UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T E.409

(05/2004)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE E: EXPLOTACIÓN GENERAL DE LA RED, SERVICIO TELEFÓNICO, EXPLOTACIÓN DEL SERVICIO Y FACTORES HUMANOS

Gestión de red – Gestión de la red internacional

Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones

Recomendación UIT-T E.409

RECOMENDACIONES UIT-T DE LA SERIE E

EXPLOTACIÓN GENERAL DE LA RED, SERVICIO TELEFÓNICO, EXPLOTACIÓN DEL SERVICIO Y FACTORES HUMANOS

EXPLOTACIÓN DE LAS RELACIONES INTERNACIONALES	
Definiciones	E.100–E.103
Disposiciones de carácter general relativas a las Administraciones	E.104–E.119
Disposiciones de carácter general relativas a los usuarios	E.120–E.139
Explotación de las relaciones telefónicas internacionales	E.140–E.159
Plan de numeración del servicio telefónico internacional	E.160–E.169
Plan de encaminamiento internacional	E.170–E.179
Tonos utilizados en los sistemas nacionales de señalización	E.180–E.189
Plan de numeración del servicio telefónico internacional	E.190–E.199
Servicio móvil marítimo y servicio móvil terrestre público	E.200–E.229
DISPOSICIONES OPERACIONALES RELATIVAS A LA TASACIÓN Y A LA CONTABILIDAD EN EL SERVICIO TELEFÓNICO INTERNACIONAL	
Tasación en el servicio internacional	E.230–E.249
Medidas y registro de la duración de las conferencias a efectos de la contabilidad	E.260–E.269
UTILIZACIÓN DE LA RED TELEFÓNICA INTERNACIONAL PARA APLICACIONES NO TELEFÓNICAS	
Generalidades	E.300–E.319
Telefotografía	E.320–E.329
DISPOSICIONES DE LA RDSI RELATIVAS A LOS USUARIOS	E.330–E.349
PLAN DE ENCAMINAMIENTO INTERNACIONAL	E.350–E.399
GESTIÓN DE RED	
Estadísticas relativas al servicio internacional	E.400–E.404
Gestión de la red internacional	**E.405–E.419**
Comprobación de la calidad del servicio telefónico internacional	E.420–E.489
INGENIERÍA DE TRÁFICO	
Medidas y registro del tráfico	E.490–E.505
Previsiones del tráfico	E.506–E.509
Determinación del número de circuitos necesarios en explotación manual	E.510–E.519
Determinación del número de circuitos necesarios en explotación automática y semiautomática	E.520–E.539
Grado de servicio	E.540–E.599
Definiciones	E.600–E.649
Ingeniería de tráfico para redes con protocolo Internet	E.650–E.699
Ingeniería de tráfico de RDSI	E.700–E.749
Ingeniería de tráfico de redes móviles	E.750–E.799
CALIDAD DE LOS SERVICIOS DE TELECOMUNICACIÓN: CONCEPTOS, MODELOS, OBJETIVOS, PLANIFICACIÓN DE LA SEGURIDAD DE FUNCIONAMIENTO	
Términos y definiciones relativos a la calidad de los servicios de telecomunicación	E.800–E.809
Modelos para los servicios de telecomunicación	E.810–E.844
Objetivos para la calidad de servicio y conceptos conexos de los servicios de telecomunicaciones	E.845–E.859
Utilización de los objetivos de calidad de servicio para la planificación de redes de telecomunicaciones.	E.860–E.879
Recopilación y evaluación de datos reales sobre la calidad de funcionamiento de equipos, redes y servicios	E.880–E.899

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T E.409

Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones

Resumen

El objetivo de esta Recomendación es analizar los hechos que se interponen en el curso normal de una acción, determinar su naturaleza y sugerir un método para crear una estructura de tratamiento de incidentes en el marco de una organización de telecomunicaciones que presta servicios de telecomunicaciones internacionales, centrada en el tipo de daño que pueden causar o en el flujo y en la forma de organizarlos. El flujo y el tratamiento son útiles para clasificarlos, según su gravedad, como evento, incidente, incidente de seguridad o crisis. La noción de flujo incluye también las primeras decisiones críticas que hay que tomar.

La delincuencia informática (ciberdelincuencia) es el resultado del auge de las computadoras en las telecomunicaciones internacionales. Los delitos han aumentado exponencialmente en los últimos años, como lo confirman varios estudios nacionales e internacionales. En la mayoría de los países no existen datos exactos acerca de la cantidad de incidentes del tipo robo de ordenadores o de violación de la seguridad, especialmente en relación con las telecomunicaciones internacionales.

En general las organizaciones o empresas de telecomunicaciones no disponen de ninguna estructura especializada para tratar los incidentes de seguridad relativos a las redes de la información y la comunicación (ICN) (pero sí tienen un grupo para solucionar cualquier tipo de crisis). Cuando ocurre un incidente de seguridad ICN se trata según convenga, es decir que quien detecta el problema asume la responsabilidad de resolverlo de la mejor manera posible. En algunas organizaciones, se suele olvidar o disimular los incidentes de seguridad ICN, ya que afectan la producción, disponibilidad e ingresos.

En general, la persona que detecta un incidente de seguridad ICN no sabe a quién comunicarlo. Esto significa que el administrador del sistema o la red tiene que encontrar un parche o soluciones rápidas, sin contar con las facultades, el tiempo o los conocimientos para corregirlo de forma que no se vuelva a producir. Por ello, es mejor tener un grupo o unidad capacitado para hacer frente a los incidentes de seguridad rápida y correctamente. Además, muchos de los problemas pueden aparecer en dominios tan diversos como las relaciones con los medios, o los asuntos jurídicos, de cumplimiento de la ley, de la cuota de mercado o financieros.

El uso de vocabularios diferentes en los informes o el manejo de los incidentes ocasiona confusión. A su vez, esto da por resultado que el incidente de seguridad ICN no reciba la atención adecuada ni se tomen las medidas oportunas para pararlo, contenerlo e impedir que vuelva a ocurrir. Las consecuencias para la organización afectada (víctima) pueden ser desastrosas.

Para comunicar y tratar los incidentes con éxito es necesario entender cómo se los detecta, trata y soluciona. Un marco general para hacer frente a los incidentes (sean físicos, administrativos, organizacionales o logísticos) da una visión general de la estructura y el flujo de un incidente. Para lograr que todos entiendan las palabras y expresiones es indispensable contar con un vocabulario uniforme.

