GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-403)

GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICOS

DICIEMBRE 2007

Edita:

NIPO: 076-07-236-6

Tirada: 1000 ejemplares
Fecha de Edición: diciembre de 2007
ISDEFE S.A. y TB Security han participado en la elaboración y modificación 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

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

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

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función, 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.

Diciembre de 2007

Alberto Sáiz
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

TABLAS

1. INTRODUCCIÓN

1. Las organizaciones tienen cada vez más una alta dependencia de sus Sistemas TIC, siendo estos activos en algunos casos realmente críticos para su funcionamiento.

2. La dedicación de un esfuerzo adicional a la seguridad de los sistemas para preservarlos de las nuevas amenazas es una tendencia común en las organizaciones. Además del establecimiento de una política de seguridad adecuada y la implantación de las medidas preventivas adecuadas, es necesario definir una capacidad de respuesta en caso que llegue a materializarse una amenaza.

3. Esta "capacidad de respuesta" obliga a la Organización a disponer de los medios materiales y humanos adecuados que con una correcta aplicación de los correspondientes procedimientos permitan disminuir el impacto provocado por un incidente de seguridad y reestablecer la confidencialidad, integridad y/o disponibilidad de los activos.

4. La gestión de incidentes de seguridad en los Sistemas de Información y Telecomunicaciones de la Organización permitirá fundamentalmente dos cosas:

    - Reacción efectiva ante el incidente para la salvaguarda de los activos.
    - Nuevo conocimiento para la mejora proactiva de la seguridad.

5. La Organización debe aprender de todos y cada uno de los incidentes que se hayan producido en ella para mejorar los mecanismos de protección y con ello prevenirlos en el futuro.

6. No importa si somos una Organización pequeña o grande, debemos asumir que tarde o temprano estamos destinados a sufrir un incidente de seguridad, por lo tanto no es cuestión de si ocurrirá sino de cuando lo hará. Esto suele ser así porque el paso del tiempo nos trae nuevas amenazas y vulnerabilidades de diferente índole que someten a la seguridad a un ciclo de vida evolutivo.

2. OBJETO

7. Servir de guía para la implantación de una capacidad de respuesta ante incidentes informáticos, definiendo procedimientos de actuación e identificando responsabilidades, y recursos humanos y materiales para resolver en el menor tiempo posible y del modo más efectivo un incidente.

3. ALCANCE

8. Esta guía contiene recomendaciones para la implantación de una capacidad de respuesta ante incidentes informáticos. Por tanto, las Autoridades responsables de la Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC) determinarán el alcance de su aplicación.

4. CONCEPTOS GENERALES

9. Un Incidente de Seguridad en un Sistema, lo constituye cualquier situación o eventualidad en la que pueda verse amenazada la información, y pueda en consecuencia dar lugar a una pérdida de:

    - Confidencialidad.
    - Integridad
    - Disponibilidad

10. Podríamos decir que un Incidente es un evento adverso a los Sistemas de Información que aunque se haya materializado puede haberlos dañado o no dependiendo del entorno y el contexto. Cabe decir que no siempre es causado de manera intencionada sino que en algún caso es fruto del azar, negligencias o desconocimiento de usuarios o administradores, etc.

11. En gran parte de los casos, la respuesta a un incidente se asemeja bastante a la aplicación de unos “primeros auxilios” donde es importante actuar con conocimiento, celeridad y determinación. La presión asociada no suele facilitar dicha tarea

12. La Capacidad de Respuesta ante Incidentes, conocida como “Computer Incident Response Capability” (CIRC), es el conjunto de medios humanos, materiales y procedimientos encargados de identificar y gestionar los incidentes de seguridad. Dentro de esta Capacidad destaca especialmente el papel a los Equipos de Respuesta de Incidentes (ERI) que se describe a continuación.

13. Un Equipo de Respuesta a Incidentes (ERI), conocido como “Computer Emergency Response Team” (CERT) o “Computer Security Incident Response Team” (CSIRT), es un conjunto de expertos en redes, sistemas y seguridad en las TIC cuyo principal objetivo es dar respuesta a los incidentes de seguridad producidos en su ámbito de actuación.

14. En una Organización pueden existir múltiples equipos que pueden dar cobertura a diferentes departamentos o áreas de la organización. Incluso en organizaciones grandes puede darse una jerarquía de equipos en un modelo totalmente distribuido. Para cualquier ERI es vital conocer cual es la comunidad (constituency) o áreas a las que ofrece sus servicios y cual es su objetivo a cumplir (mission statement).

15. Aunque el origen de las Capacidades de Respuesta está estrechamente relacionado con las acciones reactivas, en muchas ocasiones los ERI se convierten en el núcleo duro del ciclo de vida de la seguridad ofreciendo también servicios proactivos y de valor añadido a su comunidad tales como avisos de vulnerabilidades, publicación de recomendaciones y buenas prácticas, asesoramiento en tecnologías de la seguridad, etc. Una aproximación de ellos puede verse en la Tabla 1.

16. Los ERI suelen ser entornos dinámicos donde el capital humano cobra especial importancia y donde, sus componentes pueden estar dedicados o no exclusivamente a éste. La seguridad tiene un ámbito de actuación horizontal y por ello suele requerir cubrir un amplio conocimiento de las TIC con equipos multidisciplinares.

17. Como veremos en detalle, la Gestión de Incidentes de Seguridad en los Sistemas engloba el ciclo de vida completo del incidente en sus diferentes áreas: inicio, gestión y resolución.

Servicios Reactivos	Servicios Proactivos	Servicios de Valor Añadido
Alertas y avisos	Boletines y anuncios	Análisis de artefactos
Gestión de incidentes	Seguimiento tecnológico	Respuesta ante artefactos
Análisis de incidentes	Auditorias y evaluaciones de la seguridad	Coordinación de la respuesta ante artefactos
Soporte a la respuesta a incidentes	Configuración y mantenimiento de la seguridad	Análisis de riesgo
Coordinación en la respuesta a incidentes	Desarrollo de herramientas de seguridad	Planes de continuidad de la actividad y de recuperación ante desastres
Respuesta presencial ante incidentes	Detección de Intrusiones	Consultoría de seguridad
Gestión de vulnerabilidades	Difusión	Concienciación de la seguridad
Análisis de vulnerabilidades		Formación en seguridad
Respuesta ante vulnerabilidades		Evaluación y certificación de productos
Coordinación de la respuesta ante vulnerabilidades		

Tabla 1. Servicios CSIRT según CERT-CC

18. Algunos ERI no ofrecen servicios tan sólo a una Organización sino que también pueden ofrecer servicios de respuesta a incidentes, especialmente los de coordinación, cubriendo una comunidad más amplia como una red académica, un conjunto de fabricantes o proveedores de servicio o incluso una nación. En el Anexo B se puede encontrar un listado de los ERI existentes tanto en el ámbito nacional como internacional

19. En lo que se refiere a la gestión de incidentes trataremos varios aspectos vitales a considerar:

    - Organizativos: aquellos de tipo más administrativo relativos a la Organización.
    - Operacionales: aquellos de tipo más técnico relativos a la Operación.

20. La gestión de incidentes se alimenta especialmente de las notificaciones recibidas por los miembros de la Organización que alertan de la existencia de un incidente o de su posible existencia. Esto hace que cobren especial importancia los mecanismos de interfaz del ERI, como puede ser por ejemplo el formulario de alta de incidentes que permite describir en un formato establecido toda la información necesaria para iniciar la capacidad de respuesta. Disponemos de un ejemplo en el Anexo A.

21. Al inicio del incidente es necesario proporcionar información suficiente que permita responder en la medida de lo posible tanto cualitativamente como cuantitativamente las siguientes cuestiones:

    - ¿QUÉ ha sucedido o CUALES son los signos de alerta?
    - ¿DÓNDE ha ocurrido?
    - ¿CUÁNDO se produjo?
    - ¿CÓMO o en que circunstancias?
    - ¿POR QUÉ se ha producido o CUAL es su origen?

5. ASPECTOS ORGANIZATIVOS

22. La gestión de incidentes de seguridad informáticos es una de las partes más visibles dentro de la gestión de la seguridad de la información en la Organización.

23. Cada Organización cuenta con sus propias particularidades de estructura y funcionamiento y por ello para poder ofrecer una gestión de incidentes operativa y funcional, se hace necesario estudiar en detalle el papel de ERI dentro de la organización tanto en lo que respecta a sus funciones como en su potencial autoridad dentro de la jerarquía organizativa.

24. El ERI no es un proyecto más dentro de la Organización que cuente con un inicio y fin, siendo no tan solo necesaria una inversión en su creación sino su mantenimiento mediante la asignación de un presupuesto anual que permita el financiamiento de sus actividades.

5.1. DEFINICIÓN

25. La definición del ERI es el primer y más importante de los aspectos a abordar y consiste por un lado en intentar plasmar los objetivos y función a cumplir dentro de la Organización, y por otro lado delimitar su ámbito de actuación.

26. En ningún caso debemos mantener estas cuestiones abiertas o de manera ambigua ya que con toda seguridad ocasionará una falta de identidad y en algunos casos problemáticas en su autoridad y mecanismos de operación.

5.2. UBICACIÓN

27. La ubicación de un ERI en la jerarquía de la Organización puede determinar su ámbito de actuación y la autoridad que tiene sobre este. Generalmente para evitar que se perviertan sus actividades o puedan ser manipuladas según determinados intereses, deberá ser una entidad independiente y estar por encima de los departamentos o áreas a cubrir.

28. Su ubicación aunque limite parcialmente su ámbito de actuación, deberán garantizarse los mecanismos de notificación y reporte a los responsables AOSTIC.

29. Los Equipos de Respuesta pueden ser múltiples dentro de una organización siguiendo uno de estos modelos:

    - Centralizado: se controla de manera centralizada la Capacitación de Respuesta.
    - Distribuido: existen múltiples equipos que actúan de manera coordinada.
    - Híbrido: mezcla de los dos anteriores.

30. El modelo a aplicar dependerá de la organización aunque suele destacar por su eficiencia la creación de equipos híbridos donde un equipo central realiza las tareas de coordinación y de más alto nivel, mientras que existen equipos distribuidos en las diferentes áreas que realizan un trabajo de campo más directo y colaboran con el anterior.

5.3. SERVICIOS

31. Desde la creación de un equipo se deben describir cuales son los servicios reactivos, proactivos y de valor añadido a ofrecer a su comunidad.

32. Habitualmente se suele comenzar con un pequeño subconjunto de servicios agrupados en el área de servicios reactivos para posteriormente evolucionar naturalmente hacia aquellos necesarios o demandados por nuestro entorno.

33. Se recomienda no ser especialmente ambicioso en este aspecto e intentar abarcar gran multitud de áreas si ello conlleva no realizar las tareas asociadas con la calidad necesaria. Por ello el crecimiento debería ser gradual y justificado.

34. En la Tabla 1 del punto 4 se pueden encontrar algunos de los servicios habituales según una descripción del CERT-CC. En esta tabla los servicios de seguridad se encuentran clasificados bajo tres agrupaciones:

- **Servicios reactivos:** destinados a minimizar el impacto de una amenaza o incidente.
- **Servicios proactivos:** cuya función es reducir los riesgos de seguridad mediante distribución de información e implantación de sistemas de protección y detección.
- **Servicios de valor añadido:** mediante los cuales se pretenden mejorar los procesos de trabajo tanto de la comunidad a la que se da servicio como del propio CERT

35. Una descripción más detallada de los principales servicios de un CERT pueden encontrarse en el Anexo C.

5.4. RELACIÓN CON OTROS EQUIPOS

36. La respuesta a incidentes suele requerir en muchos casos la relación con equipos externos pertenecientes a otras Organizaciones. En algunos casos incluso se puede contar con equipos externos globales que garanticen la coordinación entre los incidentes de nuestra comunidad y otros equipos externos.

