñas (secretos compartidos en general)

136. Características:
    - se pueden olvidar
    - a veces los usuarios las escriben abriendo una oportunidad al conocimiento por robo
    - si el número de posibilidades es reducido y el mecanismo de validación permite probar rápidamente, un atacante puede descubrir el secreto a base de pruebas
    - nótese que la revelación de un secreto puede producirse sin el conocimiento de la parte afectada por lo que el ladrón dispone de una amplia ventana de tiempo para actuar maximizando sus oportunidades
    - la principal ventaja es que son baratas de implantar y fáciles de reemplazar en caso de pérdida

137. Se debe concienciar a los usuarios de los riesgos del uso de contraseñas e instruirles en cómo generarlas y custodiarlas.

138. La expresión "con cautela" empleada más arriba indica que debemos establecer una política rigurosa de empleo de contraseñas como mecanismo de autenticación. Una política incluye los siguientes elementos:
    - La Política de contraseñas debe formalizarse en normativa [org.2] y procedimientos operativos de seguridad [org.3].
    - Debe diferenciar entre contraseñas de usuario y contraseñas con privilegios de administrador.
    - Debe tener en cuenta si se emplea aisladamente o en combinación con otro factor de autenticación.
    - Debe fijar los procesos de creación, distribución, custodia y terminación.
    - Debe establecer las características (patrones) de las contraseñas para considerarse válidas. Por ejemplo, número de caracteres y conjunto admitido y requerido de caracteres.
    - Debe establecer un periodo máximo de validez y un tiempo mínimo de no repetición (por ejemplo, hay que renovarla al menos cada 6 meses y no se puede establecer una contraseña ya utilizada en los últimos 3 años).
    - Deben detectarse los intentos repetidos de utilización y tratarlos como posibles ataques de descubrimiento por el método de prueba-error. Y debe establecerse un procedimiento de actuación que puede ir desde la introducción de un retardo creciente en el mecanismo de validación, hasta la suspensión cautelar de la cuenta.
    - Debe ejecutarse regularmente una aplicación de descubrimiento de contraseñas por fuerza bruta (password cracker), suspendiéndose de oficio todas las contraseñas rotas.

- Deben suspenderse las contraseñas que hayan sido utilizadas con éxito en un proceso de autenticación de doble factor, incluso si el segundo factor ha bloqueado el acceso.
- Deben establecerse planes de concienciación y formación de los usuarios y administradores que emplean contraseñas.

139. Se debe implementar un procedimiento de resolución de incidencias relacionadas incidentes relacionados con contraseñas; en particular debe haber un procedimiento urgente de suspensión de cuenta tras un robo.

Claves concertadas

140. Las claves concertadas son una variante de las contraseñas, que se suponen más cómodas de establecer para el ciudadano usuario.

141. Se entienden por claves concertadas códigos generados previa identificación y autenticación del ciudadano por otros medios. Jurídicamente, el ciudadano expresa su voluntad de utilizar este mecanismo en el proceso de solicitud. Las claves concertadas deberán garantizar que el usuario no puede ser suplantado, ni por otro usuario, ni por la propia Administración. Para ello deberán:

- ser razonablemente robustas frente a ataques de adivinación, tanto por estar asociadas a datos ampliamente conocidos del ciudadano, como por falta de aleatoriedad suficiente en la generación
- ser razonablemente robustas frente a ataques de diccionario
- ser razonablemente robustas frente a ataques de fuerza bruta; es decir, deben disponer de suficiente entropía
- impedir que el ciudadano pueda ser suplantado por su contraparte en la Administración
- seguir un procedimiento de generación que garantice la autenticidad del ciudadano
- seguir un procedimiento de comunicación al interesado que garantice que llega a la persona correcta
- disponer de un procedimiento de comunicación de pérdida o robo que suspenda inmediatamente la operatividad de la clave
- disponer de procedimientos de custodia de los datos de firma y verificación de la firma durante el periodo de validez de la información firmada, incluyendo los instantes de tiempo en que se genera, se suspende y se extingue la validez de la clave concertada

142. A fin de garantizar la robustez, la Administración deberá recurrir a generadores aleatorios que proporcionen suficiente entropía (que hayan tantas claves posibles que sea imposible probarlas todas una por una).

143. Es responsabilidad del usuario custodiar dichas claves de forma segura.

144. El proceso de generación debe garantizar la identidad del sujeto y dejar evidencia documental de las pruebas de identidad empleadas.

145. El procedimiento de distribución debe garantizar que sólo se le facilita al titular legítimo. Por ejemplo:
    - usando una red privada virtual cifrada y autenticada (mp.com.2 y mp.com.3).
    - por doble canal; ej. Internet + teléfono móvil
    - por escrito en sobre cerrado
146. Deben generarse de forma aleatoria para:
    - resistir ataques de adivinación
    - resistir ataques de diccionario

Llaves o tarjetas

147. Características:
    - se pueden perder, accidental o deliberadamente
    - se pueden robar
    - se pueden hacer copias
    - en general, son caras y difíciles de reemplazar en caso de pérdida o deterioro
148. Uso habitual:
    - autenticación frente a terminales (logon)
    - acceso remoto y establecimiento de canales seguros
    - activación de dispositivos criptográficos
    - uso de dos o más tarjetas de activación
    - acceso a instalaciones
149. Parece natural que se potencie el uso del DNI electrónico como mecanismo de autenticación de la persona. Este dispositivo proporciona medios de autenticación criptográficos acreditados. Frente a su uso no autorizado se protege con un PIN de activación. Nótese que el DNI electrónico sólo está capacitado por política para identificar a la persona; el resto del sistema de control y registro de acceso debe implementarse aparte.
150. Otras tarjetas de la administración pueden proporcionar funciones de autenticación del usuario asociadas a las funciones propias de su cargo en el organismo.
151. En sistemas de nivel Alto, se deben utilizar elementos criptográficos hardware que utilicen algoritmos y parámetros acreditados por el Centro Criptológico Nacional. La Guía CCN-STIC-807 Criptografía (claves de autenticación y certificados electrónicos) indica los tipos de clave pública y funciones hash[9] que se pueden utilizar para los diferentes niveles (bajo, medio y alto).

[9] *Hash* o funciones resumen: La función de *hashing* criptográfico es una función (matemática) en la cual un algoritmo conocido toma un mensaje de longitud arbitraria como entrada y produce un resultado de longitud fija (generalmente denominado “código hash” o “resumen de mensaje”).

Biometría

152. Características:
    - normalmente no son secretas, y su robustez depende de que no se pueda suplantar al usuario; esto depende mucho del mecanismo concreto, pero algunos permiten técnicas de reproducción un tanto avanzadas.
    - en general los dispositivos son costosos
    - es difícil de reemplazar en caso de pérdida del control por parte del usuario legítimo

153. Uso habitual:
    - En la autenticación frente a terminales:
        - reconocimiento de huella dactilar
        - reconocimiento facial
        - como doble factor se puede una contraseña o un PIN
    - En el acceso a locales o áreas:
        - reconocimiento de la mano
        - reconocimiento del iris o del fondo del ojo
        - como doble factor se puede utilizar una tarjeta o un PIN

154. Guías CCN-STIC:
    - Guía CCN-STIC-436 - Herramientas de Análisis de Contraseñas
    - Guía CCN-STIC-490 Dispositivos biométricos de huella dactilar
    - Guía CCN-STIC-807 - Criptología de Empleo en el ENS
    - Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles

155. ISO/IEC 27000
    - 27002:2013:
        - 9.2.4 - Gestión de la información secreta de autenticación de usuarios
        - 9.3.1 - Uso de la información secreta de autenticación
        - 9.4.3 - Sistema de gestión de contraseñas

156. NIST SP 800-53 rev4:
    - [IA-2] Identification and Authentication (Organizational Users)
    - [IA-3] Device Identification and Authentication
    - [IA-5] Authenticator Management
    - [IA-7] Cryptographic Module Authentication
    - [IA-8] Identification and Authentication (Non-Organizational Users)

157. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.5 - Controlled Use of Administrative Privileges
  - CSC.14 - Controlled Access Based on the Need to Know
- Password Policy, SANS Institute
  http://www.sans.org/resources/policies/Password_Policy.pdf

4.2.6 [OP.ACC.6] ACCESO LOCAL (LOCAL LOGON)

158. La mayor parte de las medidas requeridas se pueden conseguir simplemente configurando los puestos de usuario según se indica.
    - Como manera preventiva, la información que se visualiza antes de acceder a un sistema deberá procurar ser la menos posible para evitar dar a conocer qué información puede encontrar dentro alguien pueda estar tentado de vulnerar el sistema. Por tanto, es recomendable que se muestre meramente el diálogo de acceso y en todo caso algo de información comercial sin valor relacionada con la información manejada. Por ejemplo, deberá evitarse texto de tipo advertencia por estar a punto de entrar a un portal o aplicación que contiene información confidencial de un determinado tipo, ya que habitualmente estas advertencias pueden atraer a usuarios no autorizados.
    - Limitar el número de intentos de acceso para bloquear la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos, ya sea mediante bloqueo de la cuenta o retardo de la solicitud de contraseña.
    - Guardar un registro o log de los accesos realizados a un sistema, tanto los accesos correctos como aquéllos realizados erróneamente. Esto último es especialmente importante de cara a detectar continuos intentos de vulnerar el sistema (mediante por ejemplo ataques de fuerza bruta), ya sea mediante revisiones periódicas de los registros (logs) o con herramientas automatizadas que detecten este tipo de eventos.
    - El usuario deberá tener conocimiento de las obligaciones tras acceder satisfactoriamente a un sistema (por ejemplo, una ventana emergente). En caso de que el sistema no permita notificar inmediatamente tras el acceso, deberá notificársele por otras vías compensatorias (por ejemplo, un correo electrónico tras el alta en el sistema).
159. El sistema debe informar al usuario del último acceso con éxito realizado con su identidad (fecha y hora), una vez haya obtenido acceso. Este mecanismo (que puede ser implementado mediante diferentes mecanismos como: pop-up, correo electrónico, SMS, etc.) permitirá al usuario detectar si su cuenta de usuario ha sido comprometida y pueda activar el procedimiento de resolución de incidentes relacionados con contraseñas. Por ejemplo, tras un periodo de inactividad en la cuenta (vacaciones, bajas, etc.), si al usuario se le notifica un acceso reciente sabrá inmediatamente que alguien ha suplantado su identidad en el sistema.

160. En caso de no ser posible la implementación de este aviso de manera proactiva por parte del sistema, se deberán establecer los mecanismos necesarios para que el usuario pueda consultar el registro de accesos.

161. Se deberá controlar que el acceso a los sistemas se restrinja en determinados momentos (por ejemplo, días festivos, fin de la jornada laboral, etc.) y lugares (direcciones IP fuera del dominio de seguridad, teletrabajo, equipos no autorizados, etc.), para evitar accesos no supervisados que puedan generar modificaciones o fraudes clandestinos o no autorizados.

162. No obstante, es posible que existan sistemas que no requieran limitar el acceso (por ejemplo, porque precisamente el propósito del sistema sea ser accesible en cualquier momento y lugar), pero deberá estar debidamente documentada esta casuística.

163. El requisito de que en ciertos puntos se requiera una identificación singular no es alcanzable por medio de configuración del puesto del usuario, sino que requiere instrumentar workflow de los procesos. Como regla general, estos puntos deben ser pocos y el sistema no debe memorizar la identidad del usuario, sino que debe verificarla cada vez.

164. Como ejemplo, piense en la firma electrónica que se exige en banca por Internet cada vez que queremos realizar una transferencia; esta 'firma' complementa la identificación y autenticación de la sesión de usuario. Esta verificación puntual acota la ventana de riesgo ante un posible robo de sesión.

165. Guías CCN-STIC:

- Serie CCN-STIC-500 Guías para Entornos Windows
- Serie CCN-STIC-600 Guías para otros Entornos

166. ISO/IEC 27000

- 27002:2013:
  - 9.4.2 - Procedimientos seguros de inicio de sesión

167. NIST SP 800-53 rev4:

- [AC-7] Unsuccessful Login Attempts
- [AC-8] System Use Notification
- [AC-9] Previous Login Notification
- [IA-5] Authenticator Management
- [IA-6] Authenticator Feedback
- [SI-11] Error Handling

4.2.7 [OP.ACC.7] ACCESO REMOTO (REMOTE LOGIN)

168. El acceso remoto es fuente de numerosos problemas porque no puede suponer el mismo nivel de controles de seguridad física que en las instalaciones corporativas. Por ello conviene tener reglas específicas respecto a qué se puede hacer y qué no

se puede hacer desde un acceso remoto. E incluso dentro de lo que está autorizado, hay que esmerarse en el cuidado del proceso de identificación y autenticación para prevenir la suplantación de la identidad de un usuario autorizado.

169. Se exige establecer un mecanismo robusto de identificación y autenticación según [op.acc.6]
170. Prácticamente se exige establecer una red privada virtual (VPN), según [mp.com.2] y [mp.com.3].
171. Se debe redactar una política que rija lo que se puede hacer remotamente: qué aplicaciones se pueden usar, qué datos son accesibles y en qué condiciones estos datos pueden almacenarse en el dispositivo externo de acceso.
172. La política también debe establecer límites al tiempo que puede estar abierta una sesión y e imponer un tiempo máximo para cerrar sesiones inactivas.
173. Además de redactar la política, hay que imponerla. Esto es casi imposible si el dispositivo es del usuario (BYOD[10)] y en general si el usuario tiene derechos de administrador del equipo. Es por ello que se procurará que el equipo remoto sea propiedad del organismo, esté configurado por el organismo y el usuario no tenga derechos de administrador.
174. A fin de limitar lo que se puede hacer en remoto, se debe establecer un filtro, bien en el servidor, bien en el propio cliente.
175. Si las limitaciones se imponen en el servidor, haremos que el usuario acceda a un segmento de red separado del núcleo corporativo y entre el segmento de acceso remoto y el núcleo estableceremos un cortafuegos interno que sólo permita las aplicaciones y protocolos autorizados.
176. Si las limitaciones se imponen en el equipo cliente, instalaremos un cortafuegos personal, configurado por el organismo, que establezca las limitaciones correspondientes.
177. En ambos escenarios se debe considerar la oportunidad de instalar una función de prevención de fuga de datos (DLP[11)] que monitorice los datos que viajan por la red.
178. En todos los casos se deben activar los registros de actividad y analizar regularmente que se cumple la política autorizada. Considere la oportunidad de un sistema de información de seguridad y administración de eventos (SIEM[12]) que levante alarmas y centralice su reporte.
179. Guías CCN-STIC:
    - Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles

[10] *Bring your own device.*
[11] *Data Loss Prevention*.
[12] *Security Information and Event Management*

180. ISO/IEC 27000
    - 27002:2013:
        - 9.4.2 - Procedimientos seguros de inicio de sesión
        - 10.1.1 - Política de uso de los controles criptográficos
        - 13.1.1 - Controles de red
        - 13.1.2 - Seguridad de los servicios de red
        - 18.1.5 - Regulación de los controles criptográficos

181. NIST SP 800-53 rev4:
    - [AC-10] Concurrent Session Control
    - [AC-17] Remote Access
    - [AC-18] Wireless Access
    - [AC-20] Use of External Information Systems
    - [MA-4] Nonlocal Maintenance
    - [SA-9] External Information System Services
    - [SC-10] Network Disconnect

182. Otras referencias:
    - http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf
    - http://www.sans.org/security-resources/policies/Remote_Access.pdf
    - http://www.sans.org/reading_room/whitepapers/vpns/remote-access-vpn-security-concerns-policy-enforcement_881

4.3 [OP.EXP] EXPLOTACIÓN

4.3.1 [OP.EXP.1] INVENTARIO DE ACTIVOS

183. El inventario debe cubrir todo el dominio de seguridad del responsable de la seguridad del sistema de información, hasta alcanzar los puntos de interconexión y los servicios prestados por terceros. La granularidad debe ser suficiente para cubrir las necesidades de reporte de incidentes y para hacer un seguimiento, tanto formal (auditorías) como reactivo en el proceso de gestión de incidentes.
    - Identificación del activo: fabricante, modelo, número de serie
    - Configuración del activo: perfil, política, software instalado
    - Software instalado: fabricante, producto, versión y parches aplicados
    - Equipamiento de red: MAC, IP asignada (o rango)
    - Ubicación del activo: ¿dónde está?
    - Propiedad del activo: persona responsable del mismo