Orígenes

La Recomendación UIT-T E.409 fue aprobada el 28 de mayo de 2004 por la Comisión de Estudio 2 (2001-2004) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Recomendación UIT-T E.409

Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones

1 Introducción

1.1 Alcance

El objetivo de esta Recomendación es analizar los hechos que se interponen en el curso normal de una acción, determinar su naturaleza y sugerir un método para crear una estructura de tratamiento de los incidentes en el marco de una organización de telecomunicaciones que proporciona telecomunicaciones internacionales, centrada en el tipo de daño que puedan causar o en el flujo, y en la forma de organizarlos. El flujo y el tratamiento son útiles para clasificarlos, según su gravedad como evento, incidente, incidente de seguridad o crisis. La noción de flujo incluye también las primeras decisiones críticas que hay que tomar.

En esta Recomendación se da una visión general y unas bases que sirven de directrices para planificar la organización de los incidentes y el tratamiento de incidentes de seguridad.

Esta Recomendación es de carácter general y no versa sobre las necesidades de redes específicas.

Esta Recomendación pretende facilitar el desarrollo de nuevos aspectos internacionales relativos a la seguridad de las redes de telecomunicaciones. Dicha labor se vería facilitada si los requisitos establecidos por la presente Recomendación se aplicaran igualmente a las redes de la información y la comunicación (ICN, *information and communication networks*) nacionales.

Para comunicar y tratar los incidentes con éxito es necesario entender cómo se los detecta, trata y soluciona. Mediante la creación de una estructura general para el tratamiento de incidentes (sean físicos, administrativos, organizacionales o logísticos) se puede obtener una visión general de la estructura y el flujo de un incidente. Para lograr que todos entiendan las palabras y expresiones es indispensable utilizar una terminología uniforme.

El uso de taxonomías diferentes en los informes o en el tratamiento de incidentes ocasiona confusión. A su vez, esto da por resultado que el incidente de seguridad ICN no reciba la atención adecuada ni se tomen las medidas oportunas para pararlo, contenerlo e impedir que vuelva a ocurrir. Las consecuencias para la organización afectada (víctima) pueden ser desastrosas.

En esta Recomendación se describen el flujo y el tratamiento de incidentes.

La definición de un incidente varía según la profesión, la organización y la persona.

De acuerdo con el significado general de la palabra incidente, éste puede ser desde un error en una copia de seguridad, una perturbación de los servicios, un ataque por un virus, hasta la intrusión en los sistemas informáticos.

1.2 Definiciones

ISO 17799 hace mención a incidentes, incidentes de seguridad e incidentes de seguridad informática.

Sólo se define el término "incidente de seguridad" como un "atentado contra la seguridad, amenaza, debilidad y mal funcionamiento que puede afectar a la seguridad de los bienes de la organización". En ninguna parte se explica el sentido de los términos "incidente" e "incidente de seguridad informática". En esta Recomendación se supone que un incidente es algo menos grave que un incidente de seguridad y que un incidente de seguridad informática es un tipo particular de incidente de seguridad.

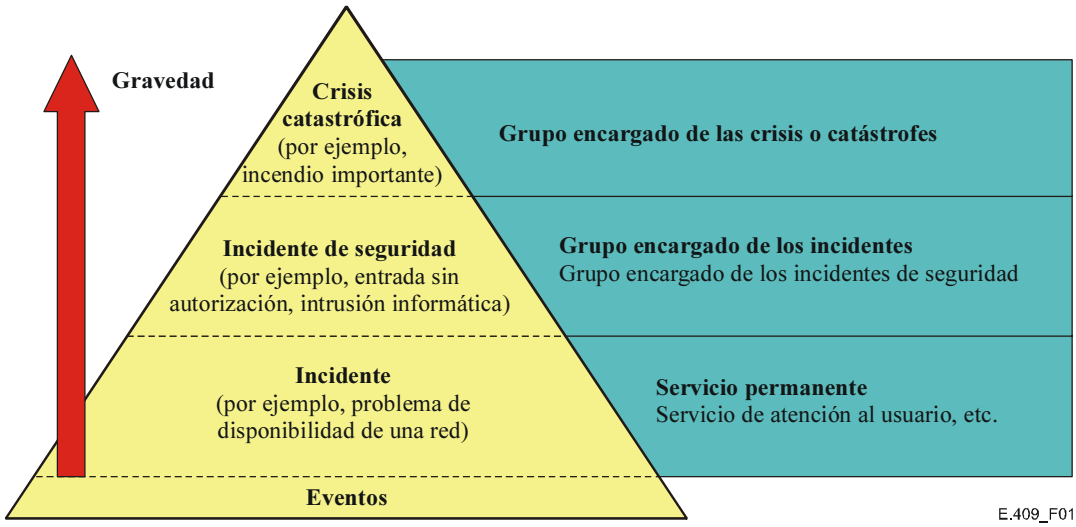

Figura 1/E.409 – La pirámide de eventos

En la figura 1 se muestra la pirámide de eventos, en cuya base se encuentra el evento, seguido por el incidente, el incidente de seguridad y en la cima la crisis catastrófica. Cuanto más arriba se encuentre un evento, mayor es su gravedad. Con el fin de tener un vocabulario común y bien fundamentado para el tratamiento de incidentes en el ámbito de las redes de la información y la comunicación, en esta Recomendación se definen los siguientes términos.

1.2.1 **evento**: Suceso perceptible que no se puede predecir o controlar (completamente).

1.2.2 **incidente**: Un evento cuyas consecuencias no son graves.

1.2.3 **incidente de seguridad**: Cualquier evento adverso que podría amenazar algún aspecto relacionado con la seguridad.

1.2.4 **incidente de seguridad de las redes de la información y la comunicación (ICN)**: Cualquier evento adverso, real o potencial, relacionado con la seguridad de las ICN. Por ejemplo:

- una intrusión en los sistemas de computación de las ICN a través de la red;
- aparición de virus informáticos;
- pruebas de vulnerabilidad en una gama de sistemas de computación a través de la red;
- filtración a través de una central automática privada conectada a la red pública (PABX, *private automatic branch exchange*);
- cualquier otro evento no deseado que surge de acciones internas o externas no autorizadas.

1.2.5 **crisis**: Estado causado por un evento, o por el hecho de saber que un evento es inminente, que puede tener consecuencias negativas graves. Durante una crisis se puede, en el mejor de los casos, tomar medidas para evitar que ésta se convierta en una catástrofe. En general, se dispone de un plan de emergencia para las empresas (BCP, *business continuency plan*) para **catástrofes** y de un equipo encargado de la gestión de crisis para que se ocupe de la situación.