37. Establecer vínculos de confianza con otros equipos es extremadamente importante a la hora de la gestión de incidentes, ya que en múltiples ocasiones necesitaremos de su ayuda y el intercambio de conocimiento o de información suele estar directamente relacionado con el nivel de confianza entre ambos.

38. Para establecer relaciones con otros equipos, se recomienda participar en foros e iniciativas de respuesta a incidentes tales como el TF-CSIRT/Trusted Introducer (TI) o FIRST.

39. Puede encontrar información sobre los mencionados foros y algunos equipos nacionales e internacionales en el Anexo B. No olvidemos que las fuerzas del orden también cuentan con su Capacitación de Respuesta a Incidentes.

6. ASPECTOS OPERACIONALES

40. La capacidad de respuesta ante incidentes informáticos hace necesaria la existencia de un conjunto de recursos humanos y materiales para poder llevar a cabo sus funciones de manera satisfactoria.

41. A continuación se describen los aspectos más importantes a tener en cuenta para la operación y correcto funcionamiento de un Equipo de Respuesta a Incidentes.

6.1. PERSONAL

42. El personal perteneciente a un ERI debe ser seleccionado cuidadosamente ya que sus conocimientos y habilidades son vitales para las tareas de respuesta a incidentes.

43. Además de los conocimientos técnicos necesarios, se debe valorar especialmente las siguientes habilidades interpersonales:

- Sentido común.
- Capacidad de comunicación oral y escrita.
- Diplomacia.
- Habilidad para seguir políticas y procedimientos.
- Motivación y ganas de aprender.
- Capacidad para trabajar bajo presión.
- Capacidad para trabajar en equipo.
- Integridad y sentido de la responsabilidad.
- Capacidad de resolución de problemas.
- Buen manejo del tiempo y reconocimiento de errores.

44. El equipo debe contar con un mínimo razonable de personal que conforme el núcleo duro de la respuesta y coordinación de incidentes aunque no todos ellos deben tener una dedicación completa. En el caso de ser parcial, se debe intentar siempre un mínimo de tiempo para que siga la actividad de las tareas que se le asignen y que se disponga de cierta flexibilidad horaria para ampliar dicha disponibilidad ante ciertas eventualidades.

45. En función del tamaño de la Organización se puede contar con especialistas no solo en áreas técnicas sino también en áreas legales, psicología, etc. Durante el ciclo de vida de un incidente se puede contar excepcionalmente con miembros de la Organización que proporcionen conocimiento en sus áreas de especialización componiendo un equipo multidisciplinar.

46. No debemos olvidar que la experiencia es un factor clave ya que los incidentes llevan al personal a un aprendizaje continuo. Se debe favorecer un entorno dinámico con rotación de roles tanto para la formación del personal como para evitar el desgaste asociado a algunas de las tareas.

47. El personal debe estar formado y entrenado de manera periódica tanto a nivel técnico como en los procedimientos de respuesta del ERI. Esto mejorará cuantitativamente y cualitativamente la calidad de la respuesta.

6.2. INSTALACIONES

48. Las instalaciones del ERI deben estar ubicadas en un espacio físico separado donde se puedan garantizar la aplicación de ciertas medidas de seguridad física.

49. Se realizará un control de acceso seguro en las instalaciones que garantice el acceso solo del personal autorizado y se registren dichos accesos.

50. Tanto el cableado de datos que llega a las instalaciones como el desplegado en su interior debe estar protegido para evitar su manipulación no autorizada que hiciera posible la intercepción de las comunicaciones.

51. Los sistemas de información, estén ubicados o no en armarios de comunicaciones, deben tener mecanismos de seguridad física que impida su apertura o manipulación no autorizada.

52. Para poder gestionar de manera segura la información en formato papel o en cualquier soporte digital, se contará con cajones y archivadores para cada miembro y compartidos. Deberá fomentarse una política de “mesas limpias” donde siempre resida el menor número de información posible sobre el espacio de trabajo de los miembros del equipo.

53. Para la preservación de las copias de seguridad y las evidencias en depósito, se hace necesaria la instalación de una caja fuerte ignífuga.

6.3. SISTEMAS DE INFORMACIÓN

54. Los Equipos de Respuesta a Incidentes deben contar con unos recursos TIC dedicados para garantizar la realización segura de las tareas que tienen asignados.

55. Se dispondrá de una red privada segmentada del resto de la infraestructura de la Organización aunque estará interconectada con ésta. En algunos casos puede incluso ser necesario disponer de una conectividad externa dedicada. Dicha red estará protegida y monitorizada utilizando los mecanismos habituales en la Organización: cortafuegos, sistemas de detección de intrusiones, antivirus, etc.

56. Para las comunicaciones electrónicas se contará con un servidor de correo electrónico. La difusión electrónica del equipo así como la publicación de la información de contacto, siguiendo como mínimo la información requerida en el estándar RFC2350, se realizará mediante un servidor web.

57. El personal contará con estaciones de trabajo fijas y portátiles para poder realizar las tareas de respuesta desde las instalaciones propias o desde el exterior. En este último caso se deberán proporcionar mecanismos de acceso remoto mediante tecnologías de redes privadas virtuales (VPN) utilizando cifrado robusto.

58. Se contará con todos aquellos dispositivos de soporte, aislados o por red, que sean necesarios tales como impresoras, facsímiles, escáneres, etc. Tampoco olvidaremos la implementación de mecanismos de copia de seguridad (backup) para todos los sistemas que lo requieran.

59. Es extremadamente importante contar con un laboratorio y una red de pruebas de manera que se puedan realizar pruebas y construir maquetas que nos permitan reproducir incidentes de seguridad, probar herramientas de ataques, analizar código malicioso, etc.

60. Dicho laboratorio deberá estar formado por una amplia variedad de sistemas y dispositivos de red. Para una mayor flexibilidad y un menor coste se recomienda optar por soluciones basadas en virtualización.

61. Dependiendo del tipo de función del ERI en la Organización, además se deberá contar con las consolas de sistemas de monitorización y gestión de eventos que le permitan recibir las alertas y eventos de seguridad e interrogarlos para obtener información útil para la investigación de los incidentes de seguridad.

6.4. COMUNICACIONES

62. Las comunicaciones es uno de los aspectos que deben cuidarse especialmente ya que son una de las principales herramientas de trabajo de los ERI. Además, por la propia naturaleza de los incidentes y los sistemas afectados, debemos considerar que en muchos casos deberá circular información sensible.

63. Los mecanismos más utilizados son los siguientes:

- Telefonía fija y móvil.
- Fax.
- Correo electrónico.
- Correo postal.
- Mensajería instantánea.
- Transferencia de datos por red.

64. El teléfono junto con el correo electrónico suelen ser los medios preferidos para la comunicación en las Organizaciones.

65. El correo electrónico es un mecanismo conveniente porque además de ser un medio de comunicación rápido y flexible, puede permitir a múltiples usuarios el acceso a un único buzón, la transmisión de datos y es menos intrusivo al ser de tipo asíncrono. La confidencialidad e integridad de los datos se puede garantizar mediante la firma y cifrado utilizando estándares como PGP o certificados digitales basados en X.509.

66. El teléfono suele ser el otro mecanismo estrella que aunque suele ser más rápido es más intrusivo al ser de tipo síncrono. Es un mecanismo que consume más recursos y en algunos casos incluso puede llevar asociado un coste económico. Su confidencialidad se puede garantizar mediante cifradores. La telefonía móvil es realmente conveniente para ofrecer servicios 24x7 y garantizar la movilidad de los miembros del ERI.

67. Cabe decir que cada vez más se están imponiendo nuevas tecnologías de comunicaciones como la Telefonía o videoconferencia IP y la Mensajería Instantánea que combinan lo mejor de ambos mundos, es decir una cierta interactividad humana combinada con la transmisión dinámica de información por la red de datos.

68. Aunque se deben aconsejar los mecanismos preferibles de comunicación, se deben proporcionar servicios sobre varios de ellos tanto por la conveniencia de la comunicación con los miembros de la Organización, como para diversidad y alta disponibilidad en las comunicaciones. Siempre debe quedar claro qué tipo de información puede comunicarse a través de ellos y bajo que requisitos.

6.5. POLÍTICAS Y PROCEDIMIENTOS

69. Los procesos administrativos y técnicos asociados al Equipo de Respuesta a Incidentes deben ser correctamente documentados en los correspondientes procedimientos. Sin olvidar que todos éstos deben estar alineados bajo el marco de una política y normativa de la Organización. Los documentos deben estar convenientemente enlazados.

70. Los procedimientos de respuesta deben estar en constante mejora para que proporcionen una información actualizada y detallada al ERI y a los propios usuarios de los pasos a tomar en cualquier acción de respuesta.

71. La política de respuesta a incidentes debe cubrir áreas especialmente sensibles como los códigos de conducta del personal, la clasificación de la información tratada, las comunicaciones y mecanismos de contacto, etc.

72. Suele ser imprescindible la recogida de la información sobre los puntos de contacto necesarios y la redacción del procedimiento de notificación y escalado que corresponda.

6.6. HERRAMIENTAS

73. Una buena capacidad de respuesta suele venir determinada no tan solo por el conocimiento de los miembros del ERI sino también por la calidad de las herramientas utilizadas.

74. Se debería disponer de herramientas básicas y avanzadas que cubran las necesidades de gestión y análisis de los incidentes en los siguientes ámbitos:

    - Análisis de tráfico.
    - Procesamiento de trazas de registro (*logs*).
    - Análisis de código malicioso (ingeniería inversa) y forense.
    - Evaluación de la seguridad y análisis de vulnerabilidades.
    - Monitorización y alerta temprana.
    - Gestión de incidentes.

75. Al ser la respuesta a incidentes la actividad principal de un ERI, convierte a la herramienta de gestión de incidentes en la más destacable y necesaria. Esta suele consistir en una base de datos y una aplicación informática en la que se registran todos los datos de los incidentes de seguridad, desde la notificación hasta la resolución de los mismos. Entre otras funcionalidades, resulta necesario identificar la situación del incidente según unos determinados estados:

    - Abierto: el incidente ha sido comunicado y dado de alta.
    - En proceso: el incidente está siendo tratado y está en fase de resolución.
    - Suspendido: en espera de alguna herramienta o investigación.
    - Cerrado: el incidente ha sido resuelto o cerrado.
    - Conclusión: se han elaborado las conclusiones.

76. Además del estado del incidente, la base de datos debe almacenar por cada incidente al menos los siguientes datos:

    - Identificador único.
    - Descripción del incidente.
    - Acciones tomadas hasta el momento para su resolución.
    - Datos de contacto.
    - Datos del Sistema afectado.
    - Tipo de información involucrada en el incidente.
    - Listado de evidencias recogidas.
    - Próximas acciones a tomar.
    - Fecha de resolución.
    - Observaciones.

77. La herramienta de gestión puede ser accesible por el resto de personal de la Organización, debiéndose entonces definir para ello una política de control de acceso, en la que se establezcan los distintos privilegios de entrada, consulta y modificación.

78. En caso de ser accesible por el resto del personal de la Organización, la comunicación del incidente podría hacerse a través de este medio, además de medios alternativos o complementarios como el correo electrónico.

79. En el Anexo D se describen las dos herramientas de este tipo más extendidas, utilizadas por equipos de respuesta a incidentes de todo el mundo, conocidas como "Request Tracker Incident Response" (RTIR) y "System for Incident Response In Operational Security"-"Open Request Tracker System" (SIRIOS-OTRS).

7. CICLO DE VIDA

80. Un incidente de seguridad pasa por diversas etapas desde su notificación e identificación hasta que se le da respuesta y solución. Es importante considerar cuales son las metas a cumplir en cada una de ellas y seguir el flujo establecido, evidentemente con una cierta adaptación a las particularidades que establece la diversidad de tipología de los incidentes.