184. ISO/IEC 27000
    - 27002:2013:

- 8.1.1 - Inventario de activos
- 8.1.2 - Propiedad de los activos

185. NIST SP 800-53 rev4:
    - [CM-8] Information System Component Inventory
    - [PM-5] Information System Inventory
186. Otras referencias:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.1 - Inventory of Authorized and Unauthorized Devices
        - CSC.2 - Inventory of Authorized and Unauthorized Software

4.3.2 [OP.EXP.2] CONFIGURACIÓN DE SEGURIDAD

187. Todos los sistemas deben ser configurados de forma sistemática antes de entrar en producción. El organismo debe elaborar unos pocos perfiles de configuración para las diferentes actividades a que pueden ser dedicados, siendo típicos los siguientes:
    - usuarios normales (uso administrativo)
    - atención a clientes
    - gestión de proveedores (incluidos bancos)
    - desarrollo
    - operadores y administradores (técnicos de sistemas)
    - responsable de seguridad (consola de configuración)
    - auditoría
188. La medida se instrumenta por medio de una lista de verificación (checklists) que se debe aplicar sistemáticamente a cada equipo antes de entrar en producción.
189. En todos los perfiles de usuario, excepto en los de administrador, se debe bloquear la opción de que éste pueda cambiar la configuración del sistema o pueda instalar nuevos programas o nuevos periféricos (drivers).
190. La configuración de seguridad debe incluir un perfil básico de auditoría de uso del equipo.
191. Guías CCN-STIC:
    - Serie CCN-STIC-500 - Guías para Entornos Windows
    - Serie CCN-STIC-600 - Guías para otros Entornos
    - Guía CCN-STIC-824 - Informe del Estado de Seguridad
    - Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles
192. ISO/IEC 27000
193. NIST SP 800-53 rev4:
    - [CM-2] Baseline Configuration
    - [CM-6] Configuration Settings

- [CM-7] Least Functionality
- [SI-5] Security Alerts, Advisories, and Directives

194. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.3 - Secure Configurations for Hardware and Software
  - CSC.9 - Limitation and Control of Network Ports
  - CSC.18 - Application Software Security

- FDCC - Federal Desktop Core Configuration
  http://nvd.nist.gov/fdcc/index.cfm

- USGCB - The United States Government Configuration Baseline
  http://usgcb.nist.gov/

- Manageable Network Plan
  - Milestone 7: Manage Your Network, Part II (Baseline Management)

4.3.3 [OP.EXP.3] GESTIÓN DE LA CONFIGURACIÓN

195. Por encima de la configuración de cada equipo, hay que tener una visión integral del sistema, de los equipos que trabajan coordinadamente, de la estructura de líneas de defensa en profundidad y de la dinámica del sistema: su evolución temporal desde el punto de vista de arquitectura del sistema y desde el punto de vista de actualizaciones de los componentes.

196. Los cambios deben ser controlados y la configuración debe ir a la par.

197. NIST SP 800-53 rev4:

- [CM-3] Configuration Change Control
- [CM-9] Configuration Management Plan

198. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.3 - Secure Configurations for Hardware and Software
- NIST 800-128 Guide for Security-Focused Configuration Management of Information Systems

4.3.4 [OP.EXP.4] MANTENIMIENTO

199. Proactivamente se deberá estar informado de los defectos anunciados por parte del fabricante o proveedor (como por ejemplo mediante suscripciones a listas de correo o RSS, consultando noticias en webs de tecnología, seguridad o fabricantes, etc.).

200. Deberá existir un procedimiento para establecer cuándo implantar los cambios y determinar su prioridad y urgencia proporcionada al riesgo que implica su no aplicación (cambios preaprobados, cambios de emergencia, etc.).

201. Guías CCN-STIC:

- Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles

202. ISO/IEC 27000

- 27002:2013:
  - 11.2.4 - Mantenimiento de los equipos
  - 12.6.1 - Gestión de las vulnerabilidades técnicas

203. NIST SP 800-53 rev4:

- [CA-2] Security Assessments
- [CA-7] Continuous Monitoring
- [CA-8] Penetration Testing
- [MA-2] Controlled Maintenance
- [MA-3] Maintenance Tools
- [MA-4] Nonlocal Maintenance
- [MA-5] Maintenance Personnel
- [MA-6] Timely Maintenance
- [RA-5] Vulnerability Scanning
- [SI-2] Flaw Remediation
- [SI-4] Information System Monitoring
- [SI-5] Security Alerts, Advisories, and Directives

204. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.4 - Continuous Vulnerability Assessment and Remediation
  - CSC.20 - Penetration Tests and Red Team Exercises
- NIST SP 800-40 - Creating a Patch and Vulnerability Management Program
- Manageable Network Plan
  - Milestone 6: Manage Your Network, Part I (Patch Management)

4.3.5 [OP.EXP.5] GESTIÓN DE CAMBIOS

205. Debe existir un procedimiento para cambiar componentes del sistema que requiere:

- la aprobación del responsable,
- la documentación del cambio,
- pruebas de la seguridad del sistema tras el cambio, en un entorno equivalente que no esté en producción (o se encuentre aislado del mismo)
- la retención de una copia del componente previo por un tiempo prestablecido

- copias de seguridad de los componentes software, cubriendo al menos la versión actual y la inmediata anterior
- se actualiza el inventario de activos
- se actualizan los procedimientos operativos relacionados con el componente actualizado
- se actualiza el plan de continuidad de negocio (si existe tal plan; ver [op.cont])

206. ISO/IEC 27000
    - 27002:2013:
        - 12.1.2 - Gestión de cambios
        - 14.2.2 - Procedimientos de control de cambios en el sistema
        - 14.2.3 - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
207. NIST SP 800-53 rev4:
    - [CA-5] Plan of Action and Milestones
    - [CM-4] Security Impact Analysis
    - [CM-5] Access Restrictions for Change
    - [MA-2] Controlled Maintenance
    - [SI-2] Flaw Remediation
    - [SI-7] Software, Firmware, and Information Integrity
208. Otras referencias:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.4 - Continuous Vulnerability Assessment and Remediation

4.3.6 [OP.EXP.6] PROTECCIÓN FRENTE A CÓDIGO DAÑINO

209. Deben monitorizarse los puntos de entrada y de salida de código dañino, primero para no vernos afectados y segundo para no expandir la infección.
210. Debe concienciarse al personal para detectar comportamiento sospechoso y establecer canales para reportarlo.
211. Deben establecerse procedimientos para reaccionar prestamente a detecciones o simples sospechas, aislar el problema recopilando evidencias suficientes para el análisis forense y el reporte a las autoridades pertinentes. Es decir, conectar con el proceso de gestión de incidencias.
212. ISO/IEC 27000
    - 27002:2013:
        - 12.2.1 Controles contra el código malicioso
213. NIST SP 800-53 rev4:
    - [SC-18] Mobile Code
    - [SI-3] Malicious Code Protection
214. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.8 - Malware Defenses
- NIST SP 800-28 - Guidelines on Active Content and Mobile Code
- NIST SP 800-83 - Guide to Malware Incident Prevention and Handling

4.3.7 [OP.EXP.7] GESTIÓN DE INCIDENTES

215. Hay que establecer un proceso de gestión que instrumente las siguientes actividades:
    - reporte de eventos de seguridad y debilidades detectados por los usuarios, detallando los criterios de clasificación y el escalado de la notificación
    - reporte de incidentes reportados por proveedores externos (terceras partes)
    - se informa a los usuarios potencialmente afectados
    - se informa a los proveedores potencialmente afectados
    - se toman medidas urgentes para contener el problema, evitar que crezca dentro de la organización e impedir que se transmita a otras organizaciones (como detener servicios, aislar el sistema, protección de registros etc.)
    - se reparan daños
216. También hay que ejecutar una serie de actividades de carácter administrativo:
    - recopilación de evidencias para analizar, aprender y reportar a los órganos de gestión
    - se documenta el incidente, su análisis y los pasos seguidos para su resolución
    - se actualizan los procedimientos operativos de seguridad afectados para evitar que se repita el incidente incluyendo información al usuario para la correcta identificación y forma de tratar el incidente
    - se actualizan los planes de continuidad afectados
    - se incluye la notificación al CCN-CERT cuando el incidente sea de impacto significativo en la seguridad de la información manejada y de los servicios prestados (artículo 36 del ENS)
217. Procedimiento que establece identificar si el incidente afecta a ficheros con datos de carácter personal y, en caso de que así sea, está alineado o integrado con el proceso de gestión de incidentes de datos personales.
218. Se recopilarán datos sobre el tiempo de cierre de los incidentes que permitan poder valorar posteriormente el sistema de gestión de incidentes.
219. Para sistemas de nivel ALTO, a efectos de monitorizar el desempeño del proceso de resolución de incidentes, se recopilarán datos sobre recursos consumidos para la resolución del incidente (horas/presupuesto).
220. En el análisis del incidente conviene identificar la causa raíz o causa última por la que se ha sido origen del incidente. Esta caracterización se incorporará a las métricas de eficacia, identificándose debilidades recurrentes y elaborando un plan para su remedio.
221. Guías CCN-STIC:

- Guía CCN-STIC-403 - Gestión de Incidentes de Seguridad informática
- Guía CCN-STIC-817 - Gestión de Ciberincidentes
- Guía CCN-STIC-824 - Informe del Estado de Seguridad
- Guía CCN-STIC-845A - LUCIA. Manual de Usuario
- Guía CCN-STIC-845B - LUCIA. Manual de Usuario con Sistema de Alerta Temprana (SAT)
- Guía CCN-STIC-845C - LUCIA. Manual Instalación Organismo
- Guía CCN-STIC-845D - LUCIA. Manual de Administrador

222. ISO/IEC 27000

- 27002:2013:
  - 6.1.3 - Contacto con las autoridades
  - 6.1.4 - Contacto con grupos de interés especial
  - 16.1 - Gestión de incidentes de seguridad de la información y mejoras

223. NIST SP 800-53 rev4:

- [IR] Incident Response
- [PM-15] Contacts with Security Groups and Associations
- [SI-5] Security Alerts, Advisories, and Directives

224. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.19 - Incident Response and Management
- NIST SP 800-61 – Computer Security Incident Handling Guide
- ISO/IEC TR 18044:2004 - Information technology – Security techniques – Information security incident management

4.3.8 [OP.EXP.8] REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

225. Se realiza una inspección regular de los registros para identificar anomalías en el uso de los sistemas (uso irregular o no previsto)

226. Se utilizan herramientas automáticas para recoger y analizar los registros en busca de actividades fuera de lo normal (por ejemplo: consola de seguridad centralizada, SIEM[13]).

227. Guías CCN-STIC:

- Guía CCN-STIC-434 - Herramientas para el análisis de ficheros de log

228. ISO/IEC 27000

- 27002:2013:
  - 12.4.1 - Registro de eventos
  - 12.4.3 - Registros de administración y operación

[13] *Security Information and Event Mangement*

229. NIST SP 800-53 rev4:
    - [AU] Audit and Accountability
230. Otras referencias:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.16 - Account Monitoring and Control

4.3.9 [OP.EXP.9] REGISTRO DE LA GESTIÓN DE INCIDENTES

Categoría MEDIA

231. Se registrarán todas las actuaciones relacionadas con la gestión de incidentes: el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
232. Guías CCN-STIC:
    - Guía CCN-STIC-845A - LUCIA. Manual de Usuario
    - Guía CCN-STIC-845B - LUCIA. Manual de Usuario con Sistema de Alerta Temprana (SAT)
    - Guía CCN-STIC-845C - LUCIA. Manual Instalación Organismo
    - Guía CCN-STIC-845D - LUCIA. Manual de Administrador
233. ISO/IEC 27000
    - 27002:2013:
        - 16.1.5 - Respuesta a incidentes de seguridad de la información
        - 16.1.7 - Recopilación de evidencias
234. NIST SP 800-53 rev4:
235. Otras referencias:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.19 - Incident Response and Management

4.3.10 [OP.EXP.10] PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

236. Se deberán retener los registros de manera adecuada:
    - existe una declaración formal de los periodos de retención habituales
    - existe un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención
    - existe un procedimiento formal para la retención de evidencias tras un incidente
237. Existen mecanismos que garanticen la corrección de la hora a la que se realiza el registro, en prevención de manipulaciones de los relojes
238. Únicamente el personal autorizado podrá modificar o eliminar los registros:

- existen mecanismos para prevenir el acceso a los registros de personas no autorizadas
- existen mecanismos para prevenir el acceso de personas no autorizadas a la configuración del sistema para el registro automático de actividades
- existe un procedimiento para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad

239. Los registros están contemplados en los procesos de copias de seguridad, garantizando las seguridades antes mencionadas.

240. ISO/IEC 27000

- 27002:2013:
  - 12.4.2 - Protección de la información de registro
  - 12.4.4 - Sincronización del reloj

241. NIST SP 800-53 rev4:

- [AU-8] Time Stamps
- [AU-9] Protection of Audit Information

242. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.6 - Maintenance, Monitoring, and Analysis of Audit Logs

- NIST SP 800-92 - Guide to Computer Security Log Management

4.3.11 [OP.EXP.11] PROTECCIÓN DE LAS CLAVES CRIPTOGRÁFICAS

243. Las claves deben generarse en un equipo y después trasladarse al equipo en el que se van a usar. Los elementos de generación que no son necesarios para el uso se quedarán en el equipo de generación. Es muy recomendable emplear un soporte de información (por ejemplo, un disco USB o una tarjeta de memoria) para trasladar las claves.

244. Cuando una clave se retira de explotación, la política marcará durante cuánto tiempo se debe retener, bien por razones operativas, bien como prueba de auditoría. El motivo operacional más habitual se da en claves de descifrado cuando se requiere poder descifrar información cifrada con claves antiguas. Un motivo de auditoría frecuente se da en claves de verificación de firma electrónica cuando puede ser necesario validar firmas realizadas en el pasado.

245. Es muy recomendable que las claves que se retienen estén en equipos separados (medios aislados de explotación). Para su uso se trasladará la información al equipo donde estén.