1.3 Bases

Se recomienda a las organizaciones de telecomunicaciones que creen grupos encargados de los incidentes (de seguridad informática) que en primer lugar especifiquen la taxonomía de incidentes a fin de evitar malentendidos. La colaboración es más fácil cuando se utiliza el mismo "idioma".

Se recomienda que las organizaciones utilicen las expresiones "incidente" e "incidente de seguridad ICN", y establezcan sus propias subcategorías basándose en la gravedad de esta última. En esencia, un incidente de seguridad ICN podría ser cualquier evento no deseado y no autorizado. Ello significa que un incidente de seguridad ICN incluye una intrusión informática, un ataque por denegación de servicio o un virus según la motivación, la experiencia y los recursos de que dispone la organización. En las organizaciones que dispongan de un equipo eficaz antivirus, cabría considerar a los virus como simples incidentes en lugar de incidentes de seguridad informática.

Un ejemplo o plantilla de esta subdivisión es:

- Incidentes
  - Violación de las normas de conducta de Internet (*Internet netiquette*) (bombardeo de correos, contenido ofensivo, etc.)
  - Violación de las políticas de seguridad
  - Virus particulares
- Incidentes de seguridad ICN
  - Exploraciones y sondeos de la vulnerabilidad
  - Intrusiones en el computador
  - Sabotaje y daño a los computadores (ataques contra la disponibilidad, como por ejemplo "bombardeo" o ataques DoS)
  - Programas informáticos maliciosos (virus, "caballos de troya", gusanos, etc.)
  - Robo de información y espionaje
  - Suplantación de persona

La utilización de la misma granularidad y precisión en la terminología puede permitir, después de todo, ganar experiencia acerca de:

- las directrices relativas a la gravedad y alcance;
- los indicios sobre la rapidez de reacción;
- las posibles contramedidas;
- los posibles costos que entrañan.

2 Descripción del sistema

2.1 Estructura y flujo

Al establecer una estructura general para el tratamiento de incidentes (sean físicos, administrativos u organizacionales, y logísticos) se obtiene una visión general de la estructura y el flujo del incidente.

2.1.1 Principios de protección

Los mecanismos de protección de la organización deben corresponder con sus necesidades en materia de la política de seguridad ICN existente, o su equivalente, incluidos los aspectos jurídicos. La organización del tratamiento de incidentes y sus tareas asociadas serán acordes con esas necesidades.

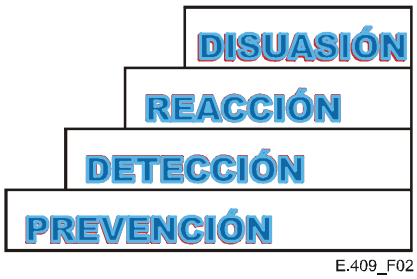

Figura 2/E.409 – Principios de protección

De la figura 2 se colige que es necesario empezar desde lo más básico. Es decir la organización debe implementar todas las etapas que intervienen en los mecanismos de seguridad para que la protección sea coherente.

Se debe empezar por establecer los mecanismos de protección *preventiva*, ya sea del tipo física o lógica, para entonces determinar y activar los mecanismos de protección de *detección*.

Los mecanismos de protección de *detección* pueden ser, en su forma más simple, la verificación o registros cronológicos, alarmas lógicas o físicas, es decir alarmas antirrobo, alarmas de incendio u otras funciones de vigilancia. Un tipo de mecanismo de detección es el sistema de detección de intrusión (IDS, *intrusion detection system*).

Cuando se detecte un incidente se han de emprender acciones que, en general, incluyen las siguientes tareas:

- parar un incidente en curso;
- identificar el alcance/escala del incidente;
- limitar los daños;
- tomar medidas para averiguar el curso de los eventos;
- impedir que el incidente vuelva a ocurrir.

Las acciones destinadas a parar y limitar el incidente (contenerlo) e impedir que vuelva a ocurrir debe realizarlas el servicio permanente, es decir el servicio de atención al usuario (*helpdesk*) o la unidad de soporte. Si el incidente degenera en una crisis, deberá intervenir un grupo especialmente entrenado en el tratamiento de crisis. Se recomienda, en lo que respecta a la investigación y el análisis del incidente, que intervenga el grupo encargado de los incidentes.

Cuando están funcionando estos tres mecanismos de protección, existe un efecto de disuasión, es decir que el autor del incidente sabe que hay mecanismos de protección y que tanto la detección como la reacción ante incidentes son inmediatas. Este efecto es aún mayor si se reacciona ante todos los incidentes y se informa acerca de cualquier incidente ilegal a las autoridades correspondientes.

2.1.2 Estructura para el tratamiento de incidentes

Con el fin de poder entender el papel que juegan el tratamiento y la organización de los incidentes en una organización, se recomienda utilizar una estructura de tratamiento de incidentes. Esta estructura presenta una visión general del flujo del incidente, que describe su producción, las acciones/medidas que han de emprenderse para contenerlo, la recuperación y el seguimiento posterior.

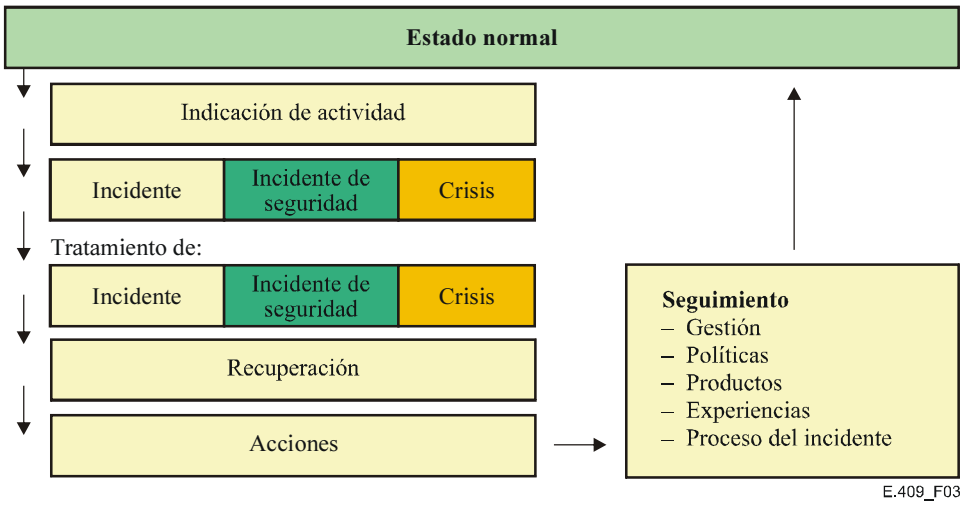

Figura 3/E.409 – Estructura para tratar los incidentes

Esta estructura (véase figura 3) muestra que todos los eventos, incidentes, incidentes de seguridad y crisis se producen a partir de un estado normal, es decir, de una situación de funcionamiento normal.