81. El ciclo de vida clásico de un incidente pasa por las siguientes etapas:

    - Prevención y preparación.
    - Detección e identificación.
    - Notificación.
    - Contención.
    - Análisis e investigación.
    - Solución y recuperación.
    - Reflexión y mejora.

82. Aunque algunas fases sean secuenciales, ello no quiere decir que no puedan ejecutarse otras en paralelo o que resulte necesario en algún caso incluso volver atrás en el proceso.

83. Podríamos destacar 3 áreas dentro de las fases descritas:

- **Inicio:** se recibe la información del incidente y se realiza un breve análisis con el objetivo de valorar el impacto y gravedad del incidente y empezar a decidir cuáles serán las primeras medidas de notificación y contención necesarias.
- **Gestión:** análisis del incidente que lleva a realizar acciones de investigación, contención y notificación con todos los entes implicados. El objetivo reside en encontrar las acciones que nos permitan su resolución con el menor impacto.
- **Resolución:** aplicación de las medidas correctores necesarias que permitan resolver el incidente y organizar toda la información recogida durante éste para generar la documentación de cierre.

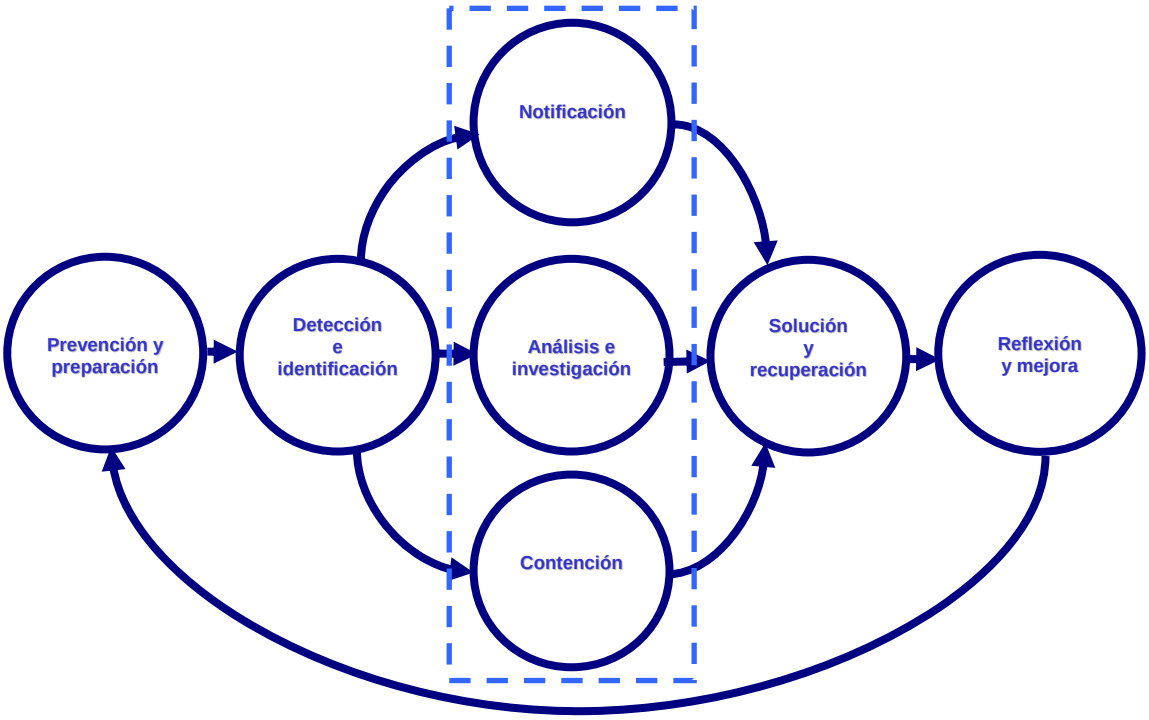


Fig. 1 - Ciclo de Vida de la Respuesta a Incidentes

84. En el Anexo E se encuentran unas listas de verificación con una lista resumen de los pasos a realizar en caso de un incidente desde la fase de “Identificación”. Se incluye una lista para las siguientes categorías de incidente:

- Incidentes en general.
- Intrusiones.
- Código malicioso.
- Phishing.
- Denegaciones de Servicio.

7.1. PREVENCIÓN Y PREPARACIÓN

85. La gestión de los incidentes también suele incluir una fase proactiva cuyo objetivo es por un lado prevenir la aparición de los incidentes y por otro preparar al ERI ante cualquier incidente que se pueda llegar a producir.

86. La prevención es vital para intentar minimizar el número o impacto de los incidentes que finalmente llegan a manos del ERI. Las tareas preventivas suelen ir íntimamente ligadas al seguimiento tanto de las amenazas y vulnerabilidades fuera de la organización como aquellas identificadas en la Organización en incidentes previos. Podemos englobar entre otras la siguientes tareas:

- Notificación de nuevas vulnerabilidades en los productos utilizados en la Organización.
- Difusión de avisos visos sobre la existencia de nuevas o inminentes amenazas tales como código malicioso de alta difusión (gusanos, troyanos, etc.).
- Recomendaciones de la aplicación de medidas de protección o identificación ante situaciones excepcionales.
- Formación y concienciación del personal en buenas prácticas del uso de los recursos TIC y en la forma de actuar cuando se identifica un posible incidente de seguridad.

87. En gran parte de los casos, la alta carga de trabajo a la que están sometidos los ERI impide que se puedan revisar y mantener las tareas de preparación adecuadas para la realización de su trabajo. La preparación es un aspecto a tener en cuenta si se desea cuidar la calidad en la Capacidad de Respuesta y suele llevar asociada entre otras estas tareas:

- Formación adecuada del personal del ERI.
- Redacción y revisión de los procedimientos, listas de verificación (*checklist*) y estrategias de respuesta a incidentes.
- Establecimiento de los contactos internos y externos adecuados: responsables de área, dirección, fuerzas del orden, ERIs de coordinación, etc.
- Mecanismos de contacto y disponibilidad de los miembros que no trabajan exclusivamente en el ERI para la creación dinámica de grupos multidisciplinares.
- Operatividad de los mecanismos de comunicación en banda y fuera de banda necesarios: correo electrónico, teléfono, fax, etc.
- Disponibilidad de un área de reuniones para la gestión del incidente con unas garantías mínimas de confidencialidad.
- Entrenamiento del ERI en incidentes simulados para identificar las carencias y problemas en las diferentes etapas del ciclo de vida y mantener la tensión y frescura de los conocimientos del equipo.
- Despliegue de mecanismos de monitorización tales como sistemas de detección de intrusiones y gestores de eventos que permitan identificar los incidentes de manera proactiva.

- Disponibilidad de un kit de respuesta a incidentes que incluya todo el material administrativo y técnico necesario para dar respuesta remota o presencial ante un incidente (teléfono, procedimientos, cables, grabador de audio/video, discos duros y flexibles, conmutadores, programas de análisis, bolsas de recogida de evidencias, etc.)

88. Como conclusión consideremos que esta fase de prevención y preparación puede mejorar substancialmente tanto la seguridad TIC de la Organización como la capacidad de respuesta ante incidentes.

7.2. DETECCIÓN E IDENTIFICACIÓN

89. Al producirse un incidente de seguridad, éste no siempre es notificado de manera instantánea bien sea porque se carecen de los mecanismos de detección necesarios o incluso por el propio desconocimiento de los mecanismos de comunicación ante incidentes de las personas que lo detectan.

90. La detección es un momento crítico en cualquier incidente porque cuanto más tarde se produzca esta situación junto con el tiempo necesario para que su notificación llegue al personal de respuesta, el impacto puede ser mayor en los sistemas de información de la Organización. Es lo que se conoce como detección temprana.

91. Los mecanismos de detección pueden ser :

- Manuales: notificado directamente por un humano o gracias a un mecanismo de alerta o de auditoría revisado por este.
- Automáticos: identificación mediante un sistema de detección automático tales como un sistema de detección de intrusiones o un sistema de gestión de eventos.

92. Cabe destacar que la detección humana mejora si se provee a éstos de las herramientas e información de signos de alerta necesarios. Lo mismo sucede con los mecanismos automáticos donde su adecuada configuración por personal cualificado es básica para una correcta detección.

93. Cualquier miembro de la Organización (usuario, administrador, personal de mantenimiento, etc.) que detecte una circunstancia anómala que, según su criterio, pueda afectar a la seguridad de un Sistema, será responsable de informar de esa circunstancia bajo los procedimientos de comunicación que se hayan puesto en su conocimiento: llamada o correo electrónico al Servicio de Informática y Atención al Usuario (SIAU), formulario web dirigido al Equipo de Respuesta a Incidentes, etc.

94. El formulario de comunicación del incidente deberá estar disponible en un lugar conocido por todos los usuarios y ser fácilmente accesible. Un ejemplo sería la intranet de la Organización. En el Anexo A se ofrece un ejemplo de formulario de alta de un incidente.

95. Se debe evitar que el desconocimiento sobre la naturaleza de los incidentes haga dudar a los usuarios sobre su modo de actuar. Por lo tanto, los procedimientos de actuación deberán ser sencillos y claros y se ejecutarán a la menor sospecha de que pudiera estar produciéndose un incidente.

96. Destacar la importancia de que el usuario informe con exactitud de lo acontecido ya que cualquier dato que se aporte puede beneficiar la investigación.

97. En algunos casos incluso la detección puede venir de entidades externas que han percibido alguna actividad anómala originada en nuestra Organización. Para ello se debe habilitar y publicar una dirección de contacto por la que recibir dicha información.

98. Evidentemente debemos intentar en la medida de lo posible que se produzca esta situación porque es indicativa de que el incidente se está propagando fuera de nuestro perímetro (dominio administrativo) y por tanto perjudicando a terceros. Se deben definir y establecer los mecanismos necesarios para que otros organismos puedan informar a la Organización de la aparición de incidentes que puedan afectarle.

99. Entendemos por identificación la tarea consistente en evaluar la información proporcionada sobre un posible incidente para confirmar su existencia. La realización de un rápido análisis nos permita tener una primera sensación de la naturaleza y amplitud del incidente y así comenzar a notificar a las personas que corresponda y tomar las primeras medidas de contención.

100. La fase de identificación requiere en algunos casos de un alto grado de capacitación y experiencia y por ello suele ser necesario la intervención de diferentes miembros del ERI e incluso la verificación de parte de la evidencias con fuentes externas.

101. Se recomienda buscar un compañero que pueda ayudar en la gestión del incidente aunque sea únicamente para documentar las acciones realizadas.

102. Si se decide avanzar en el ciclo de vida del incidente, este es el momento de comenzar la cadena de la custodia de las evidencias recogidas que garantice su preservación e integridad hasta que se considere necesario.

103. Como conclusión debemos considerar que no sólo es importante disponer de mayores y mejores mecanismos de detección automáticos sino también de procedimientos de respuesta y medios de comunicación para la notificación por parte de los miembros de la Organización. Tras recibir la notificación e información asociada, los miembros del ERI deben realizar con calidad y eficiencia la identificación que permita seguir o no adelante con el ciclo de vida del incidente.

7.3. NOTIFICACIÓN

104. Una vez detectado e identificado el incidente y antes de llevar a cabo cualquier medida de contención o reacción que implique la manipulación de los sistema implicados, resulta imprescindible poner en conocimiento el incidente a las personas administrativas y técnicas en la Organización que sean responsables de los activos implicados, como por ejemplo la Autoridad Operativa del Sistema de las TIC (AOSTIC).

105. Se elegirá un interlocutor dentro del ERI para ejercer estas funciones de notificación y seguimiento. Hay que pensar que se deberá ir informando de manera periódica según sea necesario durante la evolución del incidente.