246. En resumen, se deben proteger las claves criptográficas durante todo su ciclo de vida:

- generación

- se debe garantizar que las claves generadas son imprevisibles
- con programas evaluados o dispositivos criptográficos certificados conforme a [op.pl.5] (para sistemas de categoría media o superior)
- los medios de generación deben estar aislados de los medios de explotación

- transporte o distribución al punto de utilización
  - se debe asegurar la confidencialidad de la clave y la autenticidad del receptor
  - entrega en mano
  - uso de contenedores físicos seguros
  - uso de contenedores criptográficos (para sistemas de categoría media o superior)
  - doble canal: clave y datos de activación por separado
- custodia en explotación
  - se debe garantizar la confidencialidad de la clave en los dispositivos o aplicaciones que la emplean
  - se debe procurar su cambio cuando el volumen de datos cifrados o el tiempo que lleva en uso superen los parámetros recomendados antes de que un atacante pueda descubrirla por análisis de los datos cifrados
  - en tarjeta inteligente protegida por contraseña (para sistemas de categoría media o superior)
  - en dispositivo criptográfico certificado con control de acceso (para sistemas de categoría media o superior)
- archivo: copias de seguridad de claves activas y retención de claves retiradas de explotación activa
  - en contenedores físicos seguros (por ejemplo, caja fuerte)
  - en contenedores criptográficos (para sistemas de categoría media o superior)
  - en medios alternativos aislados de los medios de explotación
- destrucción
  - eliminación de original y copias
  - se debe garantizar su destrucción, aunque por política puede requerirse su retención durante un periodo a efectos de auditoría
  - en el caso de retención, debe garantizarse la confidencialidad de la clave controlando su acceso

247. Guías CCN-STIC:
    - Guía CCN-STIC-807 – Criptografía de empleo en el ENS
248. ISO/IEC 27000
    - 27002:2013:
      - 10.1.2 - Gestión de claves

249. NIST SP 800-53 rev4:
    - [SC-12] Cryptographic Key Establishment and Management
    - [SC-17] Public Key Infrastructure Certificates
250. Otras referencias:
    - NIST SP 800-57 Recommendation for Key Management

4.4 [OP.EXT] SERVICIOS EXTERNOS

251. Medidas para proteger al sistema de posibles perjuicios derivados de la contratación de determinados servicios a proveedores externos.
252. La Organización puede delegar funciones, pero nunca la responsabilidad sobre la información y los servicios.
253. Un problema que debe quedar resuelto es el de alineamiento de los procesos de la organización contratante y los procesos del proveedor externo, estableciendo puntos de contacto y protocolos de comunicación. Esto incluye tanto los procesos organizativos como los procesos operacionales.
254. Guías CCN-STIC:
    - Guía CCN-STIC-823 - Seguridad en entornos *cloud*
    - ITS correspondiente (pendiente de publicación)

4.4.1 [OP.EXT.1] CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO

255. Debe realizarse un análisis de riesgos que identifique los riesgos asociados al proveedor externo.
256. Debe establecerse un contrato formal, aprobado por ambas partes y actualizado periódicamente estableciendo:
    - detalle por parte del proveedor de las características del servicio a prestar, de modo que quede constancia de que abarca los requisitos de servicio y seguridad requeridos
    - roles y funciones en ambas partes, en materia de seguridad, incluyendo los mecanismos de contacto (teléfono, e-mail, etc.)
    - obligaciones de cada parte
    - responsabilidades de cada parte
    - detalle del acuerdo de nivel de servicio (SLA) y consecuencias de su incumplimiento
    - protocolo de aviso previo de actuaciones que puedan impactar a la otra parte
    - mecanismos y procedimientos para la sincronización de las actividades de gestión de incidencias
    - un conjunto de indicadores para evaluar el servicio prestado

257. También hay que tener preparado un procedimiento de desconexión o terminación de la provisión del servicio. En este escenario es especialmente

importante la recuperación de la información dentro del RPO[14] establecido y la destrucción de la información en los equipos del proveedor saliente (según [mp.si.5]).

258. ISO/IEC 27000
    - 27002:2013
        - 13.2.2 - Acuerdos de intercambio de información
        - 13.2.4 - Acuerdos de confidencialidad o no revelación
        - 15.1 - Seguridad en la relación con proveedores
259. NIST SP 800-53 rev4:
    - [SA-9] External Information System Services
260. Otras referencias:
    - Modelos de contrato de prestación de servicios (CSAE)
    - NIST SP 800-35 – Guide to Information Technology Security Services

4.4.2 [OP.EXT.2] GESTIÓN DIARIA

261. A partir de una serie de indicadores, se establece un plan de reporte y seguimiento con puntos de alarma cuando se superen ciertos umbrales. Estas alarmas dispararán procedimientos de resolución y de escalado, tratándose como una incidencia que debe resolverse.
262. El proceso de resolución de la incidencia levantada por una alarma se regirá según [op.exp.7] y [op.exp.9]
263. Guías CCN-STIC:
    - Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles
264. ISO/IEC 27000
    - 27002:2013:
        - 15.2 – Gestión de la provisión de servicios del proveedor
265. NIST SP 800-53 rev4:
    - [SA-9] External Information System Services
266. Otras referencias:
    - NIST SP 800-35 – Guide to Information Technology Security Services

[14] *Recovery Point Objective* (Punto de Recuperación Objetivo). Marca la frecuencia de copias de respaldo. Se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable.

4.4.3 [OP.EXT.9] MEDIOS ALTERNATIVOS

267. La provisión de servicios externos será parte de los planes de continuidad de la Organización ([op.cont]).
268. Se ha establecido un protocolo de comunicación con el proveedor para avisar de desastres y escalar el problema.
269. Se ha definido un procedimiento de reacción y recuperación (RTO[15]) ante fallos prolongados de servicio por parte del proveedor.
270. Se ha definido un procedimiento para recuperar la información con la antigüedad (RTPO[16]) determinada por la política de la Organización.
271. Los procesos de actuación en caso de desastre se prueban dentro del plan de pruebas periódicas ([op.cont.3]) de la Organización.

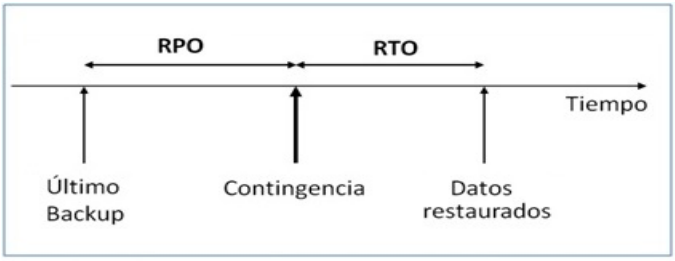

fig.1: Punto de recuperación objetivo (RPO) y tiempo de recuperación objetivo (RTO).

272. Hay una amplia variedad de opciones alternativas a un servicio prestado por un tercero:
    - El propio proveedor proporciona los medios alternativos, al estar incluidos unos niveles mínimos de SLA,s[17] que establecen la obligatoriedad de mantener la continuidad del proveedor para obtener siempre el nivel de disponibilidad establecido en el contrato, de forma que el cliente sólo tiene que conmutar el acceso. Es aconsejable seleccionar adecuadamente aquellos proveedores que realmente son críticos para la continuidad de la operación del servicio.
    - La organización cliente recurre a otro proveedor con el que hay establecido un plan de activación ([op.ext.1] y [op.ext.2]). Parte del plan es cargar (o transferir) datos frescos según política (RPO)

[15] *Recovery Time Objective* (Tiempo de Recuperación Objetivo). Tiempo en el que es necesario restaurar un determinado servicio tras una parada para que ésta no impacte significativamente en el negocio.
[16] *Recovery Time and Point Objective*. Punto de recuperación objetivo y Tiempo de recuperación objetivo.
[17] *Service Level Agreement* (Acuerdo de Nivel de Servicio).

- Si el proveedor alternativo en realidad está funcionando siempre y simplemente se hace cargo de toda la carga de trabajo, hay que establecer un procedimiento para ampliar la contratación y mantener un nivel mínimo de calidad del servicio
- La organización puede recurrir a medios, debiendo preverse los procedimientos citados en los puntos anteriores

273. NIST SP 800-53 rev. 4

4.5 [OP.CONT] CONTINUIDAD DEL SERVICIO

274. Estas actividades permiten instrumentar los principios de seguridad:
    - Artículo 7 – Prevención, reacción y recuperación.
275. Medidas para frenar incidentes desastrosos y permitir que los servicios se sigan prestando en unas condiciones mínimas tras la ocurrencia de un desastre.
276. Se entiende por desastre cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
277. Las medidas de esta sección se entienden como complemento holístico de las medidas requeridas en otros puntos relativas a medios alternativos y copias de seguridad de la información.
278. ISO/IEC 27000
    - 27002:2013:
        - 17 - Aspectos de seguridad de la información para la gestión de la continuidad del negocio
279. NIST SP 800-53 rev4:
    - [CP] Contingency Planning
280. Otras referencias:
    - NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems
    - BSI 25999 - BS 25999 Business continuity
    - BS 25999-1:2006 Business continuity management. Code of practice.
    - BS 25999-2:2007 Business continuity management. Specification.
    - ISO 22301
      Societal security – Business continuity management systems – Requirements
    - ISO/IEC 24762
      Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
    - ISO/IEC 27031
      Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

4.5.1 [OP.CONT.1] ANÁLISIS DE IMPACTO

281. Un análisis de impacto es un estudio pormenorizado de cómo afectaría un desastre a la prestación de servicios, identificando los elementos del sistema de información que son necesarios para la prestación de cada servicio.

282. Un análisis de impacto es una actividad metódica que sigue los siguientes pasos:

    - se identifican los servicios, procesos o actividades críticos,
    - se valora el impacto de la interrupción de dichos servicios, procesos o actividades en función del tiempo que dure la interrupción; sin perjuicio de que en cada caso se elija la escala más adecuada, son escalas típicas de valoración las siguientes
        - días: 1, 2, 3, …, 10 días
        - horas: 1, 2, 4, 8, 24, 48,….., 120 horas
    - se identifican los recursos necesarios para dar continuidad a cada servicio: instalaciones, personas, equipamiento, comunicaciones, software y proveedores
    - se establece un tiempo de recuperación objetivo (RTO), bien para cada servicio, bien para todos los sistemas de información del organismo, bien por familias de servicios (críticos, normales, secundarios, …) Los sistemas que intervengan en la prestación de los servicios heredarán el RTO más restrictivo de los servicios en que intervengan, pudiendo segmentarse por subsistemas.

283. Para la información, hay que analizar cuánta es aceptable que se pierda en caso de desastre. En base a ese cálculo se establece, un punto de recuperación objetivo (RPO), que marcará la frecuencia de copias de respaldo. Por ejemplo, si se hacen copias cada 24 horas, en el peor de los casos perderemos las actualizaciones de las últimas 24 horas, diciéndose que el RPO = 24h. Si no se puede admitir esa pérdida, hay que establecer objetivos más ambiciosos, aumentando la frecuencia de realización de copias. En última instancia se puede llegar a un RPO prácticamente igual a cero empleando técnicas de almacenamiento redundante.

284. El análisis de impacto debe incluir las implicaciones sobre los proveedores de servicios externos.

285. Guías CCN-STIC:

    - Guía CCN-STIC-470H1 - Manual de usuario de PILAR. Análisis y gestión de riesgos v 6.2
    - Guía CCN-STIC-470H2 - Manual de usuario de PILAR. Análisis de impacto y continuidad del negocio v 6.2

286. ISO/IEC 27000

    - 27002:2013:
        - 17.1.1 - Planificar la continuidad de la seguridad de la información

287. NIST SP 800-53 rev4:

- [CP-2] Contingency Plan

4.5.2 [OP.CONT.2] PLAN DE CONTINUIDAD

288. Se debe identificar funciones, responsabilidades y actividades a realizar en caso de desastre que impida prestar el servicio en las condiciones habituales y con los medios habituales, pudiendo diferenciarse para los distintos escenarios de continuidad que se identifiquen.

289. En particular:

- quiénes componen el comité de crisis que toma la decisión de aplicar los planes de continuidad tras analizar el desastre y evaluar las consecuencias
- quiénes se encargarán de la comunicación con las partes afectadas en caso de crisis
- quiénes se encargan de reconstruir el sistema de información (recuperación de desastre)
- las personas designadas a las funciones de los puntos anteriores serán conscientes de su rol en el Plan de Continuidad
- en caso de que las funciones se hayan asignado a roles de la entidad, existe un documento que permite identificar los roles con las personas nominales

290. Debe existir una previsión de los medios alternativos que se van a conjugar para poder seguir prestando los servicios en caso de no poder hacerse con los medios habituales:

- instalaciones alternativas (ver [mp.if.9])
- comunicaciones alternativas (ver [mp.com.9])
- equipamiento alternativo (ver [mp.eq.9])
- personal alternativo (ver [mp.per.9])
- proveedores alternativos
- recuperación de la información con una antigüedad no superior a un tope determinado a la luz del análisis de impacto (ver [mp.info.9] y [mp.cont.1])

291. Todos los medios alternativos deben estar planificados y materializados en acuerdos o contratos con los proveedores correspondientes. El plan debe determinar la coordinación de todos los elementos para alcanzar la restauración de los servicios en los plazos estipulados, así como puntos de contacto, obligaciones y canales de comunicación con los proveedores para la sincronización de la recuperación de un desastre.

292. Las personas afectadas por el plan deben recibir formación específica relativa a su papel en dicho plan.

293. El plan de continuidad debe ser parte integral y armónica con los planes de continuidad de la organización en otras materias ajenas a la seguridad.

294. Deben establecerse procedimientos para sincronizar el plan de continuidad con las actualizaciones del sistema en lo referente a arquitectura, elementos componentes y servicios y calidad de los servicios prestados. En otras palabras, los

procedimientos operativos de seguridad referentes a cambios y actualizaciones deben incluir un punto para actualizar los planes de continuidad.

295. ISO/IEC 27000
    - 27002:2013:
        - 17.1.2 Implementar la continuidad de la seguridad de la información
296. NIST SP 800-53 rev4:
    - [CP] Contingency Planning

4.5.3 [OP.CONT.3] PRUEBAS PERIÓDICAS

297. Se deben realizar pruebas periódicas para localizar (y corregir en su caso) los errores o deficiencias que puedan existir en el plan de acción en caso de desastre.
298. Se diseñarán pruebas que, aunque traten las acciones a realizar en base a pruebas parciales independientes, terminen cubriendo todo el espectro de acciones que tendrían que realizarse en caso de una situación de continuidad. Estas pruebas deberán involucrar a los responsables de su ejecución en caso de producirse y podrán ser de diversa tipología como:
    - Pruebas de validación: Validan el conocimiento del personal involucrado respecto a las decisiones y comunicaciones (llamadas, correos, herramientas, etc.) que se tienen que realizar en caso de situación de continuidad.
    - Simulacros: Validan la activación total o parcial del Plan de Continuidad del Negocio (PCN) mediante pruebas unitarias (pruebas prácticas de acciones concretas que se tendrían que realizar).
    - Prueba de entorno alternativo: Validan el funcionamiento de los sistemas en la situación alternativa de contingencia.
    - Prueba de interrupción completa: Prueba real ejecutada en entorno de producción requiriendo trabajar en situación alternativa.
299. Tras cada ejercicio debe realizarse un informe de análisis de las pruebas realizadas, destacando las incidencias propias o en subcontratistas y derivando un plan de mejoras tanto en los medios como en los procedimientos y en la concienciación y formación de las personas implicadas.
300. Se recomienda que el informe de las pruebas realizadas contenga información relativa a su eficiencia para poder establecer si se cumple con las necesidades de tiempo de ejecución del Plan de Continuidad y para identificar, al compararlo con anteriores pruebas, si se está empeorando en tiempos por algún factor que deba mejorarse.
301. Guías CCN-STIC:
    - Guía CCN-STIC-824 - Informe del Estado de Seguridad
    - Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles
302. ISO/IEC 27000

- 27002:2013:
  - 17.1.3 - Verificar, revisar y evaluar la continuidad de la seguridad de la información

303. NIST SP 800-53 rev4:
   - [CP-4] Contingency Plan Testing

4.6 [OP.MON] MONITORIZACIÓN DEL SISTEMA

4.6.1 [OP.MON.1] DETECCIÓN DE INTRUSIÓN

304. Estas actividades permiten instrumentar los principios de seguridad:
   - Artículo 7 – Prevención, reacción y recuperación.
   - Artículo 8 – Líneas de defensa.

305. La monitorización del sistema permite detectar ataques e incidentes en general habilitando las medidas de reacción y recopilando información para analizar el incidente.

306. Las herramientas de monitorización pueden observar el tráfico en la red o los registros de actividad en los equipos. En este segundo caso, hay que organizar un sistema de recopilación de información desde los puntos en que se genera.

307. Es necesario instalar un sistema de monitorización en la red corporativa. Si existen puntos de interconexión, deben instalarse sistemas de monitorización en dichos puntos, en particular si nos conectamos a redes públicas como Internet y si se permite el acceso remoto con dispositivos donde no se puede garantizar la configuración de seguridad.

308. Se monitorizarán aquellos puntos donde el análisis de riesgos ha identificado un riesgo elevado.

309. El sistema de monitorización buscará todo aquello que suponga un uso no autorizado del sistema o un uso sospechoso; por ejemplo:
   - descargas masivas de información,
   - barrido de puertos,
   - accesos fuera de horario habitual,
   - accesos con derechos de administrador,
   - frecuencias anormales de uso del sistema,
   - envío de información a servidores externos,
   - tráfico cifrado,
   - descargas de servidores externos,
   - etc.

310. Hay que detectar actividades de atacantes internos y externos, así como la existencia de troyanos o APTs[18] que pudieran haberse introducido en el sistema.