Cuando se detecta un indicio de actividad que pueda dar lugar a un incidente o incidente de seguridad, el servicio permanente se encarga de solucionarlo como se describe más adelante. El tiempo que transcurre entre la detección de los indicios y la producción del incidente de seguridad puede ser muy breve. Algunos tipos de indicios de incidentes son: virus en una sola estación de trabajo, error en la red, etc. Los indicadores de incidentes de seguridad, pueden estar en los archivos de registro cronológico, las barreras de seguridad (*firewall*), etc. Otros indicios son la activación de alarmas, la observación de las cámaras de vigilancia, etc.

Cuando *ocurre un incidente o un incidente de seguridad*, éste se evalúa según su alcance y consecuencias. Un incidente puede degenerar en un incidente de seguridad o en una crisis. El servicio permanente se encarga de tratar el incidente mientras que el equipo encargado de los incidentes informáticos (CSIRT, *computer incident response team*) se ocupa de los incidentes de seguridad. De las crisis se encarga un grupo de gestión formado especialmente para ello.

El CSIRT puede ser el equipo entero de seguridad de una organización de telecomunicaciones o un equipo totalmente distinto de éste. Por otra parte, aunque no exista un CSIRT como tal en la organización, el equipo de seguridad de ésta puede asumir implícitamente este papel.

Las *acciones/medidas* que se toman siguen una rutina preestablecida o un procedimiento habitual. En caso de incidentes graves de seguridad o crisis, las medidas están supeditadas al alcance y consecuencias del incidente. El equipo de seguridad o el equipo encargado de los incidentes toma las medidas del caso.

Durante la *recuperación* se toman las medidas necesarias para volver al funcionamiento normal. Según el tipo de evento producido, esto puede implicar el reinicio de los sistemas informáticos o de red, la reinstalación de programas o la restauración de copias de seguridad. Algunas de estas medidas pueden ser la puesta en marcha nuevamente de las alarmas, la reconstrucción de la propiedad afectada, etc.

Mientras se efectúa este trabajo, también se evalúa si se han de emprender acciones legales relacionadas con el evento. Para ello puede ser necesario efectuar una investigación más rigurosa y obtener pruebas sólidas.

Es importante hacer un *seguimiento* del trabajo que se realiza para tratar los incidentes y los incidentes de seguridad, así como las crisis, con el fin de mejorar el funcionamiento normal y los procedimientos para evitar que vuelvan a ocurrir y minimizar sus consecuencias y costos.

El informe de seguimiento puede dar por resultado modificaciones del proceso, de los productos y de las políticas en materia de incidentes. Se presenta a la administración un resumen de los incidentes e incidentes de seguridad acaecidos, de su alcance, consecuencias y costos. Asimismo, conviene incluir en el resumen aspectos relativos a la eficacia de la organización encargada del tratamiento de incidentes. Habría que crear un registro que contenga las lecciones aprendidas y las experiencias obtenidas a fin de poder comparar los diferentes incidentes y encontrar métodos y prácticas más eficaces para detectarlos y tratarlos.

2.2 Flujo de incidente

A continuación se describe el flujo de un incidente o incidente de seguridad. Se utiliza un enfoque empírico que debe ser aplicable a todas las organizaciones de telecomunicaciones y a todo tipo de incidentes, ya que se trata de un flujo sencillo y general. Se puede comparar el flujo de un incidente con las acciones que se toman en caso de un accidente, un incendio, etc. El punto de partida, o parámetro, es que ocurre un evento con implicaciones para la organización.

2.2.1 Las fases en el tratamiento de la crisis

En la gestión de crisis, éstas se presentan como si constaran de tres fases a saber:

- **La prefase**, en la que hay indicios de que algo no funciona bien. En esta fase es necesario estar alerta y preparados.
- **La fase de emergencia**, que es cuando ocurre la crisis. Una emergencia siempre es algo inesperado e inoportuno y, con frecuencia, ocurre fuera de las horas laborables o durante los fines de semana. Como cada crisis es diferente, es importante que no se la trate conforme a un procedimiento estándar en el que cada paso a seguir corresponda a una amenaza definida. Cabe indicar que las personas encargadas de la gestión de las crisis deben poseer el liderazgo necesario y ser capaces de improvisar.
- **Fase postcrisis**, o después de la crisis, es la fase crucial si la organización se dispone a resolver la crisis y a superarla. Esta fase consta de varias subfases tales como los primeros auxilios sicológicos, las acciones para retornar al funcionamiento normal, las lecciones aprendidas, etc.

2.2.2 Las fases del tratamiento de incidentes

Los incidentes se basan en la fase de emergencia de la gestión de crisis, a la que se añaden dos fases adicionales, la *fase de tratamiento* y la *fase de seguimiento*, que se describen en la figura 4.

No se utilizan las mismas fases que en la gestión de crisis porque la prefase en esta última abarca las fases en el tratamiento de incidentes como un todo. Normalmente, el tratamiento de un incidente no alcanza a llegar al nivel de gestión de una crisis. Si fuera necesario transferir un incidente a la gestión de crisis, esto implicaría que el incidente ha degenerado en una crisis.