106. En algunos casos que revistan cierta gravedad será necesario ejercer una función de escalado convenientemente procedimentado de manera que una de las personas responsables pueda, siempre que sea necesario, tomar decisiones en función de la información proporcionada por el ERI.

107. Incluso en determinadas circunstancias presumiblemente delictivas, según el marco legal en aplicación, deberá notificarse a entidades externas como por ejemplo las fuerzas policiales. En función del tipo de incidente tomarán un papel más o menos activo en el

proceso, aunque habitualmente nos requerirán un trato cuidadoso de las evidencias recogidas y una comunicación fluida sobre su evolución.

108. Si existe la posibilidad de que hayan sido o puedan verse afectadas determinadas Organizaciones externas, el ERI podrá también notificarlas para que estén alertadas y se les pueda hacer participes de algunas de las investigaciones.

109. La persona responsable de la comunicación del ERI será la única autorizada para diseminar información sobre los incidentes y será cuidadosa en dar sólo la mínima información necesaria para que cada persona pueda realizar su trabajo y evitará dar detalles técnicos innecesarios para evitar la fuga de información sensible.

7.4. CONTENCIÓN

110. Tras la valoración sobre su naturaleza y alcance realizada en la fase de identificación, el principal propósito de la fase de contención es limitar en la medida de lo posible la extensión del incidente.

111. La Organización debería disponer de procedimientos de contención detallados para los diversos tipos de incidente (denegación de servicio, código malicioso, acceso no autorizado, etc.). Las medidas de contención deben ser lo más específicas y eficientes posible, de manera que su aplicación no afecte la operación del resto de sistemas. Ver ejemplos en Anexo E. Guías de Actuación.

112. Para los casos no contemplados, se deberá evaluar la conveniencia de desconectar, deshabilitar o impedir el acceso a determinados recursos o servicios del Sistema, recabando de la Autoridad Operativa del Sistema de las TIC (AOSTIC) su decisión sobre el asunto tras el asesoramiento del ERI.

113. El ERI o el SIAU bajo las indicaciones del primero, puede solicitar a los usuarios o administradores la realización de determinadas tareas de contención en sus Sistemas.

114. Siempre será deseable realizar tareas de contención que sean lo más pasivas posible respecto de los sistemas afectados, por ejemplo un filtrado del tráfico de red.

115. La fase de contención suele conllevar la recogida y preservación de evidencias de los sistemas de información tales como copias del disco duro, recolección de trazas de registro (logs), etc.

116. Se recomienda encarecidamente documentar cualquier tipo de medida de contención aplicada, de manera que esta pueda deshabilitarse tan pronto deje de ser necesaria.

7.5. ANÁLISIS E INVESTIGACIÓN

117. Esta fase es el núcleo duro del ciclo de vida del incidente donde intentaremos obtener la información suficiente como para responder gran parte de las incógnitas del incidente que nos debe permitir afrontar su resolución.

118. Con las evidencias iniciales, el ERI podrá solicitar reiteradamente nueva información a las entidades que puedan aportar nuevas evidencias o correlar las existentes con sus fuentes de información. Se deberá valorar especialmente las evidencias que vengan apoyadas por mecanismos de integridad y además incluyan información de marca horaria (timestamp) sincronizadas con una fuente fiable.

119. Contribuye de manera sustancial al análisis, el conocimiento de los parámetros y configuración del Sistema afectado, así como las medidas de seguridad implantadas en el Sistema. Destaca el contenido de los archivos de registro de eventos (log) local o bien remotos si existe un punto de recogida centralizado, estos últimos agilizan el análisis de los mismos y suele proporcionar una garantía de que estos no han sido modificados.

120. Se debe guardar una descripción detallada de cada evidencia recogida, incluyendo:

    - Datos de identificación.
    - Personal que ha recogido la prueba.
    - Fecha y hora de recogida.
    - Lugar de almacenamiento de la prueba.

121. Deberá evitarse la manipulación directa de los soportes de información y de los sistemas, trabajando siempre que sea posible sobre las copias de las evidencias para evitar la pérdida irreversible de los datos iniciales.

122. En la recogida de evidencias, son de especial importancia las de tipo volátil, por ejemplo el estado de las conexiones de red, procesos, sesiones abiertas, fichero abiertos, contenido de la memoria dinámica, etc.

123. Se deberá documentar, con los medios disponibles (fotografía, impresora, vídeo, etc.), todas las acciones que se realicen sobre los Sistemas:

    - Se debe almacenar de forma segura y restringir el acceso únicamente al personal autorizado, a todas las pruebas recogidas durante la fase de análisis.
    - En caso de que el incidente pueda implicar procedimientos legales, tanto civiles como penales, las pruebas presentadas serán recogidas y tratadas conforme a las reglas establecidas por la legislación vigente.

124. Se hace necesaria la utilización un mecanismo seguro de comunicación y una herramienta que facilite dicha comunicación y sea el cuaderno de bitácora que nos permita realizar un seguimiento de todas las actividades. En el Anexo D se describen las herramientas RTIR y SIRIOS-OTRS que pueden cumplir dicha función.

125. Durante esta fase suele ser necesaria la incorporación al equipo de trabajo del incidente de miembros de la Organización que puedan ofrecer un conocimiento de alto nivel asociado a su área de conocimiento TIC. Por su nivel de conocimiento directo, se deberá contar necesariamente con los administradores de red, sistemas o seguridad de los sistemas implicados.

126. En algunos casos puede ser de utilidad reconstruir el incidente sobre unos sistemas de prueba lo más similares posibles a los involucrados en el incidente. Esto nos puede permitir demostrar que el incidente es reproducible siguiendo la combinación de las secuencias identificadas en los diversos análisis.

127. Se deberá estudiar en detalle todas las evidencias recogidas y tras múltiples fases de análisis, siguiendo las normas descritas, podremos llegar a resolver todas las cuestiones que nos permitan abordar su resolución y la recuperación de los Sistemas al estado anterior a la materialización del incidente.

7.6. SOLUCIÓN Y RECUPERACIÓN

128. El objetivo de esta fase es el restablecimiento de la información, servicios y recursos afectados. Es decir, se realizarán las acciones necesarias para que el Sistema recobre sus capacidades y pueda prestar servicio con normalidad.

129. En esta fase se deben dar todos los pasos necesarios para que el incidente quede resuelto o cerrado. Suele estar a cargo de los administradores del Sistema con el apoyo de la información obtenida por el ERI en las etapas anteriores.

130. Un incidente se considera resuelto cuando se ha restablecido toda la información y los recursos TIC afectados y por lo tanto el Sistema opera normalmente y se tiene un conocimiento razonable de:

    - ¿Qué ha pasado?
    - ¿Por qué ha pasado?
    - Las pérdidas ocasionadas.
    - Se conoce qué o quiénes han sido los causantes.

131. Un incidente cerrado es aquel incidente en el que no se ha podido conocer alguno de los puntos anteriores y en el que a juicio del ERI, se han agotado todas las posibilidades de análisis e investigación para su resolución.

132. La AOSTIC deberá estar informada de las actividades que se estén realizando y del momento en el que el Sistema se encuentre nuevamente operativo y el SIAU se encargará de comunicar a los usuarios, por indicación de los administradores, el momento en que los servicios o recursos afectados vuelvan a estar disponibles.

133. La resolución del incidente en ocasiones implica la limpieza o reinstalación de los sistemas que se han visto afectados. Además se suele iniciar la búsqueda de las medidas de protección a implantar para que se tenga una certeza razonable de que no volverá a ocurrir. Estas deben ser anotadas para que sean documentadas en la fase final del ciclo de vida del incidente.

134. La recuperación consiste en reestablecer la operación del Sistema que en algunos casos hará necesaria la recuperación de la información de copias de respaldo (backup). La AOSTIC deberá validar la recuperación de los sistemas. El ERI puede realizar un análisis de vulnerabilidades del sistema que ofrezca garantías de su seguridad.

135. Una vez resuelto el incidente y recuperados los sistemas, estos se deberían someter a una monitorización exhaustiva para identificar posibles problemas que hayan escapado al análisis o bien propiamente identificar que el incidente se vuelve a reproducir en su totalidad.

136. En caso de detectarse actividad que pudiera ser ilícita, se debe contactar con las Fuerzas y Cuerpos de Seguridad del Estado.

7.7. REFLEXIÓN Y MEJORA

137. Esta es una de las fases habitualmente más descuidadas y que pueden aportar información más útil tanto a la Gestión de la Seguridad TIC de la Organización como a las propias Capacidades de Respuesta.

138. Esta fase consiste en la elaboración de un informe y presentación de las conclusiones obtenidas de todas las fases del proceso de gestión de un incidente. Este debe ser revisado por el personal que ha participado en dicho incidente.

139. En cualquier caso deberá quedar constancia de toda la información de interés sobre el incidente, así como documentar los errores cometidos y las propuestas de mejora necesarias para evitar incidentes futuros en los Sistemas de la Organización. Además se debe identificar qué fases de la respuesta a incidentes podrían mejorarse de cara al futuro.

140. Es de especial importancia contar con una base de datos de conocimiento dentro de la Organización que contenga la información relativa a los incidentes, con el objetivo de agilizar la gestión en caso de que se vuelva a producir.

141. Las medidas de mejora deben ser aprobadas, difundidas e incorporadas a los procedimientos TIC de manera que se evite la repetición futura del mismo incidente.

142. Tanto el informe como todas las evidencias recogidas deberán archivarse y mantenerse bajo control para que tan solo puedan ser accedidas por personal autorizado. Algunas evidencias deben ser destruidas si legalmente su período de retención máxima así lo requiere.

ANEXO A. FORMULARIO DE ALTA DE INCIDENTE

1. INFORMACION GENERAL DE CONTACTO	
1.1. Nombre:	1.2. Despacho:
1.3. Teléfono:	1.4. Departamento:
1.5. Información adicional:	1.6. Fecha de comunicación:

2. INFORMACION DEL SISTEMA	
2.1. Tipo:	2.2. Número de serie:
2.3. Configuración hardware:	
2.4. Configuración software:	
2.5. En caso de tratarse de una estación de trabajo.	
2.5.1. Sistema Operativo, versión y nivel de parcheado:	
2.5.2. Información de red:	
2.5.3. Información de autenticación:	
2.5.4. Información de autorización (privilegios):	
2.5.5. Programas instalados:	

3. INFORMACION DEL INCIDENTE			
3.1 Hora de inicio de entrada al Sistema		3.2 Fecha y duración del incidente	
3.3 ¿Cómo se descubrió el incidente?			
3.4 Naturaleza de la información del dispositivo involucrado			
3.5 Importancia del incidente: **Leve - Media - Grave**	3.6 Clasificación de la información involucrada: **Desconocido - SinClas - Dif. Lim. - Confidencial - Reservado - Secreto**		
3.7 Grado de compromiso de seguridad de la información: Improbable - Probable - Seguro			
3.8 La incidencia impide el correcto flujo documental interno de la Organización:		SÍ	NO
3.9 La incidencia impide el correcto flujo documental externo de la Organización:		SÍ	NO
3.10 Descripción del incidente:			
3.11 Categoría del incidente de seguridad (elegir entre):			
Intento de acceso no autorizado al Sistema		Interrupción de funcionamiento no previsto o denegación de servicio.	
Intercepción, modificación, introducción, corrupción, destrucción o divulgación de información no autorizada.		Abuso de privilegios de acceso	
Cambios en las características y configuración del software no autorizados, conocidos o consentidos por el usuario.		Cambios en las características y configuración del hardware no autorizados, conocidos o consentidos por el usuario.	
Prueba, sondeo, broma o suplantación de identidad.		Utilización no autorizada de un equipo/máquina/sistema.	
Ataque procedente de la red.		Suplantación de dirección IP.	
Vulnerabilidad del producto.		Errores de configuración.	
Mal uso de los recursos de la máquina.		Virus (software malicioso).	
Irregularidades en el correo electrónico.		Emanaciones Electromagnéticas.	
Divulgación de datos sensibles del sistema por ingeniería social		Errores de mantenimiento	
Otros			
3.12 Origen / Fuente / Causa del incidente:			
3.13 Valoración personal sobre la intencionalidad del incidente:			
3.14 Medidas tomadas después del incidente:			
3.15 Estado de resolución del incidente:			