311. Guías CCN-STIC:

- Guía CCN-STIC 818 Herramientas de seguridad
- Guía CCN-STIC 432 Seguridad Perimetral - Detección de Intrusos
- Guía CCN-STIC 435 Herramientas de Monitorización de Tráfico
- Guía CCN-STIC-953 - Recomendaciones empleo herramienta Snort

312. ISO/IEC 27000

313. NIST SP 800-53 rev4:

- [SI-4] Information System Monitoring

314. Otras referencias:

- NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)

4.6.2 [OP.MON.2] SISTEMA DE MÉTRICAS

315. Estas actividades permiten instrumentar los principios de seguridad

- Artículo 7 – Prevención, reacción y recuperación.
- Artículo 9 – Reevaluación periódica.

316. Se debe disponer de métricas predictivas que anuncian posibles incidentes antes de que estos se produzcan. Típicamente se recurre a indicadores de cumplimiento y medidas de los recursos dedicados a la seguridad del sistema y a los resultados de las auditorías o autoevaluaciones realizadas.

317. Se debe disponer de métricas de eficiencia que miden si los recursos dedicados a la seguridad son de un volumen adecuado y prudente. Típicamente son medidas de recursos humanos y de dotación económica.

318. Es recomendable formalizar el proceso de generación de indicadores, debiendo estar aprobado un conjunto de indicadores, indicando para cada uno de ellos:

- el objetivo que se pretende medir
- el responsable del indicador
- el origen de la información
- el procedimiento de recogida y tratamiento de datos (mediciones)
- la frecuencia de recogida de datos
- el método de elaboración de indicadores a partir de las medidas
- la elaboración de indicadores agregados a partir de otros indicadores
- los criterios de valoración del indicador a efectos de reaccionar y tomar decisiones

[18] *Advanced Persistent Threats.* Amenazas Persistentes Avanzadas.

319. El proceso de evaluación de los indicadores es aconsejable complementarlo con un proceso de reporte a los diferentes niveles que deben tomar decisiones en la Organización:

    - debe establecerse una lista formal de las personas u órganos que van a recibir los indicadores
    - debe establecerse el conjunto de indicadores (probablemente agregados) que recibirá cada destinatario
    - cada indicador vendrá acompañado de una explicación de su objetivo y los criterios de interpretación, empleando los términos adecuados a la actividad del receptor
    - debe establecerse la frecuencia con que se suministrará cada indicador
    - debe formalizarse el canal de reporte

320. Puede resultar de utilidad el uso de herramientas automatizadas que permitan la obtención y visualización de indicadores de forma transparente, a partir de datos de entrada de otras herramientas o inventarios.

321. Por otro lado, el CCN pone a disposición de las entidades del sector público la herramienta INES (Informe Nacional del Estado de Seguridad) como posible herramienta para la recopilación y comunicación de datos que permitan conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, y confeccionar un perfil general del estado de la ciberseguridad en el sector público.

322. Se debe disponer de métricas de eficacia, que indiquen que el sistema de protección está protegiendo realmente la seguridad de la información y los servicios. Típicamente se analizan datos del proceso de gestión de incidentes de seguridad. En concreto:

    - el número de incidentes de seguridad tratados
    - el tiempo empleado para cerrar el 50% de los incidentes
    - el tiempo empleado para cerrar el 90% de los incidentes

323. Se debe disponer de métricas de eficiencia que miden si los recursos dedicados a la seguridad son de un volumen adecuado y prudente. Típicamente medidas de la fracción de recursos humanos (horas) y de dotación económica (presupuesto) dedicada a la seguridad de los sistemas TIC en relación con el total de recursos dedicados a las Tecnologías de la Información y la Comunicación. (CCN-STIC- 824)

324. Guías CCN-STIC:

    - Guía CCN-STIC-815 - Métricas e indicadores
    - Guía CCN-STIC-824 - Informe nacional del estado de la seguridad
    - Guía CCN-STIC-844 - INES – Informe Nacional del Estado de Seguridad - Manual de Usuario
    - ITS: Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

325. ISO/IEC 27000

326. NIST SP 800-53 rev. 4

    - [PM-6] Information Security Measures of Performance

327. Otras referencias:

    - NIST SP 800-55 - Performance Measurement Guide for Information Security
    - NIST SP 800-80 - Guide for Developing Performance Metrics for Information Security
    - ISO/IEC 27004 - Information technology – Security techniques – Information security management – Measurement

5. [MP] MEDIDAS DE PROTECCIÓN

5.1 [MP.IF] PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

5.1.1 [MP.IF.1] ÁREAS SEPARADAS Y CON CONTROL DE ACCESO

328. Se deben delimitar las áreas de trabajo y de equipos, disponiendo de un inventario actualizado que para cada área determine su función y las personas responsables de su seguridad y de autorizar el acceso.

329. Cuando el acceso se controle por medio de llaves o dispositivos equivalentes, se dispondrá de un inventario de llaves junto con un registro de quién las toma, quién las devuelve y en manos de quién hay copias en cada momento. En caso de sustracción o pérdida, se procederá al cambio con diligencia para evitar el riesgo.

330. Se dispondrá de medios que eviten el acceso por puntos diferentes al que dispone del control de acceso. Se evitarán ventanas accesibles y puertas desprotegidas. En particular hay que vigilar puertas de evacuación de emergencia para que no permitan la entrada ni en condiciones normales ni cuando se utilizan como vía de evacuación (por ejemplo, cámaras de vigilancia, cerraduras electrónicas que registran cada acceso, etc.).

331. ISO/IEC 27000

    - 27002:2013
        - 11.1 - Áreas seguras
        - 11.2.1 - Emplazamiento y protección de equipos

332. NIST SP 800-53 rev. 4

    - [PE-18] Location of Information System Components
    - [PE-3] Physical Access Control
    - [PE-4] Access Control for Transmission Medium
    - [PE-5] Access Control for Output Devices

5.1.2 [MP.IF.2] IDENTIFICACIÓN DE LAS PERSONAS

333. Para las áreas de acceso restringido, se debe mantener una relación de personas autorizadas y un sistema de control de acceso que verifique la identidad y la autorización y deje registro de todos los accesos de personas (por ejemplo, persona o identificador corporativo, fecha y hora de cada entrada y salida).

334. Se recomienda que exista segregación de funciones en el proceso de gestión de acceso a los locales con equipamiento (solicitud y autorización). Dichas funciones deben recaer en al menos dos personas.

335. Debe realizarse periódicamente una revisión de las autorizaciones, identificando si continúa existiendo la necesidad de acceso que motivó la autorización.

336. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 11.1.2 - Controles físicos de entrada

337. NIST SP 800-53 rev.4
    - [PE-2] Physical Access Authorizations
    - [PE-6] Monitoring Physical Access
    - [PE-8] Visitor Access Records

5.1.3 [MP.IF.3] ACONDICIONAMIENTO DE LOS LOCALES

338. Se debe disponer de unas instalaciones adecuadas para el eficaz desempeño del equipamiento que se instala en ellas.

339. Sin perjuicio de lo dispuesto en otras medidas más específicas, los locales deben:
    - garantizar que la temperatura se encuentra en el margen especificado por los fabricantes de los equipos
    - garantizar que la humedad se encuentra dentro del margen especificado por los fabricantes de los equipos
    - se debe proteger el local frente a las amenazas identificadas en el análisis de riesgos, tanto de índole natural, como derivadas del entorno o con origen humano, accidental o deliberado (complementando [mp.if.1], [mp.if4], [mp.if.5], [mp.if.6] y [mp.if.7])
    - se debe evitar que el propio local sea una amenaza en sí mismo, o factor determinante de otras amenazas, como la existencia de material innecesario o inflamable en el local (papel, cajas, etc.) o que pueda ser causa de otros incidentes (elementos con agua, etc.)
    - el cableado debe estar:
        - etiquetado: se puede identificar cada cable físico y su correspondencia a los planos de la instalación
        - controlado: para identificar el cableado fuera de uso

- protegido frente a accidentes: por ejemplo, para evitar que las personas tropiecen con los cables
- protegido frente a accesos no autorizados: protegiendo armarios de distribución y canaletas

340. ISO/IEC 27000
    - 27002:2013
        - 11.2.2 - Instalaciones de suministro
        - 11.2.3 - Seguridad del cableado
341. NIST SP 800-53 rev. 4
    - [PE-14] Temperature and Humidity Controls

5.1.4 [MP.IF.4] ENERGÍA ELÉCTRICA

342. Se deben prever medidas para atajar un posible corte de suministro eléctrico y un correcto funcionamiento de las luces de emergencia.
343. Prevención de problemas de origen interno:
    - dimensionado y protección del cableado de potencia
    - dimensionado y protección de los cuadros y armarios de potencia
344. Reacción a problemas de origen externo:
    - suministro alternativo: UPS[19], generadores, proveedor alternativo
345. Se debe disponer de un plan de emergencia, de reacción y de recuperación de desastres.
346. Hay que disponer de una alimentación suficiente para apagar los equipos de forma ordenada. Normalmente, esto supone una alimentación local (SAI, o UPS por sus siglas en inglés) que garantice el suministro eléctrico durante los minutos necesarios para activar y concluir el procedimiento de apagado de emergencia, y grupos electrógenos en caso de ser necesario.
347. ISO/IEC 27000
    - 27002:2013
        - 11.2.2 - Instalaciones de suministro
348. NIST SP 800-53 rev.4
    - [PE-9] Power Equipment and Cabling
    - [PE-10] Emergency Shutoff
    - [PE-11] Emergency Power
    - [PE-12] Emergency Lighting

[19] *Uninterruptible Power Supply*. Sistema de Alimentación Ininterrumpida (SAI)

5.1.5 [MP.IF.5] PROTECCIÓN FRENTE A INCENDIOS

349. Se debe realizar un estudio del riesgo de incendios, tanto de origen natural como industrial:
    - entorno natural proclive a incendios
    - entorno industrial que pudiera incendiarse
    - instalaciones propias con riesgo de incendio

350. Si el fuego no se puede evitar, hay que desplegar medidas de prevención, monitorización y limitación del impacto
    - disponer de carteles para evacuación
    - evitar el uso de materiales inflamables
    - aislamiento (cortafuegos, puertas ignífugas)
    - sistema de detección conectado a central de alarmas 24x7
    - medios de reacción: medios de extinción
    - plan de emergencia, de reacción y de recuperación de desastres

351. ISO/IEC 27000
    - 27002:2013
        - 11.1.4 - Protección contra las amenazas externas y de origen ambiental

352. NIST SP 800-53 rev.4
    - [PE-13] Fire Protection

353. Otras referencias:
    - Planes de emergencia y evacuación contra incendios de locales y edificios. http://www.mtas.es/insht/FDN/FDN_011.htm

5.1.6 [MP.IF.6] PROTECCIÓN FRENTE A INUNDACIONES

354. Se debe realizar un estudio del riesgo de inundaciones, tanto de origen natural como industrial:
    - cercanía a ríos o corrientes de agua
    - canalizaciones de agua (tuberías) especialmente encima de los equipos

355. Si el riesgo no se puede evitar, hay que desplegar medidas de prevención, monitorización y limitación del impacto
    - aislamiento de humedades
    - canalización de desagüe con procedimientos regulares de limpieza
    - sistema de detección conectado a central de alarmas 24x7
    - plan de reacción y recuperación de desastres; en el caso de canalizaciones industriales, el plan de reacción puede incluir el cierre de llaves o válvulas que atajen el vertido

356. ISO/IEC 27000
    - 27002:2013
        - 11.1.4 - Protección contra las amenazas externas y de origen ambiental
357. NIST SP 800-53 rev.4
    - [PE-15] Water Damage Protection

5.1.7 [MP.IF.7] REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO

358. Se debe llevar un registro pormenorizado de toda entrada y salida de equipamiento, haciendo constar en el mismo:
    - fecha y hora
    - identificación inequívoca del equipamiento (servidores, portátiles, equipos de comunicaciones, soportes de información, etc.)
    - persona que realiza la entrada o salida
    - persona que autoriza la entrada o salida
    - persona que realiza el registro
359. Se recomienda que exista segregación de funciones en el proceso de gestión de entrada y salida de equipamiento en los locales (solicitud y autorización). Dichas funciones deben recaer en al menos dos personas.
360. ISO/IEC 27000
    - 27002:2013
        - 11.2.5 - Retirada de materiales propiedad de la empresa
        - 11.2.6 - Seguridad de los equipos fuera de las instalaciones
361. NIST SP 800-53 rev. 4
    - [PE-16] Delivery and Removal

5.1.8 [MP.IF.9] INSTALACIONES ALTERNATIVAS

362. Se debe disponer de planes para poder prestar los servicios en un lugar alternativo en caso de indisponibilidad de las instalaciones actuales.
363. Las instalaciones alternativas deben garantizar las mismas medidas de protección que las habituales. En particular, en lo que respecta a control de acceso de personas y entrada y salida de equipos.
364. Las instalaciones alternativas pueden estar dispuestas para entrar en servicio inmediatamente (hot site) o requerir un tiempo de personalización (cold site). En todo caso el tiempo de entrada en servicio debe estar respaldado por un análisis de impacto (ver [op.cont.1]), ser parte del plan de continuidad probado (ver [op.cont.2]) y ser objeto de pruebas regulares para validar la viabilidad del plan (ver [op.cont.3]).

365. ISO/IEC 27000
    - 27002:2013
        - 17.2.1 - Disponibilidad de los medios de procesamiento de información
366. NIST SP 800-53 rev. 4
    - [CP-2] Contingency Plan
    - [CP-6] Alternate Storage Site
    - [CP-7] Alternate Processing Site
    - [PE-17] Alternate Work Site

5.2 [MP.PER] GESTIÓN DEL PERSONAL

367. Medidas para proteger al sistema de problemas que pudieran ser causados por las personas que disfrutan de acceso al mismo.

5.2.1 [MP.PER.1] CARACTERIZACIÓN DEL PUESTO DE TRABAJO

368. Se deben definir las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. La definición debe venir respaldada por el análisis de riesgos en la medida en que afecta a cada puesto de trabajo.
369. Se deben definir los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad.
370. Se deben tener en cuenta dichos requisitos en la selección de la persona que va a ocuparlo, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias: dentro del marco de la ley.
371. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 7.1.1 - Investigación de antecedentes
372. NIST SP 800-53 rev. 4
    - [PS-2] Position Risk Designation
    - [PS-3] Personnel Screening
    - [SA-21] Developer Screening

5.2.2 [MP.PER.2] DEBERES Y OBLIGACIONES

373. Se debe informar a cada persona relacionada con el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, incluyendo las medidas disciplinarias a que haya lugar.
374. Se debe cubrir tanto el periodo durante el cual se desempeña el puesto como las obligaciones en caso de terminación de la asignación, incluyendo el caso de traslado a otro puesto de trabajo.

375. Es de especial relevancia el deber de confidencialidad respecto de los datos a los que tengan acceso, tanto durante el periodo durante el que estén adscritos al puesto de trabajo, como su prolongación posterior a la terminación de la función para la que tuvo acceso a la información confidencial.