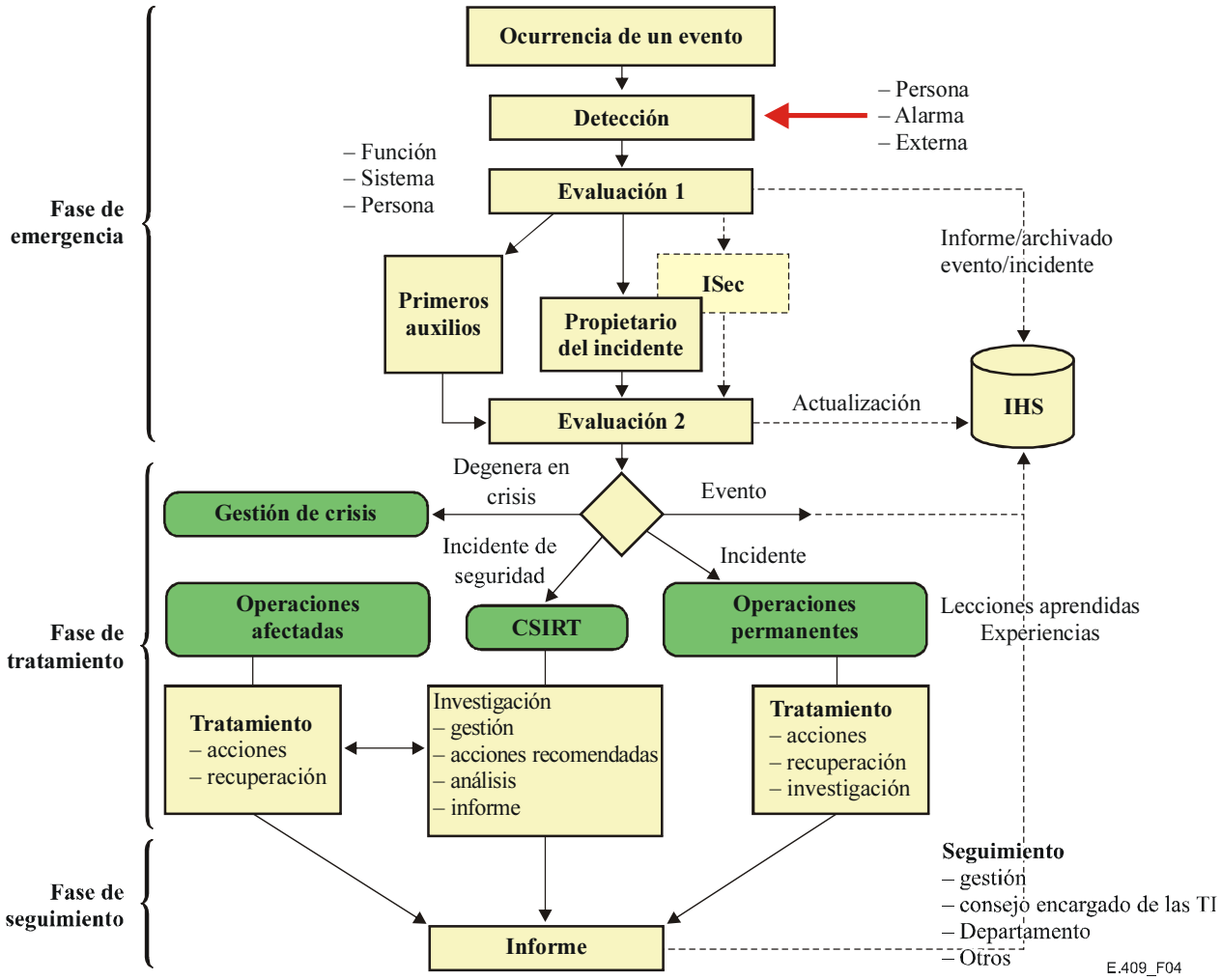

Figura 4/E.409 – Flujo de incidente

A continuación se describen las diversas fases del flujo de un incidente.

2.2.2.1 Fase de emergencia

Como se muestra en la figura 4, la fase de emergencia es la primera. Se puede hacer la comparación entre esta fase y cuando sucede un accidente, es decir en un accidente de tráfico las primeras acciones que se emprenden suelen ser importantísimas para su desenlace. Estas acciones tienen las consecuencias más importantes en lo que respecta al resultado final. En la figura 5 se describen en orden las diferentes etapas de la fase de emergencia.

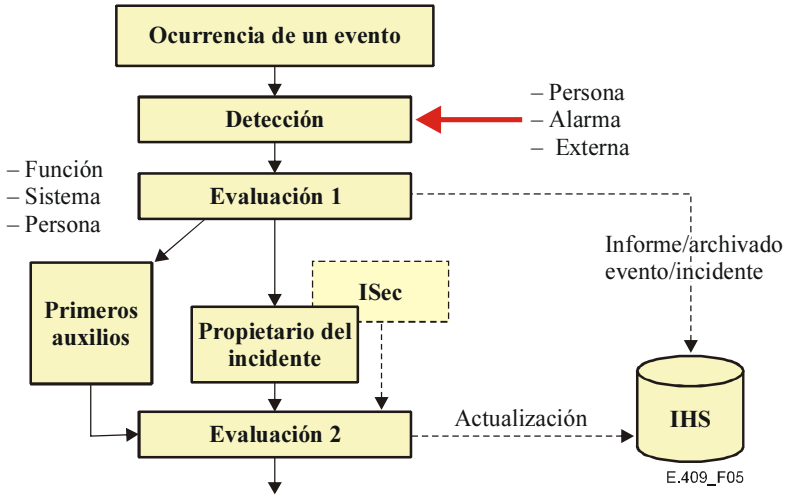

Figura 5/E.409 – Fase de emergencia

2.2.2.2 Detección

Una persona puede detectar un evento mediante la percepción visual, por ejemplo, puede observar mensajes de error, leer un archivo de resultados o efectuar un control de auditoría. La detección visual puede ocurrir cuando el operador observa a alguien cometiendo una intrusión o alguien detecta un incendio. Asimismo, cuando una persona que tenga la impresión de que algo no está bien, que algo inusual está ocurriendo.

Las alarmas lógicas son situaciones que atraen la atención del usuario extremo, del personal operador, de las funciones de seguridad, etc. Por ejemplo, una alarma activada por el programa antivirus, el subsistema de auditoría o la barrera de seguridad (*firewall*) y el sistema de detección de intrusión. De igual manera, un evento puede activar alarmas físicas como las de incendios, antirrobos, etc.

La detección externa ocurre cuando alguien que no pertenece a la organización detecta el evento. Esto podría ocurrir, en el peor de los casos, a través de las noticias o de un periodista que investiga las fuentes o entra en contacto con la organización para solicitar un comentario acerca e un evento que ésta aún no ha detectado. Podría tratarse también de las autoridades judiciales, quienes notifican al departamento de seguridad durante una investigación de un delito en curso o cuando un ciudadano descubre alguna característica desagradable en el sitio web de la organización de telecomunicaciones.

Al detectar un evento, se debe realizar una evaluación inicial de la situación para determinar su categoría y gravedad. Esto se hace clasificándolo según su tipo, es decir en incidente, incidente de seguridad, crisis o simplemente en evento; tras lo cual se han de considerar su alcance y consecuencias. A continuación se presenta una clasificación simple de eventos, válida solamente para los incidentes de seguridad ICN, que se utilizará al determinar la gravedad de un incidente o incidente de seguridad.