ANEXO B. LISTADO DE ORGANISMOS Y EQUIPOS

Internacionales

- Forum of Incident Response Teams (FIRST)
  http://www.first.org/
- Computer Emergency Response Team Coordination Center (CERT-CC)
  http://www.cert.org/

Europeos

- European Network and Information Security Agency (ENISA)
  http://www.enisa.europa.eu/
- Task Force of Computer Incident Response Teams (TF-CSIRT)
  http://www.terena.nl/activities/tf-csirt/

Nacionales

- Equipo de Respuesta a Incidentes del Centro Criptológico Nacional (CCN-CERT)
  http://www.ccn-cert.cni.es
- Equipo de Respuesta a Incidentes de la Red Académica Española - IRIS-CERT (RedIRIS)
  http://www.rediris.es/cert/
- Equipo de Respuesta a Incidentes de la Universidad Politécnica de Cataluña – esCERT (UPC)
  http://escert.upc.edu/
- Grupo de Delitos Telemáticos (GDT) de la Guardia Civil
  https://www.gdt.guardiacivil.es/
- Brigada de Investigación Tecnología (BIT) de la Policía Nacional
  http://www.policia.es/bit/
- Unitat de Delic*tes en Tecnologies de la Informació (UD*TI) de los Mossos d'Esquadra
  http://www.gencat.net/mossos/

ANEXO C. SERVICIOS DE UN CERT

SERVICIOS REACTIVOS	
Alertas y Avisos	Consisten en la diseminación de información descriptiva de ataques o intrusiones, de vulnerabilidades o amenazas, virus informáticos o falsas alarmas, contenidos ilícitos o dañinos y recomendaciones para enfrentarse a los mismos, consejos y guías de protección, o bien acciones de recuperación para los sistemas afectados.
Gestión de Incidentes	Recepción, análisis, clasificación, categorización y priorización de las peticiones e informes recibidos para luego proceder a su gestión según la misión y función del centro. Servicios de asistencia técnica y coordinación de la recuperación de los sistemas, tales como los de apoyo a servicios policiales o judiciales encargados de la investigación del incidente.
Gestión de Vulnerabilidades	Servicios de diagnóstico y auditoría de los sistemas informáticos de los usuarios, apoyo técnico mediante el desarrollo de soluciones, parches de SW o de configuración que resuelvan las vulnerabilidades encontradas, y servicios de coordinación de las actividades de mitigación del riesgo mediante la notificación e intercambio de información con entidades nacionales e internacionales.
SERVICIOS PROACTIVOS	
Anuncios y Avisos (a usuarios adscritos)	Información sobre estadísticas de incidentes, vulnerabilidades e intrusiones. Acceso a bases documentales de guías y consejos
Auditorías o evaluaciones de seguridad	Revisión de infraestructuras y configuraciones, repaso de buenas prácticas y procedimientos, detección de vulnerabilidades y posibles huecos o fallos de seguridad y pruebas de penetración en los sistemas.
Configuración y mantenimiento de elementos de seguridad	Asistencia directa para la configuración, instalación y mantenimiento de todo tipo de herramientas de seguridad.
Desarrollo de herramientas de seguridad	Desarrollo de parches, filtros o plug-ins que mejoren las capacidades de seguridad
Detección de intrusiones	Instalación de sensores en dispositivos, sistemas y aplicaciones distribuidos por toda la red de usuarios adscritos y el análisis en detalle de la información recopilada.
Diseminación de información	Orientados a proporcionar a los usuarios del centro información útil y actualizada de forma amigable sobre alertas, guías metodológicas, soluciones disponibles, estadísticas, referencias documentales, etc.
Certificación de calidad	Normas y procedimientos para que las entidades públicas puedan asegurar que su actividad en internet ofrece garantías para los

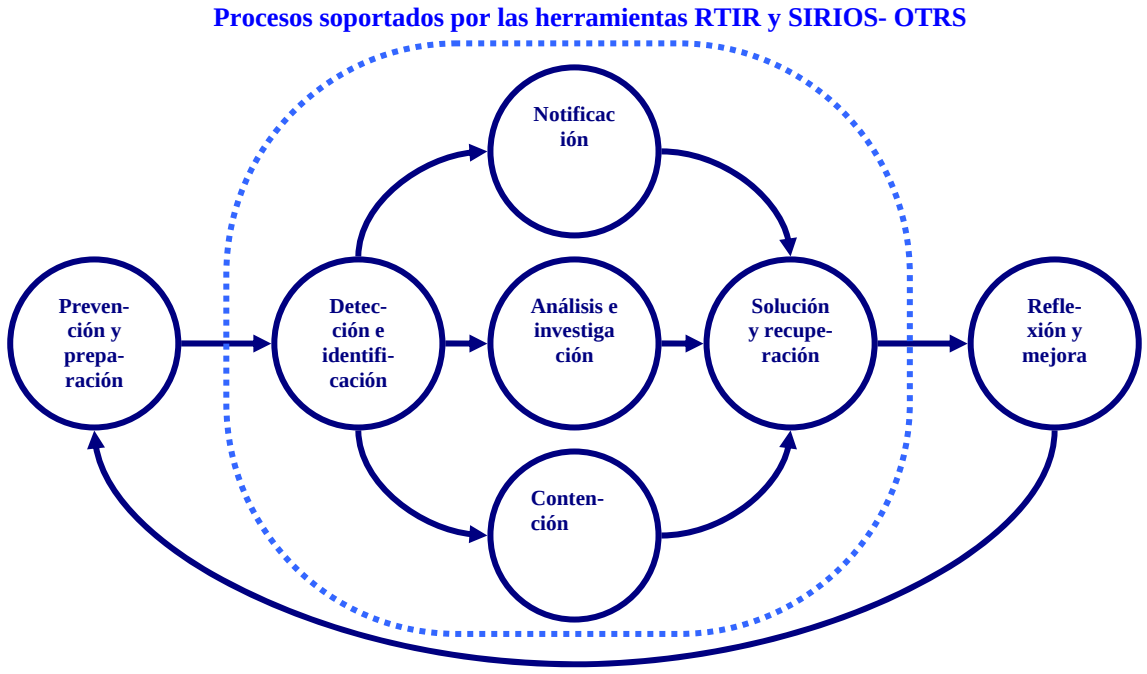
	usuarios finales.

SERVICIOS DE VALOR AÑADIDO	
Análisis código dañino	Análisis de virus informáticos, caballos de troya, gusanos y otras herramientas de SW basadas en técnicas de ingeniería social usadas para provocar daños en sistemas, caídas de servicio en redes telemáticas o difusión masiva de contenidos no solicitados. Se pueden activar en: La respuesta de las preguntas depositadas en buzones de consultas, La moderación y respuesta a las preguntas planteadas en los foros.
Análisis de riesgos	Estudios y evaluaciones de riesgos y amenazas de una instalación o red concreta.
Consultoría de seguridad informática	Servicios tales como el desarrollo e implantación de planes de seguridad o de recuperación ante desastres o graves perturbaciones de seguridad. Identificación de requisitos y apoyo en licitaciones y concursos para la adquisición o implantación de dispositivos y sistemas.
Mentalización y formación	Concienciar a los usuarios de los riesgos y amenazas a la seguridad asociados al acceso de redes telemáticas y en particular a internet, y al uso del correo electrónico, así como en la divulgación y entrenamiento en las soluciones disponibles para protegerse eficazmente de esas amenazas. • Cursos STIC. • Seminarios / workshops. • Foros de discusión.
Evaluación y certificación de productos	COMMON CRITERIA TEMPEST CIFRA.

ANEXO D. HERRAMIENTAS DE GESTIÓN DE INCIDENTES

D.1. INTRODUCCIÓN

La gestión de un incidente conlleva distintas fases y para su correcta gestión es interesante disponer una herramienta que permita centralizar toda la información relacionada con el incidente. De los principios para la gestión de incidentes seguidos por CCN-CERT y descritos en esta guía, las herramientas a continuación descritas cubren el siguiente flujo de procesos:



De este modo, durante la gestión de un incidente, toda la información que le concierne fluye entre los procesos centrales de la gestión de incidentes (procesos englobados dentro de la línea de puntos) y es interesante disponer de una herramienta que permita a los distintos actores del ERI encargados de la gestión de un incidente intercambiarse la información. Asimismo, toda la información concerniente a pasados incidentes debe quedar registrada en algún tipo de registro o base de datos.

D.2. RTIR

"*Request Tracker for Incident Response*" (RTIR) es una de las herramientas de gestión de incidentes más utilizada entre los Equipos de Respuesta a Incidentes de todo el mundo. Está basado en software de código abierto y libre distribución cuyo origen se debe al proyecto lanzado por JANET-CSIRT, el ERI de la red académica británica, para la creación de una herramienta de atención de incidentes. La implementación de dicho proyecto fue realizada por BestPractical.

Este software nació fruto de la adaptación y personalización del producto "*Request Tracker*" (RT), que es un **sistema de seguimiento de tareas y acciones mediante tiques, trasladando sobre esta aplicación el enfoque necesario para la gestión de incidentes de seguridad**.

La gran ventaja de este sistema frente a otras aplicaciones similares radica en la implementación que hace RTIR sobre la definición de un incidente de seguridad. Para ello define un incidente como una entidad superior que contiene los diferentes sucesos o eventos que pueden ocurrir a lo largo de la vida del incidente, como las quejas o evidencias recibidas sobre un problema de seguridad, las investigaciones lanzadas para la resolución o la puesta en conocimiento entre las entidades implicadas del problema, o las acciones que se pueden tomar en los dispositivos de red para paliar los efectos del incidente.

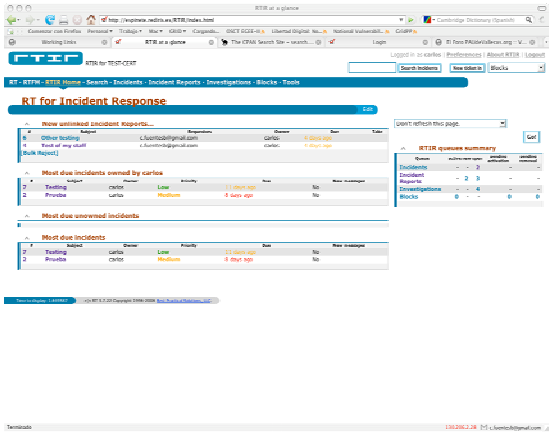
Para implementar la anterior definición de incidente de seguridad, RTIR incorpora por defecto cuatro colas, además la herramienta define un flujo de trabajo (*workflow*) para los miembros del ERI:

- Informe de incidente (*incident report*): recibe las notificaciones de nuevas quejas o evidencias y establece su fecha límite para ser gestionado en función de las reglas SLA definidas.