376. En el caso de personal contratado a través de una tercera parte:

- se deben determinar deberes y obligaciones de la persona
- se deben determinar deberes y obligaciones de la parte contratante
- se debe determinar el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones, involucrando a la parte contratante

377. ISO/IEC 27000

- 27002:2013
  - 7.1.2 - Términos y condiciones de contratación
  - 7.2.1 - Responsabilidades de la Dirección
  - 7.2.3 - Proceso disciplinario
  - 7.3.1 - Terminación o cambio de responsabilidades laborales
  - 8.1.4 - Devolución de activos
  - 13.2.4 - Acuerdos de confidencialidad o no divulgación

378. NIST 800-53 rev. 4

- [PL-4] Rules of Behavior
- [PS-6] Access Agreements
- [PS-7] Third-Party Personnel Security
- [PS-4] Personnel Termination
- [PS-5] Personnel Transfer
- [PS-8] Personnel Sanctions

5.2.3 [MP.PER.3] CONCIENCIACIÓN

379. Se debe concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

380. En particular hay que refrescar regularmente:

- la normativa de seguridad relativa al buen uso de los sistemas
- la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado
- el procedimiento de reporte de incidentes de seguridad, seas reales o falsas alarmas

381. Todo el personal debe recibir inicial y regularmente información acerca de los puntos arriba descritos.

382. ISO/IEC 27000

- 27001:2013

- 7.3 - Concienciación

- 27002:2013
  - 7.2.2 - Concienciación, formación y capacitación en seguridad de la información

383. NIST SP 800-53 rev. 4
   - [AT-2] Security Awareness Training
   - [AT-3] Role-Based Security Training
   - [CP-3] Contingency Training
   - [IR-2] Incident Response Training
   - [PM-13] Information Security Resources
384. Otras referencias:
   - NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program

5.2.4 [MP.PER.4] FORMACIÓN

385. Se debe formar regularmente a las personas en aquellas técnicas que requieran para el desempeño de sus funciones.
386. Es de destacar, sin perjuicio de otros aspectos:
   - configuración de sistemas
   - gestión de incidentes (detección y reacción)
   - procedimientos relativos a sus funciones sobre la gestión de la información (almacenamiento, transferencia, copias, distribución y destrucción)
387. La formación debe actualizarse cada vez que cambian los componentes del sistema de información, introduciéndose nuevos equipos, nuevo software, nuevas instalaciones, etc.
388. ISO/IEC 27000
   - 27001:2013
     - 7.2 - Competencias
   - 27002:2013
     - 7.2.2 - Concienciación, formación y capacitación en seguridad de la información
389. NIST SP 800-53 rev. 4
   - [AT-2] Security Awareness Training
   - [AT-3] Role-Based Security Training
   - [AT-4] Security Training Records
   - [CP-3] Contingency Training
   - [IR-2] Incident Response Training

- [PM-13] Information Security Resources

390. Otras referencias:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.17 - Security Skills Assessment and Appropriate Training to Fill Gaps
    - NIST SP 800-16 - Information Technology Security Training Requirements: A Role- and Performance-Based Model
    - NIST SP 800-50 - Building an Information Technology Security Awareness and Training Program

5.2.5 [MP.PER.9] PERSONAL ALTERNATIVO

391. Se debe prever la existencia de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual. El personal alternativo deberá ofrecer las mismas garantías de seguridad que el personal habitual.
392. Este personal alternativo puede ser, por ejemplo:
    - Personal del mismo equipo sobredimensionado con capacidad de asumir el trabajo
    - Personal de otros turnos 24x7 que puedan cubrir bajas eventuales
    - Personal de otros departamentos con los conocimientos necesarios (respetando la segregación)
    - Personal de un tercero contratado previsto en el Plan de Continuidad
393. El plan de utilización de personal alternativo se vertebra dentro del plan de continuidad de la organización, incluyéndose en las pruebas periódicas.
394. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 17.2.1 - Disponibilidad de los recursos de tratamiento de la información
395. NIST SP 800-53 rev. 4
    - [CP-2] Contingency Plan
    - [CP-6] Alternate Storage Site
    - [CP-7] Alternate Processing Site

5.3 [MP.EQ] PROTECCIÓN DE LOS EQUIPOS

5.3.1 [MP.EQ.1] PUESTO DE TRABAJO DESPEJADO

396. Se debe exigir que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento. Según se termine una tarea, el material se retirará a

otra zona: cajones, estanterías personales o comunes, cuarto de almacenamiento, etc.

397. El material de trabajo se guardará en lugar cerrado. Pueden ser cajones o armarios con llave, o un cuarto separado cerrado con llave al menos fuera del horario de trabajo.

398. ISO/IEC 27000

    - ISO/IEC 27002:2013:
        - 11.2.9 - Política de puesto de trabajo despejado y pantalla limpia

399. NIST SP 800-53 rev. 4

5.3.2 [MP.EQ.2] BLOQUEO DE PUESTO DE TRABAJO

400. Se debe bloquear automáticamente el puesto de trabajo desde el que se accede a servicios o datos de nivel medio o superior al cabo de un tiempo de inactividad, que se marcará por parte de la entidad o compañía.

401. Se debe requerir al usuario autenticarse de nuevo para reanudar la actividad en curso.

402. El tiempo mencionado será parte de la configuración del equipo y no podrá ser alterado por el usuario.

403. Se cancelarán las sesiones abiertas tanto desde dicho puesto de trabajo como las remotas al cabo de un tiempo de inactividad (superior al bloqueo del puesto de trabajo).

404. El tiempo mencionado será parte de la configuración del equipo y no podrá ser alterado por el usuario.

405. ISO/IEC 27000

    - 27002:2013:
        - 11.2.8 - Equipo de usuario desatendido

406. NIST SP 800-53 rev. 4

    - [AC-11] Session Lock
    - [AC-12] Session Termination

5.3.3 [MP.EQ.3] PROTECCIÓN DE EQUIPOS PORTÁTILES

407. Debe existir un inventario de los equipos portátiles, que identifique el equipo portátil junto a la persona responsable del mismo. Se debe verificar regularmente en el inventario que el equipo permanece bajo control del usuario al que está asignado.

408. Se recomienda que los equipos portátiles tengan instalado y activado un sistema de protección perimetral (cortafuegos personal) configurado para bloquear

accesos salvo los autorizados. Los accesos autorizados seguirán los procedimientos de autorización del organismo (ver [org.4]).

409. Los accesos realizados remotamente deberán ser distinguidos por el servidor para que pueda limitar y autorizar la información y los servicios accesibles cuando se conecten remotamente a través de redes que no pueda controlar la organización.

410. El mecanismo de control del equipo formará parte de la configuración del equipo y no podrá ser modificado por el usuario.

411. Los usuarios recibirán instrucciones sobre el uso admisible del equipo, sobre los aspectos que debe contemplar en su manejo diario y del canal de comunicación para informar al servicio de gestión de incidentes en caso de avería, pérdida, robo o terminación.

412. Se deberá comunicar al personal que los equipos portátiles no deben contener claves de acceso remoto a la organización y se identificará y aprobará formalmente aquellos casos en los que no puede aplicarse.

413. Los equipos portátiles deberán disponer de detectores de violación que permitan saber si el equipo ha sido manipulado y, en caso afirmativo, activar los procedimientos de gestión del incidente. Los detectores de violación podrán ser:

    - Físicos: por ejemplo, pegatinas que se alteran al manipularlas, bridas de protección, etc.
    - Lógicos: por ejemplo, herramientas automatizadas que detecten si algún componente del portátil ha sido extraído o sustituido

414. Se recomienda proteger el acceso a la información que contienen los equipos portátiles que sean susceptibles de salir de las instalaciones de la organización (por ejemplo, con candados, discos duros cifrados, etc.).

415. Se debe proteger la información contenida de nivel alto por medios criptográficos: [mp.si.2].

416. Las claves criptográficas deben protegerse según [op.exp.11].

417. Cuando el equipo es desmantelado, se debe aplicar lo previsto en [mp.si.5].

418. Guías CCN-STIC:

    - Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles

419. ISO/IEC 27000

    - ISO/IEC 27002:2013:
        - 6.2.1 - Política de dispositivos móviles
        - 11.2.6 - Seguridad de los equipos fuera de las instalaciones

420. NIST SP 800-53 rev4:

    - [AC-19] Access Control for Mobile Devices

5.3.4 [MP.EQ.9] MEDIOS ALTERNATIVOS

421. Se debe prever medios alternativos de tratamiento de la información para el caso de que fallen los equipos de personal habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección.
422. Se debe establecer un tiempo máximo para que los equipos alternativos entren en funcionamiento.
423. Los equipos alternativos pueden estar dispuestos para entrar en servicio inmediatamente (es decir, configurados) o requerir un tiempo de personalización (se puede disponer de ellos en el tiempo prestablecido; pero hay que configurarlos y cargar los datos). En todo caso el tiempo de entrada en servicio debe estar respaldado por un análisis de impacto (ver [op.cont.1]).
424. ISP/IEC 27000
    - 27002:2013
        - 17.2.1 - Disponibilidad de instalaciones de tratamiento de la información
425. NIST SP 800-53 rev. 4

5.4 [MP.COM] PROTECCIÓN DE LAS COMUNICACIONES

5.4.1 [MP.COM.1] PERÍMETRO SEGURO

426. Se debe delimitar el perímetro lógico del sistema; es decir, los puntos de interconexión con el exterior. Este perímetro deberá estar reflejado en la documentación de la arquitectura del sistema (por ejemplo, el esquema de red).
427. Se debe disponer de cortafuegos que separen la red interna del exterior. Todo el tráfico deberá atravesar dichos cortafuegos que sólo dejaran transitar los flujos previamente autorizados.
428. Cuando se requiera niveles de seguridad ALTA, el sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada. Estos cortafuegos podrán ser equipos físicos o instalaciones o aplicaciones cortafuegos virtuales.
429. Cuando la disponibilidad de las transmisiones a través del cortafuegos sea de nivel ALTO, se dispondrán sistemas redundantes.
430. Los ataques de denegación de servicio pueden ser afrontados en el perímetro, aunque pueden requerir la intervención de otros elementos. En el perímetro se pueden detectar patrones sospechosos de comportamiento: avalanchas de peticiones, peticiones trucadas y, en general, un uso malicioso de los protocolos de comunicaciones. Algunas de estas peticiones pueden ser denegadas directamente por el equipo perimetral, en otras ocasiones hay que levantar una

alarma para actuar en donde corresponda (servidores web, servidores de bases de datos... o contactando con los centros de respuesta a incidentes).

431. Guías CCN-STIC:

- Guía CCN-STIC-408 - Seguridad Perimetral - Cortafuegos
- Guía CCN-STIC-419 - Configuración segura con IPtables
- Serie CCN-STIC-500 - Guías para Entornos Windows
- Serie CCN-STIC-600 - Guías para otros Entornos
- Guía CCN-STIC-811 - Interconexión

432. ISO/IEC 27000

- 27002:2013:
  - 13.1.2 - Seguridad de los servicios de red

433. NIST SP 800-53 rev. 4

- [AC-4] Information Flow Enforcement
- [CA-3] System Interconnections
- [SC-7] Boundary Protection

434. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.8 - Malware Defenses
  - CSC.9 – Limitation and Control of Network Ports
  - CSC.11 – Secure Configurations for Network Devices
  - CSC.12 – Boundary Defense
  - CSC.13 – Data Protection
  - CSC.15 - Wireless Access Control

- NIST SP 800-41 - Guidelines on Firewalls and Firewall Policy

5.4.2 [MP.COM.2] PROTECCIÓN DE LA CONFIDENCIALIDAD

435. 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. Es por ello que esta medida suele implementarse a la par que [mp.com.3].

436. Se deben emplear algoritmos acreditados por el Centro Criptológico Nacional que garanticen el secreto de los datos transmitidos.

437. En conexiones establecidas fuera del dominio de seguridad de la organización, se recurrirá a redes privadas virtuales que, con métodos criptográficos y tras una autenticación fiable (ver [mp.com.3]), establecen una clave de cifrado para la sesión.

438. El cifrado de las comunicaciones es especialmente adecuado en redes inalámbricas (WiFi)[20]. Los equipos inalámbricos llevan incorporados mecanismos de cifrado de las comunicaciones, que deberán ser configurados de forma segura (ver [op.exp.2] y [op.exp.3]) empleando mecanismos actualizados.

439. Hay que atender al secreto de las claves de cifrado según lo indicado en [op.exp.11]. En el caso de redes privadas virtuales, el secreto debe ser impredecible, mantenerse bajo custodia mientras dure la sesión, y ser destruido al terminar. En el caso de otros procedimientos de cifrado, hay que cuidar de las claves de cifrado durante su ciclo de vida: generación, distribución, empleo, retirada del servicio y retención si la hubiera.

440. Hay que seleccionar algoritmos evaluados o acreditados. A menudo basta con seleccionar los algoritmos y los parámetros adecuados dentro de las opciones posibles.

441. Hay que procurar que las tareas de cifrado en los extremos se realicen en equipos hardware especializados y certificados, conforme a [op.pl.5], evitando el cifrado por software.

442. Guías CCN-STIC:

- Guía CCN-STIC-807 Criptografía de empleo en el ENS
- Guía CCN-STIC-827 - Gestión y uso de dispositivos móviles
- Guía CCN-STIC-406 - Seguridad en Redes Inalámbricas
- Guía CCN-STIC-416 - Seguridad en redes privadas virtuales

443. ISO/IEC 27000

- ISO/IEC 27002:2013:
  - 10.1.1 - Política de uso de los controles criptográficos
  - 13.1.1 - Controles de red
  - 13.1.2 - Seguridad de los servicios de red
  - 14.1.2 - Asegurar los servicios de aplicaciones en redes públicas
  - 18.1.5 - Regulación de los controles criptográficos

444. NIST 800-53 rev. 4

- [AC-4] Information Flow Enforcement
- [AC-18] Wireless Access
- [SC-8] Transmission Confidentiality and Integrity
- [SC-12] Cryptographic Key Establishment and Management
- [SC-13] Cryptographic Protection
- [SC-40] Wireless Link Protection

445. Otras referencias:

[20] *Wireless Fidelity*

- SANS - CIS Critical Security Controls - Version 6.1
    - CSC.15 - Wireless Access Control
- NIST SP 800-48 - Wireless Network Security for IEEE 802.11a/b/g and Bluetooth
- NIST SP 800-52 - Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
- NIST SP 800-77 - Guide to IPsec VPNs
- NIST SP 800-113 - Guide to SSL VPNs
- NIST SP 800-121 - Guide to Bluetooth Security
- NIST SP 800-127 - Guide to Securing WiMAX Wireless Communications
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)

- SSL – Secure Sockets Layer
    - [RFC 6101] The Secure Sockets Layer (SSL) Protocol Version 3.0
    - Guía CCN-STIC-826 Configuración de SSL/TLS

- TLS – Transport Layer Security
    - [RFC 5246] The Transport Layer Security (TLS) Protocol – Version 1.2
    - [RFC 6176] Prohibiting Secure Sockets Layer (SSL) Version 2.0
    - Guía CCN-STIC-826 Configuración de SSL/TLS

- SSH – Secure Shell
- SCP – Secure copy
- SFTP – SSH File Transfer Protocol

5.4.3 [MP.COM.3] PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

446. 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. Es por ello que esta medida suele implementarse a la par que [mp.com.2].

447. Se debe establecer de forma fehaciente la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna.

448. Se debe evitar la utilización de mecanismos de autenticación y protocolos no contemplados en la normativa de la organización.

449. Se deben usar protocolos que garanticen o al menos comprueben y detecten violaciones en la integridad de los datos intercambiados y en la secuencia de los paquetes.

450. La forma más habitual de establecer esta medida es establecer una red privada virtual que:
    - garantice la autenticación de las partes al inicio de sesión, cuando la red se establece
    - controle que la sesión no puede ser secuestrada por una tercera parte
    - que no permita realizar ataques activos (alteración de la información en tránsito o inyección de información espuria) sin que sea, al menos, detectada

451. Hay que seleccionar algoritmos evaluados o acreditados por el Centro Criptológico Nacional que garanticen el secreto de los datos transmitidos. A menudo basta con seleccionar los algoritmos y los parámetros adecuados dentro de las opciones posibles.

452. Se debe evitar la utilización de mecanismos de autenticación y protocolos no contemplados en la normativa de aplicación. Además, en caso de utilizar claves concertadas, deberán utilizarse con cautela aplicando exigencias medias de calidad.

453. En conexiones establecidas fuera del dominio de seguridad de la organización, se puede recurrir a redes privadas virtuales que, con métodos criptográficos y tras una autenticación fiable, establecen una clave de cifrado para la sesión.

454. El cifrado de las comunicaciones es especialmente adecuado en redes inalámbricas (WiFi). Los equipos inalámbricos llevan incorporados mecanismos de cifrado de las comunicaciones, que deberán ser configurados de forma segura (ver [op.exp.2] y [op.exp.3]) empleando mecanismos actualizados.

455. Hay que atender al secreto de las claves de cifrado según lo indicado en [op.exp.11]. En el caso de redes privadas virtuales, el secreto debe ser impredecible, mantenerse bajo custodia mientras dure la sesión, y ser destruido al terminar. En el caso de otros procedimientos de cifrado, hay que cuidar de las claves de cifrado durante su ciclo de vida: generación, distribución, empleo, retirada del servicio y retención si la hubiera.