Esta evaluación puede ser llevada a cabo por la persona que detecta el evento, quien puede también decidir si informa acerca del evento detectado a un servicio, es decir a un servicio de ayuda al usuario, o al departamento de seguridad informática. Si se informa a un servicio, éste asume la responsabilidad. Esos servicios se conocen también como puntos de contacto (POC, *point-of-contact*) y se encargan de resolver la situación. Las alarmas suelen transferirse automáticamente a las personas, servicios o sistemas responsables. Todos los eventos notificados deben registrarse en un sistema de tratamiento de incidentes (IHS, *incident handling system*).

Un punto de contacto (POC) es una unidad o persona a quien se le informa acerca de un evento. Algunas veces, es una unidad o servicio del tipo servicio de ayuda al usuario, control de producción, departamento de seguridad o de seguridad informática (ISec). No es posible informar sobre un evento al CSIRT ya que este grupo virtual se crea cuando ocurre un incidente de seguridad. Es posible informar de los incidentes de seguridad al departamento de seguridad de la información (ISec, *information security department*), que se encarga del CSIRT, o a cualquier otro POC donde se realizará la evaluación correcta y se pondrá en contacto con las unidades encargadas.

• Clase 4	Muy grave	Incidentes de seguridad que tienen consecuencias importantes para la organización, por ejemplo ataques coordinados, intrusiones informáticas, robo de información confidencial, etc. Un incidente de seguridad que pertenezca a esta categoría puede producir daños significativos e implica tomar medidas importantes.
• Clase 3	Grave	Incidentes de seguridad que tienen consecuencias para la organización, como pueden ser sabotajes a los equipos informáticos, fraude informático, o atentado contra la integridad informática, utilización inadecuada o divulgación de información relativa a la organización o a sus clientes.
• Clase 2	Menos grave	Incidentes de seguridad, como intentos de intrusión, utilización inadecuada de recursos informáticos, etc. Un incidente de seguridad que pertenezca a esta categoría tiene consecuencias menos graves que el anterior, provoca daños menores, y no es necesario tomar medidas importantes.
• Clase 1	Sin consecuencias	Incidentes de los que se ocupa el servicio permanente pero que pueden haber degenerado en incidentes de seguridad, como por ejemplo exploración de la vulnerabilidad, virus no extendidos, abusos, ataques a los sistemas de correo electrónico, etc. En esta clase suelen encontrarse incidentes que afectan a la producción normal. Un incidente de seguridad que pertenezca a esta clase no causa daños o éstos son poco importantes y si se toman medidas éstas son poco importantes.

Se suele informar al servicio de ayuda al usuario acerca de los eventos producidos, en especial cuando éstos han sido detectados por un usuario extremo. Con frecuencia, éstos informan acerca de todos los eventos y errores a dicho servicio. En otros casos, puede ser el administrador o el operador de sistema quien detecte el evento. Los centros de control de funcionamiento para comunicaciones, y los servicios de seguridad de sistema y física también detectan eventos al recibir alarmas provenientes de los sensores físicos y lógicos o de fuentes externas.

Es necesario instruir a todos los servicios y unidades que puedan recibir alarmas o tener indicios de un evento acerca de cómo reaccionar ante ello, con el fin de evitar que se haga caso omiso o se traten incorrectamente las alarmas.

2.2.2.2.1 Evaluación 1

Esta evaluación es realizada por una persona, un servicio (POC) o un sistema (IDS). En la mayoría de los casos efectúa la evaluación quien recibe la alarma u otra información acerca del evento.

Se debe clasificar un evento dentro de una de las siguientes cinco categorías:

- Crisis.
- Incidente de seguridad.
- Incidente.
- Evento.
- Falsa alarma.

Si no se le puede clasificar en una de estas categorías, se le debe clasificar como incidente y debe ser tratado por el servicio permanente, es decir por el servicio de ayuda al usuario. Algunos eventos no generan ninguna acción pues se les considera como "errores del usuario" o malinterpretaciones.

Además, también se debe evaluar el evento teniendo en cuenta su efecto en la organización o en sus actividades. Este "nivel de gravedad" se evalúa de conformidad con los siguientes cuatro niveles:

- Consecuencias muy graves para la organización de telecomunicaciones.
- Consecuencias graves para la organización de telecomunicaciones.
- Algunas consecuencias para la organización de telecomunicaciones.
- Sin consecuencias para la organización de telecomunicaciones.

Las evaluaciones se deberán registrar en el sistema de tratamiento de incidentes, (IHS).

De haber incidentes, incidentes de seguridad o crisis, se suministrará inmediatamente una ayuda inicial (primeros auxilios), que incluye el informe inicial sobre daños, una estimación de las consecuencias y una evaluación que indique si puede haber alguna solución expedita que limite los daños. Esta evaluación suele ser efectuada por la persona o el servicio que recibe la alarma o información acerca del evento.

En lo que respecta a los incidentes, la persona o POC informa a los departamentos afectados y toma las medidas del caso. Dependiendo del alcance y consecuencias del incidente, puede dar lugar a la intervención inmediata de los expertos en su solución. En el caso de un virus informático extendido en un solo departamento, el servicio de ayuda puede encargarse del asunto en el marco de sus operaciones normales.

Al mismo tiempo, se *informa* al servicio de ayuda al usuario acerca del evento, de su naturaleza, de las medidas que se han emprendido y de cuándo los sistemas informáticos y de red volverán a funcionar con normalidad. De esta manera se informa a los operarios de este servicio, quienes serán los primeros en recibir las llamadas de los usuarios afectados por el incidente y podrán informarles de que ya se están tomando medidas al respecto. Otra razón, aún más importante, es que si otra persona informa acerca del mismo evento, o de uno similar, el servicio de ayuda al usuario sabrá cómo notificar que se ha producido de nuevo el evento.

No obstante, cuando se disemina un virus informático que está contaminando diferentes departamentos se deben coordinar las medidas que se tomen para limitar eficazmente los daños y eliminar este virus.

Todas las *indagaciones externas* deben ser dirigidas al departamento de seguridad informática.

Antes de que se tome cualquier decisión acerca de los siguientes pasos a seguir, el incidente se debe dejar en manos de su propietario o del departamento de seguridad informática (ISec). El propietario del incidente es la persona encargada del departamento afectado o el propietario del sistema afectado, y debe responsabilizarse de las posibles pérdidas y sus costos.

Cuando haya varios departamentos afectados, aquel que haya sufrido la mayor pérdida o costos será el propietario del incidente. Cuando el incidente afecte a la infraestructura de la organización de telecomunicaciones, el responsable será el departamento correspondiente. De no poderse determinar quién es el propietario, se considerará como tal al departamento de seguridad informática (ISec).

El propietario del incidente es el encargado de solucionarlo.