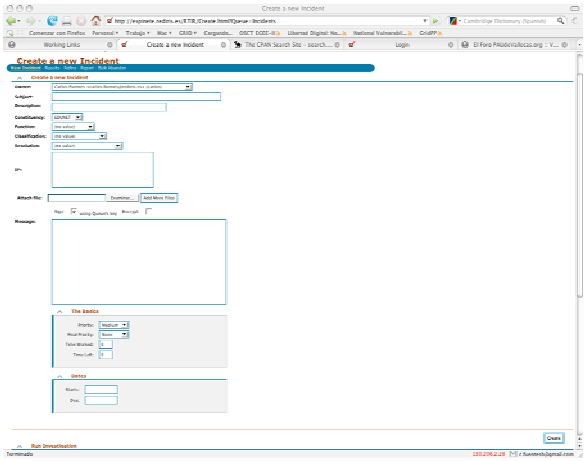
- Investigación (*investigation*): solicitud a terceros para iniciar la búsqueda de información adicional y correlación o investigación de los datos ya recogidos, estableciendo también una fecha limite para su gestión en función de las reglas SLA definidas

- Filtrado (*blocks*): solicitud y seguimiento de los filtros o mecanismos de contención aplicados durante el incidente.

- Incidente (*incident*): cuando el ERI verifica que un informe de incidente es válido crea un incidente o lo relaciona con otro incidente ya existente en el sistema. La herramienta incorpora de forma automática la información relevante del informe de incidente.



Vista general de la herramienta



Creación de un nuevo tique de incidente

La interacción del sistema con los usuarios finales se hace principalmente a través de correo electrónico, también es posible hacerlo a través del interfaz web, aunque en general ningún ERI recomienda usar esta opción, para evitar posibles riesgos de seguridad. Para la gestión de los incidentes de seguridad la aplicación define, por defecto, el rol de gestor de incidentes, el cual conlleva los permisos necesarios para llevar a cabo su tarea, y que le permiten acceder a toda la información que necesita. Este rol también puede ser modificado dependiendo del flujo de trabajo de cada ERI.

El sistema también permite definir otros roles que puedan estar definidos en el ERI, y que vaya a interactuar con la herramienta.

El flujo de trabajo básico que la herramienta lleva implícito se podría explicar en los siguientes pasos:

- Recepción de una o varias notificaciones de un incidente que se añaden de manera automática o manual al sistema.
- Creación de un incidente o enlace a uno existente para almacenar todas las quejas o evidencias recibidas y todas las acciones tomadas para llevar a cabo la resolución del problema.
- Solicitudes de investigación y/o filtrado a terceros internos o externos a la organización, para realizar las intervenciones necesarios para la resolución del incidente.
- Conclusión de todas las actividades de investigación y filtrados iniciadas con anterioridad.
- Documentación y conclusión del incidente donde se aten todos los cabos sueltos y se cuide especialmente las lecciones aprendidas del incidente, pudiéndose crear un ticket de la base de conocimiento, RTFM, que permita futuras consultas.
- Notificación a todos los implicados de la resolución del incidente.

Para facilitar la tarea de gestión de los incidentes de seguridad, la herramienta permite la realización de búsquedas con un solo clic de información adicional sobre piezas de información relevantes como las direcciones IP, nombres de dominio, etc. De manera adicional se permite mejorar sus funcionalidades mediante la creación de acciones automatizadas (*scripts*) que nos permita reducir el tiempo necesario para las tareas habituales, por ejemplo iniciar una nueva investigación dirigida a todos los administradores responsables de todas y cada una de las direcciones IP descritas en un incidente.

Desde Enero de 2004, existe un grupo de trabajo dentro del TF-CSIRT/TERENA, que tiene por objetivo mejorar la herramienta, tanto a nivel de definición de nuevas funcionalidades, como de hacerla mas adaptable para los diferentes ERIs. Por ello, en Octubre de 2005 se inició el proyecto para la creación de la versión 2 de RTIR, que fue concluido en Enero de 2008.

Esta segunda versión del producto trae consigo nuevas características, que no solo amplían las funcionalidades de RTIR, sino también lo hacen mucho más adaptable. Algunas de ellas son:

- Integración con RT, de forma que se hacen accesibles todas las funcionalidades que RT posee.
- Nueva interfaz gráfica
- Integración de GnuPG, de forma que la herramienta pueda cifrar/descifrar y firmar/verificar correos electrónicos.
- Integración con la base de conocimiento RTFM, con lo que, entre otras cosas, se permite la gestión de vulnerabilidades y su asociación con incidentes de seguridad gestionados por RTIR.
- Gestión de múltiples ámbitos de actuación de un ERI, teniéndolos perfectamente diferenciados y desasociados, de forma que los gestores de incidentes de uno de los ámbitos de actuación no vean los incidentes del otro ámbito y viceversa.
- Asociación con el responsable del incidente de forma automática en función de la IP, que origino el ataque.
- Sistema de caducidad de incidentes, que permite eliminar de la base de datos de trabajo aquellos incidentes de más de una determinada edad, manteniendo un resumen del incidente eliminado en la base de conocimiento.
- Sistema de bloqueos de los incidentes.
- Cola de bloqueos configurable. Para algunos ERIs esta cola no tiene sentido, ya que no poseen infraestructura de red sobre la que son responsables. El nuevo RTIR permite eliminar su uso.
- Herramienta de informes.

D.3. SIRIOS

La aplicación SIRIOS[1] (System for Incident Response in Operational Security) ha sido desarrollada sobre la aplicación OTRS[2] (Open Ticket Request System) por el CERT-Bund[3], Equipo de Respuesta ante Incidentes Oficial de la R.F.A.

El objeto del sistema OTRS (y por extensión de SIRIOS, aunque este último más centrado en la gestión de los distintos procesos de un CERT) es ofrecer un sistema para la gestión del proceso de soporte. La gestión del soporte recoge toda la información acerca de una solicitud de soporte realizada por un "cliente" del servicio de soporte en forma de un tique que es empleado por los "agentes" del servicio de soporte para resolver la solicitud realizada.

Por lo tanto, los tiques constituyen en SIRIOS – OTRS el reflejo en el sistema de una solicitud realizada por un cliente y que puede llegar por medio de un correo electrónico y directamente se ve reflejada en un ticket en el sistema (nuevo o uno ya existente) o por teléfono y en este caso la información tiene que ser incorporada a un tique (nuevo o uno ya existente) por un agente. Los tiques se almacenan de manera organizada en el sistema en lo que se denominan **colas**. Asimismo, SIRIOS emplea una agrupación de ciertas colas en lo que se denominan "workflows".

Por lo tanto, la comunidad generará solicitudes cuando detecte un incidente y necesite que el ERI realice un seguimiento o asistencia en la resolución del mismo. Estas solicitudes generan un tique en el sistema SIRIOS – OTRS que recogerá toda la información relacionada con el incidente, incluyendo toda la información que intercambie el ERI y el "cliente" que notificó el incidente.

Estos tiques se encontrarán en una u otra cola dependiendo del estado de progresión en la atención al incidente. En este sentido la finalidad de cada una de las colas es la siguiente:

- Cola "*Hotline*": corresponde a la cola donde se reciben todas las notificaciones inicialmente y donde se realiza una atención y filtrado de primer nivel. Todas aquellas notificaciones que potencialmente sean identificables con un incidente serán progresadas a la cola "Coordination".

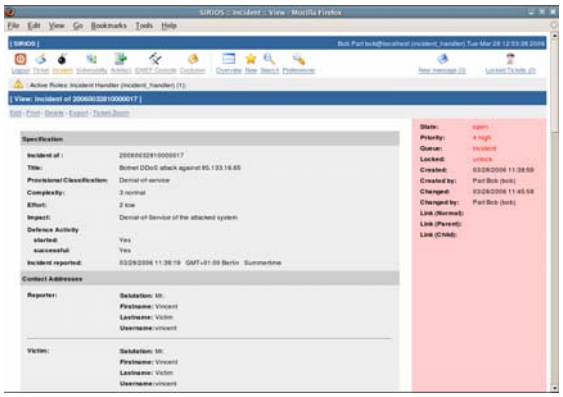
- Cola "*Coordination*": se trata de la cola donde únicamente llegarán las notificaciones de incidentes reales. En este punto, el agente que gestione la cola deberá identificar que experto es el más adecuado para la gestión de la incidencia por el criterio que él decida, por ejemplo temática del incidente o bien por la identidad especialmente crítica del "cliente". Por lo tanto, asignará la propiedad del tique a un agente concreto y progresará el tique a la cola "Incident".

[1] http://sirios.org
[2] http://otrs.org
[3] http://www.bsi.bund.de/english/index.htm

- Cola "*Incident*": una vez se ha asignado el tique a aquel más adecuado para dar la asistencia el agente encargado de gestionar el incidente realizará las investigaciones, averiguaciones apropiadas, dará las indicaciones necesarias para contener el incidente y para recuperar los sistemas afectados y todas las acciones las reflejará en el tique asignado a la incidencia. Asimismo, elaborará el registro de la incidencia que quedará adjuntado al tique.

- Cola "*Junk*": cuando los agentes consideren que un tique ha de ser eliminado completamente del sistema. Un ejemplo de situación donde podría resultar necesario sería si el agente de Hotline crease un tique telefónico porque un cliente ha contactado con el ERI pero posteriormente se recibe también se recibe la notificación por correo porque el cliente ha cumplimentado un formulario de notificación del incidente. El agente tendría la posibilidad de "mezclar" los dos tiques o bien borrar uno de ellos enviándolo a la cola JUNK.

Creación de un nuevo tique de incidente



Detalle de un tique de incidente

En el proceso de gestión de incidentes en SIRIOS intervienen los siguientes **actores**:

- **Rol MIEMBRO DE LA COMUNIDAD**: corresponde al rol del primer nivel de detección y notificación de incidentes, aunque también es posible que el propio ERI detecte situaciones que deban ser notificadas como incidentes.

- **Rol HELPDESK**: este rol será realizado por personal que pertenece a la estructura del ERI y que realizará el filtrado de primer nivel.

- **Rol COORDINATION**: este rol será realizado por personal que pertenece a la estructura del ERI y que realizará las funciones de análisis de 2º nivel, priorización y asignación de los incidentes para su gestión a los expertos del ERI.

- **Rol INCIDENT_HANDLER**: este rol será realizado por los expertos del ERI que darán la asistencia a la comunidad para puedan gestionar internamente el incidente, y en caso que el coordinador lo indique podrán realizar la actuación directa en colaboración con la comunidad.

- **Rol CARGOS SUPERIORES**: este rol será realizado por personal del ERI que se encuentra involucrado en la gestión del equipo y en este caso se encargarán de analizar el funcionamiento del proceso de gestión de incidentes para evaluar el rendimiento del servicio y determinar las necesidades futuras del equipo.

Además SIRIOS incluye las siguientes funcionalidades:

- Gestión de artefactos: inclusión de ficheros y evidencias al sistema
- Relacionar un incidente con uno o varios artefactos
- Gestión de vulnerabilidades: creación de vulnerabilidades (formato EISPP) e importación directamente de una fuente de datos (NVD, OSVDB, etc.)
- Relacionar un incidente con una o varias vulnerabilidades
- Visor de alertas generadas por un sistema de detección de intrusos en formato IDMEF

ANEXO E. GUIAS DE ACTUACIÓN

E.1. RESPUESTA A INCIDENTES: ESCENARIO GENERAL

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
0. Durante todo el proceso **Documentar todo**: incluyendo acciones realizadas, evidencia recolectada, conversaciones y datos suministrados por usuarios, administradores y otras personas relacionadas con el incidente.	
1. Identificación del incidente	
• Buscar un compañero que pueda ayudar en la gestión del incidente aunque sea únicamente para documentar las acciones realizadas.	
• Analizar la evidencia inicial para confirmar si realmente se trata de un incidente.	
2. Notificación	
• Notificar a los responsables dentro de la organización. Sólo dando la mínima información para que cada persona pueda realizar su trabajo y evitando dar detalles técnicos innecesarios para evitar la fuga de información sensible.	
• Notificar al CCN-CERT para solicitar ayuda especializada en la gestión del incidente.	
3. Contención	
• Tomar las acciones necesarias según el tipo de incidente para mitigar el ataque, modificando lo menos posible los sistemas afectados, con el fin de preservar el máximo de evidencias del incidente que permitan investigarlo y resolverlo del mejor modo, consiguiendo a la vez la mayor cantidad de información posible.	
4. Análisis e Investigación	
• Obtener todas las evidencias necesarias para afrontar la resolución del incidente.	
• Guardar descripción detallada de cada evidencia recogida.	
• Analizar evidencias buscando origen, técnicas empleadas, acciones	

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
realizadas, motivaciones, etc.	
5. Solución y Recuperación	
• Resolver el incidente, actuando ya sea sobre el origen del ataque o sobre las debilidades que lo hayan hecho posible.	
• Pasado un tiempo prudencial, confirmar que la situación ha vuelto a la normalidad antes de dar por resuelto el incidente.	
• En caso de detectarse actividad que pudiera ser ilícita contactar con Fuerzas y Cuerpos de Seguridad del Estado.	
6. Reflexión y Mejora	
• Documentar el proceso de respuesta a incidentes junto con un resumen ejecutivo.	
• Documentar los errores cometidos durante la gestión del incidente y las posibles acciones a tomar para mejorar la prevención y gestión de incidentes en el futuro.	