456. Hay que procurar que las tareas de cifrado en los extremos se realicen en equipos hardware especializados y certificados, conforme a [op.pl.5], evitando el cifrado por software.

457. Se debe evitar la utilización de mecanismos de autenticación y protocolos no contemplados en la normativa de aplicación. Además, en caso de utilizar claves concertadas, deberán utilizarse con cautela aplicando exigencias altas de calidad.

458. Guías CCN-STIC:
    - Guía CCN-STIC-416 - Seguridad en redes privadas virtuales
    - Guía CCN-STIC-807 – Criptografía de empleo en el ENS

459. ISO/IEC 27000
    - ISO/IEC 27002:2013:

- 10.1.1 - Política de uso de los controles criptográficos
- 13.1.1 - Controles de red
- 13.1.2 - Seguridad de los servicios de red
- 14.1.2 - Asegurar los servicios de aplicaciones en redes públicas

460. NIST SP 800-53 rev. 4

- [AC-18] Wireless Access
- [SC-8] Transmission Confidentiality and Integrity
- [SC-13] Cryptographic Protection
- [SC-23] Session Authenticity
- [SC-40] Wireless Link Protection

461. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.15 - Wireless Access Control

5.4.4 [MP.COM.4] SEGREGACIÓN DE REDES

462. La segregación de redes acota el acceso a la información y acota la propagación de los incidentes de seguridad que quedan restringidos al entorno donde ocurren. Esta deberá quedar reflejada en documentación de la arquitectura del sistema (por ejemplo, el esquema de red) [op.pl.2].

463. Se debe segmentar la red de forma que haya:

- control (de entrada) de los usuarios que pueden trabajar en cada segmento, en particular si el acceso se realiza desde el exterior del segmento, tanto si es desde otro segmento de la red corporativa como si el acceso procede del exterior de la red, extremando las precauciones en este último escenario.
- control (de salida) de la información disponible en cada segmento
- control (de entrada) de las aplicaciones utilizables en cada segmento

464. El punto de interconexión debe estar particularmente asegurado, mantenido y monitorizado (ver [mp.com.1]). Estos puntos de interconexión interna son una defensa crítica frente a intrusos que han logrado superar las barreas exteriores y se alojan en el interior. Nótese que a menudo el objetivo de estas intrusiones es extraer información y enviarla al exterior, lo que se traduce en que hay que vigilar los protocolos de comunicaciones que se establecen y los datos que se transmiten.

465. No debería permitirse ningún protocolo directo entre los segmentos internos y el exterior, intermediando todos los intercambios de información.

466. Las redes se pueden segmentar por dispositivos físicos o lógicos.

467. Esta medida puede establecerse dinámicamente como reacción frente a intrusiones (supuestas o detectadas) y que van a requerir un cierto periodo de tiempo (días) en poder ser erradicadas. Los primeros servicios a aislar serían los servidores de datos y los servidores de autenticación para monitorizar y controlar

su uso. Otros candidatos a ser aislados son los servicios de administración del propio sistema para evitar que se capturen credenciales con privilegios de administración o se pueda suplantar la identidad de los administradores.

468. Guías CCN-STIC:
    - Guía CCN-STIC-408 - Seguridad perimetral (cortafuegos)
    - Guía CCN-STIC-419 - Configuración segura con IPtables
    - Serie CCN-STIC-600 Guías para otros Entornos
    - Guía CCN-STIC-641 - Seguridad en routers Cisco
469. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 13.1.3 - Segregación en redes
470. NIST SP 800-53 rev. 4
    - [SC-32] Information System Partitioning

5.4.5 [MP.COM.9] MEDIOS ALTERNATIVOS

471. Se debe prever medios alternativos de comunicación para el caso de que fallen los medios habituales. Estos medios alternativos deben proporcionar las mismas garantías de seguridad que los medios habituales y deberá establecerse un tiempo máximo de entrada en funcionamiento que esté aprobado por su responsable.
472. En todo caso, el tiempo de entrada en servicio debe estar respaldado por un análisis de impacto (ver [op.cont.1]), ser parte del plan de continuidad probado (ver [op.cont.2]) y ser objeto de pruebas regulares para validar la viabilidad del plan (ver [op.cont.3]).
473. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 17.2.1 - Disponibilidad de los recursos de tratamiento de la información
474. NIST SP 800-53 rev. 4
    - [CP-8] Telecommunications Services
    - [CP-11] Alternate Communications Protocol

5.5 [MP.SI] PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

475. Los soportes de información incluyen:
    - discos de los servidores y equipos de usuario final, con especial consideración a equipos portátiles y discos removibles

- PDAs[21]
- disquetes, cintas, CD, DVD, ...
- discos USB[22]
- tarjetas de memoria y tarjetas inteligentes
- componentes de impresoras
- material impreso
- otros medios de almacenamiento de información con capacidad de que la información pueda ser recuperada de formar automática o manual

476. Referencias:
    - Guía CCN-STIC-404 Control de Soportes Informáticos

5.5.1 [MP.SI.1] ETIQUETADO

477. Se debe etiquetar de forma que, sin revelar su contenido, se indique el nivel de calificación más alto de la información contenida.
478. Una opción es que el propio soporte, en su exterior, lleve escrito el nivel de información que contiene o puede contener.
479. Una alternativa es que el soporte sea identificable por medio de algún código o referencia y que el usuario pueda acceder a un repositorio de información donde se indica el nivel de información que el soporte contiene o puede contener.
480. La etiqueta del soporte determina las normativas y los procedimientos que deben aplicarse al mismo, concretamente en lo referente a:
    - control de acceso
    - cifrado del contenido
    - entrada y salida de las instalaciones
    - medios de transporte
481. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 8.2.2 - Etiquetado de la información
        - 8.3.1 - Gestión de soportes extraíbles
482. NIST SP 800-53 rev. 4
    - [MP-3] Media Marking

[21] *Personal Digital Assistant,* asistente digital personal o agenda electrónica de bolsillo.
[22] *Universal Serial Bus*

5.5.2 [MP.SI.2] CRIPTOGRAFÍA

483. Este requisito se aplica, en particular, a todos los dispositivos removibles (como CD, DVD, discos USB, etc.).

484. En lo referente a claves criptográficas, se debe aplicar [op.exp.11].

485. Una opción es asegurarse que los datos se protegen antes de copiarse al soporte; es decir, se cifran o se firman exteriormente.

486. Otra opción es proteger todo el soporte instalando en el mismo un disco virtual que se encarga de acoger todo lo que se copie en el mismo, así como controlar el acceso al mismo.

487. Otra opción es emplear soportes con cifrado incorporado por hardware que se encarga de acoger todo lo que se copie en el soporte, así como controlar el acceso al mismo.

488. Guías CCN-STIC:

- Guía CCN-STIC-807 - Criptografía
- Guía CCN-STIC-437 - Herramientas de Cifrado Software
- Guía CCN-STIC-955 - Recomendaciones empleo GnuPG

489. ISO/IEC 27000

- 27002:2013:
  - 8.3.1 - Gestión de soportes extraíbles
  - 10.1.1 - Política de uso de los controles criptográficos

490. NIST SP 800-53 rev4:

- [SC-28] Protection of Information at Rest

491. Otras referencias:

- NIST SP 800-111 - Guide to Storage Encryption Technologies for End User Devices

492. Productos. Hay muchos donde elegir; sólo se citan algunos de uso frecuente:

- BitLocker – Microsoft
- Crypt2000 – Secuware
- GPG – http://www.gnupg.org/
- PGP – Symantec
- Veracrypt

5.5.3 [MP.SI.3] CUSTODIA

493. Se debe aplicar la debida diligencia y control a los soportes de información (tanto en soporte electrónico como no electrónico) que permanecen bajo la responsabilidad de la organización:
    - garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7) o lógicas ([mp.si.2]) o ambas
    - garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial en lo referente a temperatura, humedad y otros agresores medioambientales
494. Se recomienda conservar la historia de cada dispositivo, desde su primer uso hasta la terminación de su vida útil y verificar regularmente que los soportes cumplen las reglas acordes a su etiquetado.
495. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 8.3.1 - Gestión de soportes extraíbles
496. NIST SP 800-53 rev. 4
    - [MP-4] Media Storage
497. Otras referencias:
    - NIST SP 800-111 – Guide to Storage Encryption Technologies for End User Devices

5.5.4 [MP.SI.4] TRANSPORTE

498. Se debe garantizar que los dispositivos permanecen bajo control y se satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.
499. Se debe:
    - disponer de un registro de salida que identifica al menos la etiqueta y al transportista que recibe el soporte para su traslado (tanto electrónico como no electrónico)
    - disponer de un registro de entrada que identifica al menos la etiqueta y al transportista que lo entrega
    - disponer de un procedimiento rutinario que coteja las salidas con las llegadas y levanta las alarmas pertinentes cuando se detecta algún incidente
    - utilizar los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de clasificación de la información contenida de mayor nivel
    - gestionar las claves según [op.exp.11]
500. Se recomienda disponer de un procedimiento al respecto y se verifica regularmente que los procedimientos establecidos se siguen, aplicando medidas correctivas en su defecto.

501. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 8.3.3 - Soportes físicos en tránsito
        - 11.2.5 - Retirada de materiales propiedad de la empresa
502. NIST SP 800-53 rev4:
    - [MP-5] Media Transport

5.5.5 [MP.SI.5] BORRADO Y DESTRUCCIÓN

503. Se debe aplicar un mecanismo de borrado seguro a los soportes extraíbles (electrónicos y no electrónicos) que vayan a ser reutilizados para otra información o liberados a otra organización. El mecanismo de borrado será proporcionado a la clasificación de la información que ha estado presente en el soporte.
504. Se deben destruir los soportes, de forma segura:
    - cuando la naturaleza del soporte no permita un borrado seguro
    - cuando el procedimiento asociado al nivel de clasificación de la información contenida así lo requiera
505. El mecanismo de destrucción será proporcionado a la clasificación de la información contenida.
506. Los mecanismos de borrado y destrucción deben tener en la normativa de protección medioambiental y los certificados de calidad medioambiental de la organización.
507. Se deben elegir productos certificados conforme a lo establecido en [op.pl.5]
508. Recomendaciones (tomadas de NIST SP 800-88):

medio	procedimiento	
papel microfilm	destruir	• trituradora en tiras o cuadraditos: 2mm
móviles PDAs	borrar manualmente	• agenda • mensajes • llamadas • resetear a la configuración de fábrica
routers	borrar manualmente	• tablas de encaminamiento • registros de actividad • cuentas de administración • resetear a la configuración de fábrica
impresoras fax	borrar manualmente	• resetear a la configuración

		de fábrica
discos reescribibles	reescribir	• reescribir 3 veces: con ceros, con unos, con datos aleatorios
discos de solo lectura	destruir	• trituradora: 5mm
discos virtuales cifrados	además de lo anterior	• destruir las claves

Tabla 4: Recomendaciones NIST SP 800-88 para borrado y destrucción

509. Guías CCN-STIC:
    - Guía CCN-STIC-305 – Destrucción y *sanitización* de soportes informáticos (uso oficial)
    - Guía CCN-STIC-400 - Manual de seguridad de las TIC
    - Guía CCN-STIC-403 - Herramientas de seguridad
    - Guía CCN-STIC-404 - Control de soportes informáticos
    - Guía CCN-STIC-818 - Herramientas de seguridad
510. ISO/IEC 27000
    - 27002:2013:
        - 8.3.2 - Eliminación de soportes
        - 11.2.7 - Reutilización o eliminación segura de equipos
511. NIST SP 800-53 rev4:
    - [MP-6] Media Sanitization
    - [MP-8] Media Downgrading
512. Otras referencias:
    - NIST SP 800-88 - Guidelines for Media Sanitization
    - DoD 5220 Block Erase

5.6 [MP.SW] PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS

5.6.1 [MP.SW.1] DESARROLLO

513. El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción. Ver [op.acc.3] sobre segregación de funciones. Para que la segregación sea creíble, se deben separar los entornos y controlar los mecanismos de identificación, autenticación y control de acceso de los usuarios diferenciando rigurosamente los privilegios de cada uno.
514. La metodología de desarrollo conviene que sea un estándar reconocido que incluya la seguridad como parte integral del desarrollo (por ejemplo, METRICA, Security Development Lifecycle, Correctness by Construction, Building Security In

Maturity Model, OWASP, etc.). Es decir, desde la concepción arquitectónica hay que plantear los requisitos de seguridad del sistema final e ir optando por soluciones que introduzcan los controles necesarios en el software desarrollado.

515. Hay que evitar que se desarrolle pensando únicamente en la funcionalidad y que los requisitos de seguridad se añadan posteriormente parcheando.

516. Desarrollo integral significa que las funciones de seguridad son parte de la interfaz de usuario, que los registros de actividad e incidencias son parte de la arquitectura de registro y que existen mecanismos de validación, protección de la información y verificación de que se respeta la política de seguridad deseada.

517. Durante las pruebas de desarrollo y de aceptación no se usarán datos de prueba reales, sino datos específicos para pruebas. Cuando los datos de prueba procedan de datos reales, se manipularán para que no se puedan reconocer datos reales en las pruebas. En último caso, si fuera inevitable usar datos reales, se protegerán como si estuvieran en producción. Por último, los datos de prueba deben retirarse cuando el sistema pasa a producción.

518. La inspección del código fuente debe ser posible tanto durante el desarrollo como durante la vida útil del software. Inspeccionar todo el código es costoso y probablemente injustificado en los sistemas de soporte al ENS; pero es necesario acceder al código fuente para analizar incidentes y para planificar pruebas de penetración. Por ello debe estar disponible con las debidas garantías de control de acceso.

519. En todo caso hay que revisar fallos típicos de programación que puedan derivar en problemas de seguridad:

    - desbordamiento de buffers,
    - información residual en almacenamiento temporal (RAM, ficheros en disco, datos en la red, datos en la nube, …),
    - almacenamiento de claves y material criptográfico,
    - validación de los datos de entrada, de usuarios y entre procesos,
    - validación de la configuración,
    - posibilidades de inyección de código,
    - posibles race conditions (carreras de concurrencia),
    - escalado de privilegios,
    - comunicaciones sin autenticar y/o sin cifrar,
    - etc.

520. Se incluyen normas de programación segura. Se recomienda adoptar soluciones automatizadas de análisis de código estático que permitan verificar ante cada nueva versión que no es publicada con errores de programación conocidos.

521. Guías CCN-STIC:

    - Guía CCN-STIC-205 - Actividades Seguridad Ciclo Vida CIS

522. ISO/IEC 27000

- ISO/IEC 27002:2013:
  - 9.4.5 - Control de acceso al código fuente de los programas
  - 12.1.4 - Separación de los recursos de desarrollo, prueba y operación
  - 14.2.1 - Política de desarrollo seguro
  - 14.2.5 - Principios de ingeniería de sistemas seguros
  - 14.2.6 - Entorno de desarrollo seguro
  - 14.2.7 - Externalización del desarrollo de software
  - 14.3.1 - Protección de los datos de prueba

523. NIST SP 800-53 rev. 4

- [CM-4] (1) Security Impact Analysis - Separate Test Environments
- [SA-3] System Development Life Cycle
- [SA-4] Acquisition Process
- [SA-8] Security Engineering Principles
- [SA-10] Developer Configuration Management
- [SA-11] Developer Security Testing and Evaluation
- [SA-12] Supply Chain Protections
- [SA-15] Development Process, Standards, and Tools
- [SA-17] Developer Security Architecture and Design

524. Otras referencias:

- SANS
  http://www.sans.org/curricula/secure-software-development
- Métrica v3 - Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información, Ministerio de Administraciones Públicas, Consejo Superior de Administración Electrónica
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle

5.6.2 [MP.SW.2] ACEPTACIÓN Y PUESTA EN SERVICIO

Categoría BÁSICA

525. Se realizan pruebas estándar de aceptación para que un nuevo software se integre en un proceso, ya sea un software desarrollado en la propia entidad o adquirido. Esto incluye verificar que se satisfacen los requisitos de seguridad, que hay mecanismos que detectan y registran los fallos reales o sospechas de violación de la seguridad y que están preparados los procedimientos de gestión de incidentes.