2.2.2.2.2 Evaluación 2

De ella se encarga el propietario del incidente o el Departamento de Seguridad Informática (ISec). El Departamento de Seguridad Informática y el CSIRT poseen los conocimientos necesarios en materia de seguridad y seguridad ICN. Se les puede consultar a fin de evaluar el alcance y las consecuencias del incidente.

Se trata de verificar la evaluación anterior relativa a la clasificación del incidente (es decir, si éste es un evento, incidente, incidente de seguridad o crisis). El propietario del incidente decide si el incidente se ha evaluado correctamente o si se deben efectuar correcciones. Asimismo, toma una decisión respecto al tratamiento posterior del incidente, incluido quién debe encargarse de tratarlo e investigarlo (si la gestión de crisis, el CSIRT o la organización permanente).

El propietario del incidente toma la decisión de informar o no al servicio de ayuda al usuario. En algunos casos es mejor posponer esta decisión hasta que se haya nombrado un encargado y se haya creado el equipo encargado del incidente.

De haber alguna duda sobre si la organización permanente puede encargarse del tratamiento del incidente, se ha de contactar a la persona de contacto del CSIRT. Si se trata de un incidente de seguridad se debe entrar en contacto con el CSIRT. De existir un departamento de seguridad informática también se le puede informar. A esas alturas, se debe tener muy claro el alcance del incidente de seguridad y se efectuará una evaluación mutua que determine si conviene o no acudir a la gestión de crisis.

Se actualiza el registro del incidente real en el sistema de tratamiento de incidentes (IHS), incluso si no se ha emprendido ninguna acción. El propósito es determinar si algunos eventos aislados, o varios eventos pueden estar relacionados con otros eventos, incidentes o incidentes de seguridad, aunque no existan pruebas al respecto en ese momento. De ocurrir un incidente de seguridad la conexión entre estos eventos y dicho incidente puede entonces ser clara.

Tras esta fase, el incidente de seguridad entra en la fase de tratamiento.

2.2.2.2.3 Fase de tratamiento

Durante esta fase se realiza el tratamiento real del evento. Este último puede ser un incidente, un incidente de seguridad o una crisis. Al entrar en esta fase adquiere su estado "oficial" y se le debe dar el tratamiento que se explica a continuación.

En caso de **crisis** o cuando un evento **degenera en crisis**, interviene la gestión de crisis y se encarga del tratamiento del incidente siguiendo un procedimiento preestablecido. Las medidas que se tomen también siguen procedimientos preestablecidos para los casos de crisis, en particular la creación de un grupo de gestión de crisis. La gestión y el tratamiento de crisis están fuera del alcance de esta Recomendación.

El servicio de telecomunicaciones permanente, es decir el control de producción, el servicio de ayuda, seguridad y vigilancia, etc., se encarga del tratamiento del **incidente**. Éste puede consistir en errores y problemas en la producción, visitantes "que andan por allí sueltos", etc. Para el tratamiento de los incidentes, el servicio permanente:

- Emprende acciones para contrarrestar la causa y los efectos del incidente y evitar que vuelva a ocurrir.
- Recupera el estado de tal manera que se pueda volver a un funcionamiento normal.
- Investiga la causa del incidente y sus consecuencias y documenta las acciones realizadas.

Se sugiere que la unidad de ayuda a la producción y su servicio establecido se ocupen del tratamiento de los incidentes de producción.

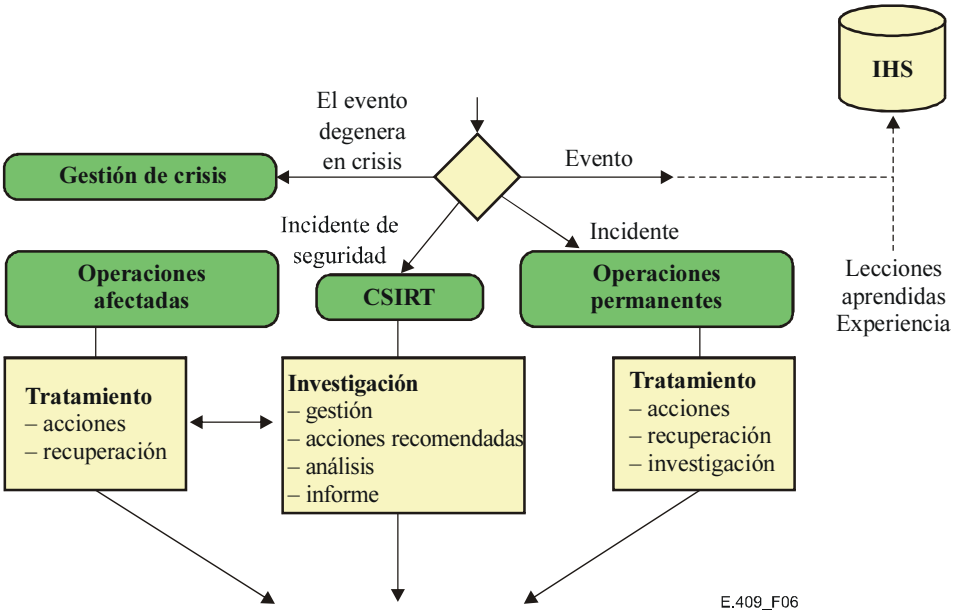

Figura 6/E.409 – La fase de tratamiento

Al entrar un **incidente de seguridad** en la fase de tratamiento, éste se efectúa siguiendo un procedimiento preestablecido.

El propietario del incidente, de común acuerdo con el departamento de seguridad informática (ISec), inicia y crea el equipo virtual y temporal encargado del incidente, CSIRT. Se escoge también un líder del equipo, que puede ser cualquier persona de la unidad de ayuda afectada, de la vigilancia o del departamento de seguridad informática (ISec). Se crea el equipo encargado del incidente, CSIRT, teniendo en cuenta las personas y calificaciones adecuadas para ello.

El CSIRT investiga el incidente de seguridad, es decir:

- Gestiona y ejecuta el trabajo de investigación.
- Emprende acciones para parar y limitar las consecuencias del incidente de seguridad (contención), en colaboración con el departamento afectado. El CSIRT suele actuar como una unidad de soporte.
- Recupera el estado a fin de poder regresar al funcionamiento normal, junto con el departamento afectado. El CSIRT suele ser una unidad de soporte.
- Analiza las circunstancias y las causas del incidente, sus consecuencias, y produce los documentos relativos a las acciones realizadas y a los costos correspondientes.
- Informa a las partes involucradas, es decir al departamento de seguridad informática, al servicio de ayuda al usuario, etc.