E.2. RESPUESTA A INCIDENTES: CASOS DE INTRUSIÓN

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
0. Durante todo el proceso **Documentar todo**: incluyendo acciones realizadas, evidencia recolectada, conversaciones y datos suministrados por usuarios, administradores y otras personas relacionadas con el incidente.	
1. Identificación	
• Buscar un compañero que pueda ayudar en la gestión del incidente aunque sea únicamente para documentar las acciones realizadas	
• Analizar evidencia inicial para confirmar si realmente se trata de un incidente:	
i. Logs anómalos en los sistemas	
ii. Cambios en el comportamiento de las aplicaciones	
iii. Nuevas aplicaciones en el sistema	
iv. Tráfico anómalo (entrada/salida) en sistemas afectados	
2. Notificación	
• Notificar a los responsables dentro de la organización. Sólo dando la mínima información para que cada persona pueda realizar su trabajo y evitando dar detalles técnicos innecesarios para evitar la fuga de información sensible.	
• Notificar al CCN-CERT para solicitar ayuda especializada en la gestión del incidente	
3. Contención	
• Mitigar el ataque modificando lo menos posible a los sistemas afectados, con el fin de preservar el máximo de evidencias del incidente que permitan investigarlo y resolverlo del mejor modo, consiguiendo la mayor cantidad de información posible acerca de los orígenes, técnicas empleadas, acciones realizadas, motivaciones, etc.	
i. Si existe un servidor secundario (de backup): parchear y mover el servicio al servidor secundario → Si no se parchea correctamente existe el riesgo de que también comprometan el servidor secundario.	
ii. Bloquear acceso a las partes modificadas (casos de *defacement*) o al contenido ilícito (distribución malware, warez, etc.)	
iii. Bloquear el acceso al servidor o al componente vulnerable.	

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
iv. Apagar servidor. Esta acción solo se debería realizar en sistemas que no tengan una función crítica para las operaciones de negocio.	
4. Análisis e Investigación	
• Determinar si por la criticidad de los sistemas afectados es posible realizar una adquisición de datos para preservar evidencias del incidente. Para ello se realizará una copia (imagen) del disco.	
• Obtener evidencia de forma que no se modifique el sistema atacado:	
i. Revisar logs de los dispositivos perimetrales (IDS, Firewall, etc.)	
iii. Para revisar los logs del sistema afectado acceder a la copia de estos en un centralizador de logs si está disponible	
• Realizar un análisis forense de la imagen del disco para analizar en detalle la actividad del atacante en el sistema.	
• Comprobar que el atacante no ha podido comprometer otros sistemas	
5. Solución y Recuperación	
• Eliminación de componentes del ataque que puedan haber quedado en el sistema como código malicioso, material no apropiado, u otros cambios realizados al sistema.	
• Si existen indicios de que el sistema pueda estar comprometido, reconstruir el sistema desde la última copia de seguridad fiable o en su defecto reinstalar el sistema.	
• Corregir las vulnerabilidades antes de poner el sistema de nuevo en producción, de forma que el incidente no pueda repetirse.	
• Verificar que todos los datos, aplicaciones y sistemas afectados por el incidente vuelven a funcionar de la forma habitual.	
• Confirmar pasado un tiempo prudencial que la situación ha vuelto a la normalidad antes de dar por resuelto el incidente.	
• En caso de detectarse actividad que pudiera ser ilícita contactar con Fuerzas y Cuerpos de seguridad del Estado	
7. Reflexión y Mejora	
• Documentar el proceso de respuesta a incidentes junto con un resumen ejecutivo.	
• Documentar los errores cometidos durante la gestión del incidente y las posibles acciones a tomar para mejorar la prevención y gestión de incidentes en el futuro.	

E.3. RESPUESTA A INCIDENTES: CASOS DE CÓDIGO MALICIOSO

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
0. Durante todo el proceso **Documentar todo**: incluyendo acciones realizadas, evidencia recolectada, conversaciones y datos suministrados por usuarios, administradores y otras personas relacionadas con el incidente.	
1. Identificación	
• Buscar un compañero que pueda ayudar en la gestión del incidente aunque sea únicamente para documentar las acciones realizadas	
• Analizar evidencia inicial para confirmar si realmente se trata de un incidente:	
i. Logs anómalos en los sistemas	
ii. Cambios en el comportamiento de las aplicaciones	
iii. Nuevas aplicaciones en los sistemas	
iv. Tráfico anómalo (entrada/salida) en sistemas afectados	
2. Notificación	
• Notificar a los responsables dentro de la organización. Sólo dando la mínima información para que cada persona pueda realizar su trabajo y evitando dar detalles técnicos innecesarios para evitar la fuga de información sensible.	
• Notificar al CCN-CERT para solicitar ayuda especializada en la gestión del incidente.	
3. Contención	
• Mitigar el ataque modificando lo menos posible a los sistemas afectados, con el fin de preservar el máximo de evidencias del incidente que permitan investigarlo y resolverlo del mejor modo, consiguiendo la mayor cantidad de información posible acerca de los orígenes, técnicas empleadas, acciones realizadas, motivaciones, etc.	
• Evitar la propagación del malware tanto dentro como fuera de nuestras redes:	
i. Bloquear servicios y/o máquinas mediante routers/firewalls. Si resulta necesario, es posible bloquear todo el tráfico en el perímetro o incluso bloquear absolutamente todo el tráfico de red.	

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
ii. Deshabilitar los servicios de red atacados en servidores y estaciones de trabajo.	
iii. En caso de propagarse por e-mail, bloquear los correos con un tema (subject) que identifique al malware. Si resulta necesario, deshabilitar el servicio de correo hasta que se solucione el incidente.	
iv. Actualizar todos los sistemas AntiVirus, Antispam, Antispyware, etc.	
v. Activar sistemas de protección contra intrusos (IPS).	
4. Análisis e Investigación	
• Determinar si por la criticidad de los sistemas afectados es posible realizar una adquisición de datos para preservar evidencias del incidente. En el caso de múltiples sistemas afectados por el malware, se analizará el menos crítico. Para ello se realizará una copia (imagen) del disco.	
• Obtener evidencia de forma que no se modifique el sistema atacado:	
i. Revisar los logs de los dispositivos perimetrales (IDS, Firewall, etc.)	
ii. Para revisar los logs del sistema afectado, acceder a la copia de estos en un centralizador de logs si está disponible	
• Analizar evidencia y contrastar información con las páginas Web de fabricantes antivirus.	
• Analizar los sistemas con varios motores antivirus.	
• Analizar comportamiento de “artefactos” encontrados y analizar con *Virustotal*	
• Identificar todos los sistemas afectados por el malware.	
5. Solución y Recuperación	
• Eliminar componentes del ataque que puedan haber quedado en el sistema como código malicioso, material no apropiado, u otros cambios realizados al sistema.	
• Si existen indicios de que el sistema pueda estar comprometido, reconstruir el sistema desde la última copia de seguridad fiable o en su defecto reinstalar el sistema.	
• Corregir las vulnerabilidades antes de poner el sistema en producción de forma que el incidente no pueda repetirse.	
• Verificar que todos los datos, aplicaciones y sistemas afectados por el incidente vuelven a funcionar en la forma habitual.	
• Confirmar pasado un tiempo prudencial que la situación ha vuelto a la normalidad antes de dar por resuelto el incidente.	

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
• Realizar un análisis forense de la imagen del disco tomada durante la fase de contención para analizar en detalle la actividad del malware en el sistema.	
• En caso de tratarse de un ataque dirigido, contactar con Fuerzas y Cuerpos de seguridad del Estado	
6. Reflexión y Mejora	
• Documentar el proceso de respuesta a incidentes junto con un resumen ejecutivo.	
• Documentar los errores cometidos durante la gestión del incidente y las posibles acciones a tomar para mejorar la prevención y gestión de incidentes en el futuro.	

E.4. RESPUESTA A INCIDENTES: CASOS DE PHISHING

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
0. Durante todo el proceso **Documentar todo**: incluyendo acciones realizadas, evidencia recolectada, conversaciones y datos suministrados por usuarios, administradores y otras personas relacionadas con el incidente.	
1. Identificación	
• Buscar un compañero que pueda ayudar en la gestión del incidente aunque sea únicamente para documentar las acciones realizadas	
• Analizar evidencia para confirmar si realmente se trata de un incidente	
i. Analizar el mensaje usado para propagar el phishing (p.ej. email) buscando signos que indiquen un posible fraude.	
ii. Si se tiene acceso a logs del servidor Web de la organización afectada, buscar "referrers" a los recursos de tipo gráfico (css, imágenes, etc.) ya que es práctica habitual que los sitios de phishing utilicen estas imágenes.	
2. Notificación	
• Notificar a los responsables dentro de la organización. Sólo dando la mínima información para que cada persona pueda realizar su trabajo y evitando dar detalles técnicos innecesarios para evitar la fuga de información sensible.	
• Notificar al CCN-CERT para solicitar ayuda especializada en la gestión del incidente	
3. Contención	
• Reportar la URL a los sitios antiphishing:	
i. Phishtank - http://www.phishtank.com/	
ii. APWG - http://www.antiphishing.org/report_phishing.html	
iii. Netcraft - http://toolbar.netcraft.com/report_url	
iv. Google - http://www.google.com/safebrowsing/report_phish/	
v. Microsoft - https://phishingfilter.microsoft.com/feedback.aspx?result=none&URL=…	
• Preservar evidencia del incidente	

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
i. Realizar copia del sitio Web con una herramienta de tipo spider	
ii. Solicitar al ISP una copia del contenido del sitio Web	
• Inyectar (dilución) datos falsos pero creíbles en la página del phishing de forma automática	
• En caso de que el ataque afecte a una comunidad que accede desde alguna red concreta se podría filtrar el acceso de esa comunidad a la URL o IP del ataque.	
4. Análisis e Investigación	
• Obtener y analizar evidencias para afrontar resolución del incidente	
i. Analizar la infraestructura empleada para crear el sitio phishing (redirecciones entre dominios, uso de *frames*, uso de proxies inversos o mecanismos de alta disponibilidad y/o balanceo de la carga, etc.)	
ii. Visitar el sitio phishing con distintos navegadores	
iii. Recopilar datos sobre el/los servidor/es donde se aloja el phishing	
1. Whois	
2. DNS	
3. RIR's	
4. Buscadores de Internet	
5. Solución y Recuperación	
• Notificar al ISP mediante el medio apropiado (teléfono, FAX, e-mail) sobre la existencia del phishing y solicitar el cierre inmediato del mismo.	
• En caso de existir un dominio creado expresamente para el ataque notificar a al agente registrador (registrant) donde se registró y solicitar el cierre.	
• Verificar que tras el cierre del sitio fraudulento este no reaparece horas más tarde ya sea en el mismo servidor o utilizando otros servidores atacados.	
6. Reflexión y Mejora	
• Documentar el proceso de respuesta a incidentes junto con un resumen ejecutivo.	
• Documentar los errores cometidos durante la gestión del incidente y las posibles acciones a tomar para mejorar la prevención y gestión de incidentes en el futuro.	