526. Las pruebas deben hacerse en un entorno separado para no causar problemas a la producción, ni alterando datos, ni abriendo brechas de seguridad por defectos de convivencia. Es conveniente utilizar un entorno de pre-producción (aunque podrá utilizarse excepcionalmente para las pruebas, un equipo del entorno de producción que esté debidamente aislado) y asegure el nivel de seguridad adecuado a los datos utilizados.

527. Las pruebas de aceptación se realizarán con datos ficticios o disociados, evitando el uso de datos reales siempre que sea posible, salvo que se asegure el nivel de seguridad adecuado a los datos utilizados.

Categoría MEDIA

528. El análisis de vulnerabilidades constará de 3 fases:

- Revisión exhaustiva de los componentes del software, centrándose en su superficie de interacción con los usuarios con servicios de soporte y con otros programas.
- Debería verificarse que el sistema no incluye versiones de librerías con vulnerabilidades conocidas.
- Análisis de posibles vulnerabilidades en los elementos identificados en el primer paso y estimación del impacto potencial que supondría un incidente.
- Pruebas de penetración para cerciorarse de si la vulnerabilidad es utilizable, priorizando aquellos puntos de mayor impacto potencial.

529. Deben hacerse pruebas simulando usuarios externos y usuarios internos, en función de a quienes sea accesible el software.

Categoría ALTA

530. El análisis de coherencia se hace a nivel de procesos, concretamente de los que componen el proceso administrativo que le compete a la organización. Para cada proceso propio, hay que ejecutar pruebas comprobando que los datos de entrada producen los datos de salida correctos, y que datos incorrectos de entrada son detectados y atajados antes de destruir la integridad del sistema.

531. Para categoría ALTA, el ENS pide que se considere una auditoría de código fuente. Se refiere a la expresión inglesa "*source code review*" y no puede ser obligatorio para todos los sistemas ya que es un proceso desproporcionadamente lento y costoso. Además, es un proceso cuya profundidad es muy modulable.

532. La revisión de código fuente va más allá del empleo de herramientas automatizadas para buscar librerías, funciones o patrones de vulnerablidades, aspectos que ya se contemplan en categoría MEDIA. La revisión de código fuente es una actividad que requiere inteligencia humana para revisar sistemáticamente que el código se ejecutará de forma segura sin dejarle oportunidades a incidentes accidentales o deliberados, que no quedan puertas abiertas y que los controles de seguridad están implantados de forma efectiva. Por una parte, se busca que no haya vulnerabilidades y por otra que la aplicación sea capaz de defenderse a sí misma (*self-defending*) en el contexto en el que va a operar.

533. Esta actividad de expertos suele apoyarse en herramientas de auditoría y ataques controlados de penetración; pero va un paso más allá a analizar la integración de piezas de código o componentes. Las herramientas son ideales para tratar sistemáticamente grandes volúmenes de código y para validar que las vulnerabilidades son efectivamente explotables. Las personas son necesarias para comprender el contexto.

534. Por ejemplo, se buscan carreras (*race conditions*) en ejecución concurrente, oportunidades de escalar privilegios, fallos de limpieza de información sensible, acceso seguro a otros servicios, existencia de credenciales empotrados en el código, etc.

535. A efectos de cumplir con lo prescrito en el ENS, se valorará la oportunidad de proceder a la inspección del código fuente; pero en la práctica solo se justifica en sistemas críticos como pueden ser elementos de frontera con una red pública y solamente si el software no está acreditado en el sentido de [op.pl.5].

536. ISO/IEC 27000

- ISO/IEC 27002:2013:
  - 12.1.4 - Separación de los recursos de desarrollo, prueba y operación
  - 12.5.1 - Instalación del software en explotación
  - 14.2.8 - Pruebas funcionales de seguridad de sistemas
  - 14.2.9 - Pruebas de aceptación de sistemas
  - 14.2.7 - Externalización del desarrollo de software
  - 14.3.1 - Protección de los datos de prueba

537. NIST SP 800-53 rev. 4

538. Otras referencias:

- Métrica v3 - Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información, Ministerio de Administraciones Públicas, Consejo Superior de Administración Electrónica

5.7 [MP.INFO] PROTECCIÓN DE LA INFORMACIÓN

5.7.1 [MP.INFO.1] DATOS DE CARÁCTER PERSONAL

539. Es obligatorio el cumplimiento de la regulación de protección de información personal que esté vigente, ya sean las medidas de protección determinadas para cada nivel en el Real Decreto 1720/2007 o las especificaciones del Reglamento General de Protección de Datos.

540. Referencias

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. Nº 298, de 14 de diciembre de 1999)
- 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.
- Real Decreto 3/2010, de 8 de enero, del Esquema Nacional de Seguridad

- Real Decreto 951/2015, de 23 de octubre, de modificación 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.

5.7.2 [MP.INFO.2] CALIFICACIÓN DE LA INFORMACIÓN

541. Se debe establecer un esquema para asignar un nivel de calificación a la información, en función de sus necesidades de confidencialidad.

542. El sistema de calificación:

- debe ser acorde con otros sistemas de calificación propios del entorno en el que desarrolla su actividad la organización
- debe ser acorde con lo indicado en el Anexo I del ENS sobre calificación de la información y categorización de los sistemas de información
- debe establecer las responsabilidades para adscribir inicialmente una cierta información a una cierta calificación y para posibles re-calificaciones posteriores (niveles de seguridad) y determinar el responsable de la documentación y aprobación formal

543. Se deben desarrollar procedimientos de uso de la información para cada nivel (etiquetado y tratamiento), cubriendo al menos los siguientes aspectos:

- cómo se controla el acceso, es decir, normativa, y procedimientos de autorización y mecanismos de control [op.acc]
- cómo se realiza el almacenamiento (local, en la nube, cifrado, etc.) [mp.si.2] y [mp.si.3]
- normativa relativa a la realización de copias en diferentes medios: proceso de autorización y mecanismos de control [mp.info.9]
- cómo se marcan los documentos (etiquetado de soportes) [mp.si.1]
- condiciones de adquisición, inventario, marcado, uso, borrado y destrucción de los soportes de información
- cómo se gestiona el papel impreso y quién y dónde puede imprimir
- transporte físico: condiciones sobre el medio de transporte, del mensajero, autorizaciones de salida y controles de recepción
- condiciones de seguridad sobre el canal de comunicaciones (especialmente, autenticación y cifrado) y autorizaciones necesarias para poder trasmitir por redes de comunicaciones [mp.com]

544. Cabe esperar que los organismos organicen la información en tres niveles: BAJO, MEDIO y ALTO, alineados a los niveles del Anexo I. Siguiendo este esquema, se pueden desarrollar tablas como la siguiente:

	Bajo	Medio	Alto
responsable de la calificación: originador			
autorizado para recalificar: organismo			
autorizador de acceso [org.4]	• accesible a todo el personal propio	• accesible a los que lo necesitan conocer por sus funciones	• autorización del organismo a la persona
copias impresas [mp.si]	• marcadas • cada persona se encarga de su destrucción cuando ya no hace falta	• marcadas • destrucción usando destructora	• marcadas • se lleva un inventario de las copias realizadas • destrucción procedimentada con actualización del inventario
soportes electrónicos de información [mp.si]	• etiquetados • se borra el contenido o se inhabilita	• etiquetados • se cifra el contenido • se usa software de borrado seguro o se destruye	• etiquetados • se cifra el contenido • se usa software de borrado seguro o se destruye en trituradora homologada
uso en equipos portátiles y PDAs [mp.info.3] [mp.eq.3]	• con control de acceso	• con control de acceso	• debe estar cifrada en reposo
transmisión telemática [mp.com.2] [mp.com.3]	• canales autenticados	• canales autenticados y cifrados	• canales autenticados y cifrados

Tabla 5: Ejemplo de criterios de uso de acuerdo con la calificación de la información según categoría del sistema

545. Guías CCN-STIC:

- Guía CCN-STIC-001 - Seguridad de las TIC que manejan información nacional clasificada en la Administración

546. ISO/IEC 27000

- ISO/IEC 27002:2013:
  - 8.1.2 - Propiedad de los activos
  - 8.2.1 - Clasificación de la información

547. NIST SP 800-53 rev.

5.7.3 [MP.INFO.3] CIFRADO

548. Se debe cifrar la información de nivel alto, tanto durante su almacenamiento (mp.si.2) como durante su transmisión (mp.com.2). Sólo estará en claro mientras se está haciendo uso de ella. Esto incluye:
    - cifrado de ficheros
    - cifrado de directorios
    - discos virtuales cifrados
    - cifrado de datos en bases de datos

549. Se debe cifrar la información en función de su calificación y el medio en el que se almacena.

550. Guías CCN-STIC:
    - Guía CCN-STIC-807 – Criptografía de empleo en el ENS
    - Guía CCN-STIC-955 - Recomendaciones empleo GnuPG v 1.4.7
    - Guía CCN-STIC-955 B - Recomendaciones empleo GPG

551. ISO/IEC 27000
    - 27002:2013:
        - 10.1.1 - Política de uso de los controles criptográficos
        - 14.1.3 - Protección de las transacciones de servicios de aplicaciones
        - 18.1.5 - Regulación de los controles criptográficos

552. NIST SP 800-53 rev4:
    - [SC-13] Cryptographic Protection
    - [SC-28] Protection of Information at Rest

553. Otras referencias:
    - GNUPG – The GNU Privacy Guard
    - PGP – Pretty Good Privacy
    - Veracrypt

5.7.4 [MP.INFO.4] FIRMA ELECTRÓNICA

554. Todas las actividades relacionadas con la firma electrónica y el sellado de tiempo deben regirse por un marco técnico y procedimental aprobado formalmente. Se suele denominar Política de Firma.

555. En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio.

Política de firma electrónica

556. Política de firma electrónica. En el caso de la Administración General del Estado, debe cumplir los requisitos establecidos en el artículo 24 del Real Decreto 1671/2009.

557. En todos los casos debe cubrir los siguientes puntos técnicos y procedimentales:

- delimitación del ámbito de aplicación; es decir, qué información irá firmada y en qué procesos o procedimientos se firmará y se verificará cada firma
- los roles y funciones del personal involucrado en la generación y verificación de firmas
- los roles y funciones del personal involucrado en la administración de los medios de firma
- los roles y funciones del personal involucrado en la generación, custodia y distribución de claves y certificados
- directrices y normas técnicas aplicables a la utilización de certificados y firmas electrónicas
- los requisitos exigibles a las firmas electrónicas presentadas
- los medios de validación y verificación de firmas: protocolos y prestadores del servicio

558. En la Administración General del Estado se dispone de un marco de referencia. Ver http://administracionelectronica.gob.es/es/ctt/politicafirma

559. La política de firma debe cumplir los requisitos del Esquema Nacional de Interoperabilidad.

560. En cualquier escenario se debe buscar una interoperabilidad de las firmas electrónicas por lo que se recomienda fuertemente que los organismos referencien la política de firma de electrónica de un órgano superior y sólo en muy contadas ocasiones se establezca una política independiente.

Uso de claves concertadas para firmar

561. La firma con un secreto compartido requiere algunas cautelas.

562. Lo más que podemos hacer es:

- presentarle la información al ciudadano en una página web
- pedirle que introduzca la clave de firma (sin memoria: hay que introducirla expresamente)
- conservar como evidencia el HMAC[23] (documento + clave_concertada)

563. Este mecanismo garantiza la integridad del documento e identifica al ciudadano; pero no garantiza el no-repudio ya que cualquiera que puede verificar la firma,

[23] *hash message authentication code*. Código de autenticación de mensajes con función matemática resumen.

puede también generarla. Es decir, no cumple los requisitos de una firma electrónica avanzada, que requiere que "haya sido creada por medios que el firmante puede mantener bajo su exclusivo control" (Ley 59/2003).

564. Se considerará firma electrónica, sin más.

Código seguro de verificación

565. Se trata de una forma alternativa de asegurar la autenticidad e integridad de la información proporcionada por la Administración.

566. En lugar de proteger la información por medio de una firma inviolable, lo que se proporciona es una forma cómoda de verificar que la información es auténtica y no se ha modificado (es íntegra).

567. El sistema de código seguro de verificación (CSV) deberá garantizar, en todo caso:

- El carácter único del código generado para cada documento.
- Su vinculación con el documento generado y con el firmante.
- Asimismo, se debe garantizar la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento.

568. La Administración queda obligada a:

- garantizar la disponibilidad del mecanismo de verificación
- garantizar la integridad del documento referenciado
- garantizar la confidencialidad del documento correspondiente; por ejemplo, controlando el acceso para que sólo accedan las personas autorizadas

569. Una forma fácil de proporcionar CSVs es usar un número consecutivo en un archivo documental identificado (lo que sería una clave primaria en una base de datos documental). Al ciudadano hay que proporcionarle la identificación del archivo y el número de expediente.

570. Una forma fácil de cumplir los requisitos de autenticidad e integridad es que el documento referenciado por medio del CSV, sea en sí mismo un documento firmado electrónicamente. De esta forma, el ciudadano (o cualquier tercera parte autorizada) puede en cualquier momento recabar el documento y conservarlo en su poder.

Integridad o autenticidad: nivel BAJO

571. Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.

Integridad o autenticidad: nivel MEDIO

572. Si se utiliza una firma electrónica avanzada basada en certificados, estos certificados deberán ser cualificados.

573. Se emplean algoritmos y parámetros acreditados por el Centro Criptológico Nacional.

574. Se utilizan los formatos establecidos por la normativa para asegurar la validez de la firma (sin perjuicio de que se pueda ampliar el periodo): verificación de la validez del certificado y aportación de pruebas adicionales de validez (tales como consultas OCSP, CRL, etc.).

575. Se adjunta a la firma, o se referencia, toda la información pertinente para su verificación y validación: certificados y datos de verificación y validación.

576. Se protegen la firma, el certificado y los datos de verificación y validación con un sello de tiempo.

Integridad o autenticidad: nivel ALTO

577. Se usa una firma electrónica cualificada, que incorpora certificados cualificados y dispositivos cualificados de creación de firma.

578. Se emplean productos certificados, conforme a lo establecido en [op.pl.5].

579. Guías CCN-STIC:

- Guía CCN-STIC-807 – Criptografía de empleo en el ENS
- Guía CCN-STIC-405 - Algoritmos y Parámetros de Firma Electrónica

580. ISO/IEC 27000

- ISO/IEC 27002:2013:
  - 10.1.1 - Política de uso de los controles criptográficos
  - 14.1.3 - Protección de las transacciones de servicios de aplicaciones
  - 18.1.5 - Regulación de los controles criptográficos

581. NIST SP 800-53 rev. 4

- [SC-13] Cryptographic Protection
- [SC-28] Protection of Information at Rest

582. Otras referencias:

- Reglamento (UE) 910/2014, del Parlamento Europeo y el Consejo, de 23 de julio de 2014, relativo a la identificación electrónica (eID) y los servicios de confianza para transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Real Decreto 1671 de 2009
- NIST SP 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección

tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.

5.7.5 [MP.INFO.5] SELLOS DE TIEMPO

583. Los sellos de tiempo previenen la posibilidad de un repudio posterior de la información que sea susceptible de ser utilizada como evidencia en el futuro, o que requiera capacidad probatoria según la ley de procedimiento administrativo. Por ello, todas las actividades relacionadas con la firma electrónica y el sellado de tiempo deben regirse por un marco técnico y procedimental aprobado formalmente. Se suele denominar Política de Firma.
584. Debe identificarse y establecerse el tiempo de retención de la información.
585. Se fechan electrónicamente los documentos cuya fecha y hora de entrada debe acreditarse fehacientemente.
586. Se fechan electrónicamente los documentos cuya fecha y hora de salida debe acreditarse fehacientemente.
587. Se fechan electrónicamente las firmas cuya validez deba extenderse por largos periodos o así lo exija la normativa aplicable, hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte; alternativamente se pueden utilizar formatos de firma avanzada que incluyan fechado.
588. Guías CCN-STIC:
    - Guía CCN-STIC-807 Criptografía de empleo en el ENS
589. ISO/IEC 27000
    - ISO/IEC 27002:2013:
        - 14.1.3 - Protección de las transacciones de servicios de aplicaciones
590. NIST SP 800-53 rev. 4
    - [AU-10] Non-repudiation
    - ISO/IEC 18014-1:2008
      Information technology – Security techniques – Time-stamping services – Part 1: Framework
    - ISO/IEC 18014-2:2009
      Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens
    - ISO/IEC 18014-3:2009
      Information technology – Security techniques – Time-stamping services – Part 3: Mechanisms producing linked tokens
    - ISO/IEC TR 29149:2012
      Information technology – Security techniques –
      Best practices for the provision and use of time-stamping services
    - RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

5.7.6 [MP.INFO.6] LIMPIEZA DE DOCUMENTOS

591. Se debe retirar de los documentos que van a ser trasferido a un ámbito fuera del dominio de seguridad toda la información adicional contenida en campos ocultos, meta-datos, comentarios, revisiones anteriores, etc. salvo cuando dicha información sea pertinente para el receptor del documento.

592. Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorios de información.

593. El incumplimiento de esta medida puede perjudicar:

- al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento
- al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento
- a la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer

594. Guías CCN-STIC:

- Guía CCN-STIC-835 Borrado de metadatos en el marco del ENS

595. NIST SP 800-53 rev. 4

5.7.7 [MP.INFO.9] COPIAS DE SEGURIDAD (BACKUP)

596. Se deben realizar copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad a determinar por la organización.

597. Las copias de respaldo poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, debe considerarse la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad (en cuyo caso se estará a lo dispuesto en [op.exp.11]).

598. Se recomienda establecer un proceso de autorización para la recuperación de información de las copias de respaldo.

599. Se recomienda conservar las copias de respaldo en lugar(es) suficientemente independiente(s) de la ubicación normal de la información en explotación como para que los incidentes previstos en el análisis de riesgos no se den

simultáneamente en ambos lugares, por ejemplo, si se conservan en la misma sala utilizar un armario ignífugo.

600. El transporte de copias de respaldo desde el lugar donde se producen hasta su lugar de almacenamiento garantiza las mismas seguridades que los controles de acceso a la información original.

601. Las copias de respaldo deben abarcar:

- información de trabajo de la organización
- aplicaciones en explotación, incluyendo los sistemas operativos
- datos de configuración, servicios, aplicaciones, equipos, etc.
- claves utilizadas para preservar la confidencialidad de la información

602. Para los puntos anteriores ver [op.exp] y [mp.info.3].

603. El responsable de la información debe determinar la frecuencia con la que deben realizarse las copias y el periodo de retención durante el que mantenerlas.

604. En caso de disponer de un Plan de Continuidad, las copias de seguridad deberán realizarse con una frecuencia que permita cumplir con el RPO y con un objetivo de tiempo de restauración que permita cumplir el RTO.

605. Se recomienda realizar periódicamente pruebas de restauración de copias de seguridad.

606. ISO/IEC 27000

- 27002:2013:
  - 12.3.1 - Copias de seguridad de la información

607. NIST SP 800-53 rev4:

- [CP-6] Alternate Storage Site
- [CP-9] Information System Backup
- [CP-10] Information System Recovery and Reconstitution

608. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.10 - Data Recovery Capability

5.8 [MP.S] PROTECCIÓN DE LOS SERVICIOS

5.8.1 [MP.S.1] PROTECCIÓN DEL CORREO ELECTRÓNICO (E-MAIL)

609. Cuando se ofrezca correo electrónico como parte del sistema, deberá protegerse frente a las amenazas que le son propias mediante:

- Protección del cuerpo de los mensajes y documentos adjuntos que pueda contener el correo electrónico

- Protección del encaminamiento de mensajes (por ejemplo, protegiendo el servidor DNS[24] y su configuración) y del establecimiento de las conexiones (impidiendo que el usuario final pueda conectarse a un servidor de correo que no sea el corporativo)
- Protección de la organización frente a correos no solicitados (spam), virus, gusanos, troyanos, programas espías (spyware) y código móvil tipo applet[25] (por ejemplo, con la instalación de un antivirus, ya sea en el servidor de correo o en el puesto de usuario)
- Limitación del uso del correo electrónico al estrictamente profesional y concienciación y formación relativas al uso adecuado del mismo

610. Guías CCN-STIC:

- Guía CCN-STIC-681 – Configuración segura de servidores de correo Postfix
- Guía CCN-STIC-682 – Configuración segura de Sendmail
- Guía CCN-STIC-814 – Seguridad en Correo electrónico

611. ISO/IEC 27000

- ISO/IEC 27002:2013:
  - 13.2.3 - Mensajería electrónica

612. NIST 800-53 rev. 4

- [SI-8] Spam Protection

613. Otras referencias:

- SANS - CIS Critical Security Controls - Version 6.1
  - CSC.7 - Email and Web Browser Protections
- NIST SP 800-45 – Guidelines on Electronic Mail Security

5.8.2 [MP.S.2] PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB

614. Se debe proteger a los subsistemas dedicados a la publicación de información frente a los ataques o amenazas que les son propias.

615. Una serie de medidas son preventivas, poniendo el énfasis en los procesos de

- desarrollo de aplicaciones y servicios (mp.sw),
- configuración de seguridad (op.exp.2 y op.exp.3),
- en los controles de mantenimiento (op.exp.4) y
- en las protecciones de separación de tareas (op.acc.3)

[24] *Domain Name System*

[25] Programa empotrado en una página web. Cuando se accede a la página con un navegador, dicho programa se descarga y ejecuta automáticamente en el equipo del usuario. Ejemplos: applets java, ActiveX. CCN-STIC-401

616. Las tareas preventivas no excusan de un sistema de monitorización y reacción frente a ataques exitosos.

617. Pueden presentarse ataques a nivel de red, a nivel del sistema operativo del servidor y a nivel de la aplicación que atiende a peticiones web. De los dos primeros modos de ataque nos defenderemos protegiendo el equipo de frontera.

618. Básicamente hay 2 formas de proteger el servidor frontal: protegiendo el equipo y el software que proporciona la interfaz para acceso al servicio web, o disponiendo una protección previa en forma de cortafuegos de aplicación (appliance) entre el servidor y los usuarios.

619. Los ataques a nivel de aplicación pueden detectarse en el servidor frontal o en algún servidor de soporte en la retaguardia; es decir, puede haber ataques que aparecen como correctos (sintácticamente correctos) pero que causan problemas por el tipo de petición o por la secuencia de peticiones (semántica incorrecta). Para los ataques que entran en el nivel interno será necesario desarrollar reglas específicas para detectar y reaccionar. Reglas de tipo:

    - límite en el número de sesiones, total o por usuario anónimo o identificado
    - cierre de sesiones al cabo de un tiempo
    - límite en el volumen de datos (individual y agregado)

620. Para verificar que en el proceso de desarrollo de la aplicación se han establecido los controles frente a ataques potenciales se deben identificar posibles vulnerabilidades a corregir. Para ello se pueden realizar auditorías de seguridad periódicas o pruebas de penetración (hacking ético) de los servicios y aplicaciones web para posteriormente modificar el aplicativo o establecer elementos que lo protejan al menos frente a:

    - Ataques que eviten el control de acceso obviando la autenticación, si la hubiera, mediante accesos por vías alternativas al protocolo predefinido (por ejemplo, HTTP y HTTPS, manipulaciones de URL[26] o cookies[27] o ataques de inyección de código (como introducir caracteres no autorizados por la aplicación).
    - Ataques de escalado de privilegios (como ejecutar acciones haciéndose pasar por otro usuario).
    - Ataques de Cross Site Scripting (XSS) que permiten robar información delicada, secuestrar sesiones de usuario o comprometer la integridad del sistema (introduciendo información en la página web que se muestre así posteriormente al usuario, por ejemplo)
    - Ataques de manipulación de proxies y cachés, en caso de utilizar estas tecnologías.

[26] Uniform Resource Locator
[27] Pequeña cantidad de información que se le manda al navegador del cliente y que permite que éste quede identificado en conexiones sucesivas. CCN_STIC-401

621. Guías CCN-STIC:
    - Serie CCN-STIC-500 - Guías para Entornos Windows
    - Serie CCN-STIC-600 - Guías para otros Entornos
    - Guía CCN-STIC-812 - Seguridad en entornos y aplicaciones Web
622. ISO/IEC 27000
    - 27002:2013:
        - 14.1.2 - Asegurar los servicios de aplicaciones en redes públicas
623. NIST SP 800-53 rev. 4
624. Otras referencias:
    - SANS - CIS Critical Security Controls - Version 6.1
        - CSC.7 - Email and Web Browser Protections
    - NIST SP 800-44 - Guidelines on Securing Public Web Servers
    - PCI-DSS v3.0
        - Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

5.8.3 [MP.S.8] PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO

625. Se deben establecer medidas preventivas y reactivas frente a ataques de denegación de servicio (DoS[28]).
626. Los ataques de denegación de servicio pueden prevenirse dimensionando con holgura los elementos susceptibles de ser atacados desde el exterior, aunque poco se puede hacer frente a un ataque con suficientes recursos por parte del atacante.
627. Múltiples ataques de denegación de servicio son facilitados por un software deficiente por parte del servidor, bien porque no se han actualizado las versiones, bien porque la configuración no es idónea. Ambos aspectos deberán ser analizados y reparados (ver medidas de protección [mp.exp] en lo relativo a configuración, mantenimiento y cambios), de modo que se actualicen y bastionen las tecnologías utilizadas de cara a prevenir ataques conocidos.
628. Aun estando preparados, podemos ser víctimas de un nuevo tipo de ataque imprevisto, en cuyo caso hay que detectarlo rápidamente y gestionar la incidencia.
629. Los ataques de denegación de servicio pueden ser detectados y afrontados en el perímetro ([mp.com.1]), aunque pueden requerir la intervención de otros elementos. En el perímetro se pueden detectar patrones sospechosos de comportamiento: avalanchas de peticiones, peticiones trucadas y, en general, un uso malicioso de los protocolos de comunicaciones. Algunas de estas peticiones

[28] Denial of Service

pueden ser denegadas directamente por el equipo perimetral, en otras ocasiones hay que reaccionar ante ellos y levantar una alarma para actuar en donde corresponda (servidores web, servidores de bases de datos…, y contactando con el proveedor de comunicaciones o los centros de respuesta a incidentes, CERT[29]). Por tanto, es importante disponer de un procedimiento documentado que indique el procedimiento de reacción ante los ataques.

630. Es responsabilidad del organismo detectar y bloquear el uso deliberado o accidental del propio sistema de información para atacar a terceros desde las propias instalaciones. Nótese que el organismo puede ser simplemente víctima de una infección dañina de elementos agresivos que son lanzados contra otros o de un ataque deliberado por parte de un empleado interno y al proveedor de comunicaciones o al centro de respuesta de emergencia (CERT) para coordinar la respuesta.

631. Como posibles tecnologías a utilizar para prevenir ataques se encuentran los sistemas de detección de intrusos (IDS[30]), monitores con alarmas al alcanzar un consumo determinado de ancho de banda o de solicitud de peticiones, mecanismos para bloquear un número elevado de conexiones internas concurrentes o para bloquear el envío de grandes cantidades de información, etc.

632. Guías CCN-STIC:

- Guía CCN-STIC-820 – Guía de protección contra Denegación de Servicio

633. ISO/IEC 27000

- ISO/IEC 27002:2013:
  - 12.1.3 - Gestión de capacidades

634. NIST SP 800-53 rev. 4

- [CP-2] (2) Contingency Plan - Capacity Planning
- [SC-5] (2) Denial of Service Protection - Excess Capacity / Bandwidth / Redundancy

5.8.4 [MP.S.9] MEDIOS ALTERNATIVOS

635. Se debe prever medios alternativos para ofrecer los servicios en el caso de que fallen los medios habituales, mientras se recupera la disponibilidad de éstos (como por ejemplo una instancia alternativa a un portal). Estos medios alternativos estarán sujetos a las mismas garantías de protección.

636. Se debe establecer un tiempo máximo para que los servicios alternativos entren en funcionamiento.

[29] Computer Emergency Response Team
[30] Intrusion Detection System

637. Los servicios alternativos pueden estar dispuestos para entrar en servicio inmediatamente o requerir un tiempo de personalización. En todo caso, el tiempo de entrada en servicio debe estar respaldado por un análisis de impacto (ver [op.cont.1]).

638. El plan de utilización de servicios alternativos se vertebrará dentro del plan de continuidad aprobado (ver [op.cont.2]) y ser objeto de pruebas regulares para validar la viabilidad del plan (ver [op.cont.3]).

639. ISO/IEC 27000

- ISO/IEC 27002:2013:
  - 17.2.1 - Disponibilidad de los recursos de tratamiento de la información

640. NIST SP 800-53 rev. 4

- [CP] Contingency Planning

ANEXO A. GLOSARIO DE TERMINOS Y ABREVIATURAS

1. Ver guía CCN-STIC-800 Glosario de Términos y Abreviaturas del ENS.

ANEXO B. REFERENCIAS

1. Guías relacionadas con el ENS del CCN-CERT (https://www.ccn-cert.cni.es/)
   - 800 – Glosario de Términos y Abreviaturas
   - 801 – Responsables y Funciones
   - 802 – Guía de Auditoría
   - 803 – Valoración de los Sistemas
   - 804 – Guía de Implantación
   - 805 – Política de Seguridad de la Información
   - 806 – Plan de Adecuación
   - 807 – Criptología de empleo en el ENS
   - 808 – Verificación de Cumplimiento de las Medidas en el ENS (auditoría técnica)
   - 809 – Declaración y Certificación de Conformidad del ENS y distintivos de cumplimiento.
   - 810 –Guía de Creación de un CERT/CSIRT
   - 811 – Interconexión en el ENS
   - 812 – Seguridad en entornos y aplicaciones Web
   - 813 – Componentes Certificados en el ENS
   - 814 – Seguridad en Correo Electrónico
   - 815 – ENS Métricas e Indicadores
   - 817 – Gestión de Ciberincidentes
   - 818 – Herramientas de Seguridad en el ENS
   - 820 – Guía de protección contra Denegación de Servicio
   - 821 – ENS Normas de Seguridad
   - 822 – ENS Procedimientos Operativos de Seguridad
   - 823 – Utilización de Servicios en la nube
   - 824 – ENS Informe del Estado de Seguridad
   - 825 –Certificaciones 27001
   - 827 –Gestión y uso de dispositivos móviles
   - 830 – Ámbito de aplicación del Esquema Nacional de Seguridad
   - 835—Borrado de metadatos en el marco del ENS
   - 844 – INES – Informe Nacional del Estado de Seguridad - Manual de Usuario
   - 845A – LUCIA. Manual de Usuario
   - 845B – LUCIA. Manual de Usuario con Sistema de Alerta Temprana (SAT)
   - 845C – LUCIA. Manual Instalación Organismo
   - 845D – LUCIA. Manual de Administrador
2. DSD - Australian Defence Signals Directorate (DSD)

Top 35 Mitigation Strategies
http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

3. ENS
   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 actualizado por Real Decreto 951/2015, de 23 de octubre,
   https://www.ccn-cert.cni.es/publico/ens/ens/index.html
4. ISO/IEC 27000
   Information technology – Security techniques – Information security management systems – Overview and vocabulary
5. ISO/IEC 27001
   Information technology – Security techniques – Information security management systems – Requirements
6. ISO/IEC 27002
   Information technology – Security techniques – Code of practice for information security management
7. ISO/IEC 27003
   Information technology – Security techniques – Information security management system implementation guidance
8. ISO/IEC 27005
   Information technology – Security techniques – Information security risk management
9. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
10. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
11. Manageable Network Plan
    NSA, version 2.2, April 2012
12. NIST SP 800-37 Rev.1
    Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
13. NIST SP 800-39
    Managing Information Security Risk: Organization, Mission, and Information System View
14. NIST SP 800-53 rev. 4
    Recommended Security Controls for Federal Information Systems,
    http://web.nvd.nist.gov/view/800-53/home
    http://csrc.nist.gov/

15. RD 1065/2007

Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos.

16. 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

17. SANS

    20 Critical Security Controls
    http://www.sans.org/critical-security-controls/