Es posible describir con muchísimo más detalle esos procedimientos, por lo que lo anterior se puede utilizar como una simple directriz.

La rutina consta de cinco etapas diferentes:

1) Identificación del tipo, alcance y consecuencias del incidente.
2) Contención, es decir parar y limitar las consecuencias del incidente de seguridad.
3) Erradicación de la causa y evitar que vuelva a ocurrir.
4) Recuperación del estado de funcionamiento normal.
5) Seguimiento.

Cuando se forma el CSIRT, la "Identificación" es un procedimiento habitual al informar a los miembros del CSIRT. Se les informa también acerca del incidente de seguridad, su estado real, las medidas emprendidas y las precauciones, etc.

2.2.2.2.4 Fase de seguimiento

Al llegar a esta fase, ya se ha resuelto la crisis, el incidente de seguridad o el incidente, y se han minimizado sus consecuencias. Queda por evaluar el evento y su tratamiento, e informar a la gestión, al departamento de seguridad informática y a los controles de producción, etc.

El informe de seguimiento debe describir cómo se detectó el incidente, el tiempo transcurrido entre la detección y la (re)acción, las medidas que se tomaron, así como su eficacia y resultado. También debe informar acerca de puntos débiles encontrados en el entorno original (de redes de la información y la comunicación), deficiencias en el tratamiento y en los procedimientos. Todo ha de registrarse en un archivo de Lecciones aprendidas o Experiencia, que podrá ser utilizado en el futuro para evitar caer en los mismos errores. Se deben estimar tanto los costos directos como los indirectos en los que se incurra a causa del incidente.

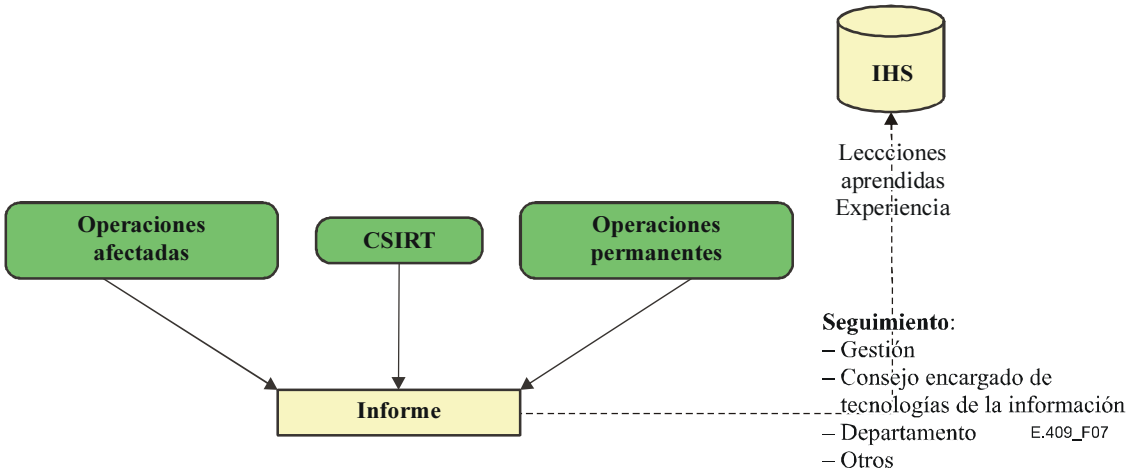

Figura 7/E.409 – Fase de seguimiento

Durante esta fase se completa el registro del incidente en el IHS. Se debe crear el archivo de Lecciones aprendidas o Experiencias, con el fin de repasar y recordar las experiencias aprendidas durante las fases de emergencia, tratamiento y seguimiento.

3 Sistema de tratamiento de incidentes

Es fundamental implementar un sistema de tratamiento de incidentes que guarde la información relativa a cada evento, incidente, incidente de seguridad y crisis, detectados y notificados. El estudio de estos archivos permite aprender los tipos de eventos que ocurren con más frecuencia, las razones por las que se producen, cómo se los detecta, su alcance, consecuencias y costos. Es importante registrar eventos que no sean incidentes, incidentes de seguridad o crisis, pues aunque no constituyan ninguna amenaza vistos como eventos aislados, sí pueden ofrecer en su conjunto una visión general acerca de cómo ocurren los incidentes. Estos eventos podrían ayudar a comprender las relaciones entre los incidentes de seguridad que se producen en contra de la organización. Algunos eventos que parecen sin importancia si se les considera aisladamente, por ejemplo una solicitud incorrecta de servicio de red, pueden ser una exploración de la vulnerabilidad de las redes de la organización de telecomunicaciones, en concreto los sistemas y redes de computación de la organización si se les mira como un conjunto.

BIBLIOGRAFÍA

– Excerpts from Master's Thesis in Incident Organization and Security Incident Handling, Jimmy Arvidsson, FIINA, 2001.

– CERT/CC (URL: http://www.cert.org) 2000-09-26.

– Federal Incident Response Capability (URL: http://www.fedcirc.llnl.gov) 2000-05-20.

– Internet Security Glossary; R. Shirey, GTE/BBN Technologies, mayo de 2000.

– Informationssäkerhetshandbok, del 5 – Katastrofskydd för IT-verksamhet, v.2, Jan-Olof Andersson, JOA InfoSäk, 1999.

– Handbook for Computer Security Incident Response Teams (CSIRTs); Moira J. West-Brown, Dan Stikvoort, Klaus-Peter Kossakowski; Carnegie Mellons, Software Engineering Institute, 1998.

– Computer Security Incident Handling – Step by step, SANS Institute, NSWC, 1998.

– Intrusion Detection, Edward Amoroso, Intrusion.Net Books, 1998.

– Best Current Practice; Expectations for Computer Security Incident Response; N. Brownlee, The University of Auckland, E. Guttman, Sun Microsystems, junio de 1998.

– Computer Security Incident Handling Procedure, NSWC Dahlgren, octubre de 1996.

– Computer Crime: A Crimefighter's Handbook, David Icove, Karl Seger and William – VonStorch, O'Reilly & Associates, 1995.

– An Analysis of Security Incidents On The Internet, 1989-1995, John Howard, CERT/CC (URL: http://www.cert.org/research/JHThesis/Start.html) 2000-05-20.

– Establishing a Computer Security Incident Response Capability (CSIRC), NIST, noviembre de 1991.

– "The Oxford Reference Dictionary"; Oxford University Press, 1986.

– A Common Language for Computer Security Incidents; John D. Howard and Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667].

– Intrusion Detection – Network Security Beyond The Firewall, Terry Escamilla.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	**Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos**
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2004