E.5. RESPUESTA A INCIDENTES: CASOS DE DENEGACIÓN DE SERVICIO

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
0. Durante todo el proceso **Documentar todo**: incluyendo acciones realizadas, evidencia recolectada, conversaciones y datos suministrados por usuarios, administradores y otras personas relacionadas con el incidente.	
1. Identificación	
• Buscar un compañero que pueda ayudar en la gestión del incidente aunque sea únicamente para documentar las acciones realizadas	
• Analizar evidencia para confirmar si realmente se trata de un incidente:	
i. Origen del ataque	
ii. Tipo de tráfico utilizado (TCP/UDP/ICMP)	
iii. Protocolo utilizado y tipo de peticiones	
2. Notificación	
• Notificar a los responsables dentro de la organización. Sólo dando la mínima información para que cada persona pueda realizar su trabajo y evitando dar detalles técnicos innecesarios para evitar la fuga de información sensible.	
• Notificar al CCN-CERT para solicitar ayuda especializada en la gestión del incidente	
3. Contención	
• Añadir servidores/infraestructura de red a los clusters balanceados	
• Usar redes de distribución de contenido, tipo Akamai	
• A nivel de Red:	
i. FW's e IPS	
1. Activar mecanismos Anti-Flood y Anti-Spoofing	
2. Revisar/Activar reglas Anti-DDoS en IPS	
3. Diseñar reglas de filtrado más eficientes e inteligentes	
ii. Filtrar stream malicioso en los puntos más externos del perímetro	
iii. Si el ancho de banda está saturado, intentar gestionar una ampliación inmediata de caudal, si es posible.	

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
iv. "Desconectar" la red atacada de Internet, para mantener la disponibilidad de los servicios para los usuarios de la red interna.	
• A nivel de Servidores:	
i. Para servidores Web:	
1. Cambiar a páginas más ligeras → menos recursos de servidor y menos ancho banda.	
2. Desactivar todos los sistemas de búsqueda y operaciones pesadas.	
3. Eliminar módulos no imprescindibles de los servidores atacados para hacerlos más eficientes.	
4. Intentar identificar las peticiones maliciosas y bloquearlas (por ejemplo: sin Referral o un Referral concreto, por User-Agent, etc, usando Mod_Security en entornos Apache o firewalls de aplicación).	
5. Activar mecanismos de bloqueo en base a exceso de peticiones (Mod_Evasive, en entornos Apache).	
ii. Para servidores de Correo:	
1. Configurar los sistemas Antispam de forma agresiva.	
2. Activar todas las listas negras posibles, y configurar el Antispam rechazando conexiones de esas IP's (la mayoría de las botnets son usadas para envío de SPAM, por lo que suelen estar con frecuencia en listas negras)	
iii. Para Servidores DNS:	
1. Configurar servidores DNS alternativos conectados por redes alternativas	
2. Añadir / Modificar los nuevos servidores en el registrador del dominio	
3. Configurar el servicio de resolución de DNS ofrecido por la mayoría de los registradores	
4. Análisis e Investigación	
• Recopilar información sobre los orígenes y métodos de ataque.	
• Recopilar información sobre el funcionamiento de la botnet incluyendo centros de control, canales de comunicación, etc.	
• Obtener y analizar un ordenador zombie o software utilizado en el ataque para entender mejor el funcionamiento y posibles soluciones.	
5. Solución y Recuperación	

Pasos a tomar para responder a un incidente o cuando hay indicios de que podría haberlo	√
• En caso de que el ataque sea distribuido coordinarse con otros equipos de respuesta a incidentes e ISP:	
i. Desactivar las botnets	
ii. Solicitud a ISP para filtrado de ataques en origen.	
• Neutralizar botnet	
i. Actuar contra el origen de las ordenes (Por ejemplo, cerrar el canal IRC).	
ii. Análisis de la comunicación Zombie-Master y envío de ordenes de finalizar a los zombies	
• Confirmar pasado un tiempo prudencial que la situación ha vuelto a la normalidad antes de dar por resuelto el incidente.	
6. Reflexión y Mejora	
• Documentar el proceso de respuesta a incidentes junto con un resumen ejecutivo.	
• Documentar los errores cometidos durante la gestión del incidente y las posibles acciones a tomar para mejorar la prevención y gestión de incidentes.	

ANEXO F. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Acreditación	Situación alcanzada por los Sistemas que hayan superado con éxito el proceso de acreditación.
Activos	Son los recursos del Sistema, o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección.
Amenaza	Cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un Sistema de las TIC resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio Sistema.
Análisis de riesgos	Es el proceso por el cual se identifican y valoran los riesgos.
Autoridad de Acreditación (AA)	Autoridad responsable de conceder la autorización a un Sistema para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.
Autoridad Delegada Acreditación (ADA)	Autoridad en la que ha delegado la Acreditación la AA, y que es responsable de la aplicación de la normativa de acreditación vigente.
Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones (AOSTIC)	Autoridad responsable del desarrollo, la operación y mantenimiento del Sistema durante su ciclo de vida, de sus especificaciones, de su instalación y de la verificación de su correcto funcionamiento.
Botnet	Red formada por múltiples (entre 1.000-100.000) ordenadores bot (también llamados zombie) que suelen utilizarse para el envío masivo de SPAM o para lanzar ataques de Denegación de Servicio.
Bug	Error, generalmente de diseño, en un programa o producto *software* que es descubierto después de ser lanzado al mercado o puesto en producción.
Confidencialidad	Cualidad o condición de la información que asegura que ésta no es conocida por individuos, entidades o procesos no autorizados.
Disponibilidad	Cualidad o condición de la información que permite, a las personas o procesos autorizados, acceder a ella cuando se requiera de acuerdo a los requisitos establecidos.
Gestión del riesgo	Proceso, que se basa en los resultados de la evaluación del riesgo, consistente en seleccionar las salvaguardas.
Impacto	Consecuencia sobre un activo de la materialización de una amenaza.
Ingeniería social	Eufemismo empleado para referirse a medios no técnicos o de baja complejidad tecnológica utilizados para atacar a Sistemas de información, tales como mentiras, suplantaciones, engaños, sobornos y chantajes.
Integridad	Cualidad o condición de la información que garantiza que no ha sido modificada por personas no autorizadas.
Riesgo	Es la posibilidad de que se materialice una amenaza sobre un activo, ocasionando una pérdida en la Organización.
Riesgo residual	Es el riesgo resultante de la aplicación de contramedidas y, por tanto, constituye el riesgo a asumir.

Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC)	Protección de la información almacenada, procesada o transmitida, por Sistemas de las Tecnologías de la Información y las Comunicaciones (Sistemas), mediante la aplicación de las medidas necesarias que aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios Sistemas.
Seguridad de las Emanaciones o Seguridad TEMPEST	Conjunto de medidas destinadas a evitar fugas de información derivadas de emisiones electromagnéticas no deseadas de equipos electrónicos.
Sistema de las Tecnologías de la Información y las Comunicaciones (Sistema)	Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información que está bajo responsabilidad de una única Autoridad.
TEMPEST	Término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.
Vulnerabilidad	Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso del Sistema.
Zombie	Sistema informático comprometido que pertenece a una botnet y que es utilizado para realizar actividades con fines maliciosos.

ANEXO G. ABREVIATURAS

AA	Autoridad de Acreditación
ACC	Autoridad de Certificación Criptológica
ACMC	Autoridad de Control de Material de Cifra
ADA	Autoridad Delegada de Acreditación
AOSTIC	Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones
ASS	Administrador de Seguridad del Sistema
ASTIC	Autoridad de Seguridad de las de las Tecnologías de la Información y las Comunicaciones
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
CO	Concepto de Operación
DRS	Declaración de Requisitos de Seguridad
DRSI	Declaración de Requisitos de Seguridad de la Interconexión
ERIS	Equipo de Respuesta ante Incidentes de Seguridad
O.M.	Orden Ministerial
ODBC	Órgano de Distribución de Material de Cifra
OTAN	Organización del Tratado del Atlántico Norte
POS	Procedimientos Operativos de Seguridad
RSA	Responsable de Seguridad del Área
Sistema	SISTEMA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
SLA	Nivel de Servicio Acordado (*Service Level Agreement*)
STIC	Supervisor de Seguridad de las de las Tecnologías de la Información y las Comunicaciones
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones.
TIC	Tecnologías de la Información y las Comunicaciones
UE	Unión Europea.

ANEXO H. REFERENCIAS

[Ref.- 1]	FCC “Computer Security Incident Response Guide” http://csrc.nist.gov/groups/SMA/fasp/documents/incident_response/Incident-Response-Guide.pdf
[Ref.- 2]	NIST, “Computer Security Incident Handling Guide” http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
[Ref.- 3]	NIST “Guide to Integrating Forensic Techniques into Incident Response” http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
[Ref.- 4]	NIST “Guide to Malware Incident Prevention and Handling” http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
[Ref.- 5]	O’Reilly “Incident Response” http://www.oreilly.com/catalog/incidentres/index.html
[Ref.- 6]	“Forum of Incident Response and Security Teams” http://www.first.org/
[Ref.- 7]	TERENA “Task Force of Computer Security Incident Response Teams” http://www.terena.nl/activities/tf-csirt/
[Ref.- 8]	CERT Coordination Center (CERT-CC) http://www.cert.org/
[Ref.- 9]	ENISA “A step-by-step approach on how to set up a CSIRT” http://www.enisa.europa.eu/cert_guide/downloads/CSIRT_setting_up_guide_ENISA.pdf
[Ref.- 10]	ENISA “Inventory of CERT Activities in Europe v1.3” http://www.enisa.europa.eu/cert%5Finventory/downloads/Enisa_CERT_inventory.pdf http://www.enisa.europa.eu/cert%5Finventory/downloads/CERT_Euromap.pdf
[Ref.- 11]	European Cooperation of Abuse fighting Teams (E-CoAT) http://www.e-coat.org/
[Ref.- 12]	NSP-SEC http://www.nspsec.org/
[Ref.- 13]	Distributed Intrusion Detection System http://www.dshield.org/
[Ref.- 14]	Network Intrusion Detection and Reporting http://www.mynetwatchman.com/
[Ref.- 15]	CERT-CC “Handbook for CSIRTs” http://www.cert.org/archive/pdf/csirt-handbook.pdf
[Ref.- 16]	State of the Practice of Computer Security Incident Response Teams (CSIRTs) http://www.cert.org/archive/pdf/03tr001.pdf
[Ref.- 17]	CSIRT Services http://www.cert.org/csirts/services.html
[Ref.- 18]	Steps for Creating National CSIRTs http://www.cert.org/archive/pdf/NationalCSIRTs.pdf
[Ref.- 19]	CERT®-Certified Computer Security Incident Handler http://www.cert.org/certification/
[Ref.- 20]	Action List for Developing a Computer Security Incident Response Team (CSIRT) http://www.cert.org/archive/pdf/csirts_action_list.pdf
[Ref.- 21]	GIAC Certified Incident Handler (GCIH) http://www.giac.org/certifications/security/gcih.php
[Ref.- 22]	“Training of Network Security Incident Teams Staff (TRANSITS)” http://www.terena.nl/activities/csirt-training/
[Ref.- 23]	RedRIS, “Mesa Redonda: Evolución de los Equipos de Respuesta a Incidentes” Jornadas Técnicas 2005 http://www.rediris.es/jt/jt2005/archivo/archivo-jt.es.html