Unión Internacional de Telecomunicaciones

Guía de ciberseguridad para los países en desarrollo

Edición 2007

Union internationale des télécommunications

Las denominaciones y clasificaciones empleadas en el presente Informe no suponen manifestación de opinión alguna por parte de la Unión Internacional de Telecomunicaciones sobre el estatus jurídico o de otra naturaleza de ningún territorio, ni la aceptación ni aprobación de ninguna frontera. La palabra «país» utilizada en el presente Informe designa un país o territorio.

Cláusula de exención de responsabilidad

Las referencias a países, sociedades, productos, iniciativas y directivas específicas no implican su aprobación ni recomendación por parte de la UIT con preferencia a otros de naturaleza similar que no se hayan mencionado. Las opiniones expresadas en esta publicación son las del autor y no son vinculantes para la UIT.

PREFACIO

La Cumbre Mundial sobre la Sociedad de la Información en sus fases de Ginebra y Túnez congregó a organizaciones, Gobiernos, empresas y la sociedad civil para acordar una visión común de la sociedad de la información.

Sin embargo, esta visión común sólo podrá hacerse realidad para todos los pueblos del mundo si conseguimos efectuar transacciones en línea con seguridad, proteger las infraestructuras críticas de información y salvaguardar los sistemas de información y los datos de los que dependen las empresas, los ciudadanos y los Gobiernos.

Entre los retos que debemos afrontar todos juntos podemos destacar la inadecuación de ciertas soluciones de ciberseguridad, la falta de consenso sobre las cuestiones que se plantean y la necesidad de abordar este problema a nivel mundial.

La Unión Internacional de Telecomunicaciones (UIT) como moderadora/facilitadora para la Línea de Acción C.5 de la CMSI – *Creación de confianza y seguridad en la utilización de las TIC* se ha comprometido a trabajar con todas las partes interesadas a fin de alcanzar un entendimiento común de los retos que se nos plantean y utilizar conjuntamente nuestros recursos para construir un marco mundial de seguridad y confianza.

Les invito a todos ustedes a que trabajen con nosotros para que esta visión de la creación de una sociedad de la información mundial y segura llegue a ser una realidad.

Dr Hamadoun I. Touré

Secretario General
Unión Internacional de Telecomunicaciones

PREÁMBULO

El nacimiento de una nueva sociedad mundial de la información sin fronteras supone la aparición de nuevas oportunidades para todos los países del mundo. Esto se debe a la creciente importancia de la tecnología en el desarrollo social y económico. Las aplicaciones de las TIC han hecho posible la creación de nuevos servicios en el ámbito de la sanidad, la educación, la empresa, las finanzas y la administración pública.

Por otra parte, las TIC presentan nuevos retos que deben afrontarse para poder realizar con seguridad transacciones en el ámbito de la cibersalud, para que los ciudadanos puedan acceder a los servicios de la ciberadministración, para ofrecer la necesaria confianza en la ejecución de las transacciones comerciales y empresariales en línea y para mantener la integridad de los sistemas y recursos que utilizamos en el marco de la tecnología de la información.

La implantación de soluciones adecuadas de seguridad y confianza constituye por tanto uno de los principales retos para la Oficina de Desarrollo de las Telecomunicaciones de la UIT en su empeño por ayudar a los países a explotar los recursos de telecomunicaciones y de las TIC.

El carácter transfronterizo de la sociedad de la información supone además que la búsqueda de soluciones pase por el entendimiento común entre todas las naciones de las posibilidades de las aplicaciones TIC seguras y de los retos que plantea la creación de confianza en la seguridad. Por consiguiente, resulta indispensable que además de dedicar nuestros esfuerzos a la reducción de la brecha digital, nos esforcemos en acortar el desnivel de conocimientos mediante la formación de una conciencia básica y la creación de capacidades humanas e institucionales.

Esta Guía tiene por objeto ofrecer a los países en desarrollo una herramienta que les permitirá alcanzar una comprensión más profunda de las cuestiones que afectan a la seguridad de las TI, presentarles ejemplos de soluciones aplicadas por otros países para resolver estos problemas. Se citan asimismo otras publicaciones que contienen información específica adicional sobre ciberseguridad. Esta Guía no pretende ser un documento exhaustivo ni un informe sobre la materia, sino un resumen de los principales problemas que existen hoy en día en los países que desean aprovechar las ventajas de la sociedad de la información.

El contenido de esta Guía se ha seleccionado teniendo en cuenta las necesidades de los países en desarrollo, especialmente de los menos adelantados, en lo que se refiere a la utilización de las tecnologías de la información y las comunicaciones para la prestación de servicios básicos en diversos sectores, sin perjuicio del compromiso con el desarrollo del potencial local y el fomento de la concienciación entre todas las partes interesadas.

Para evitar repetir la exposición de estos temas, en la elaboración del contenido de la presente publicación se han tenido en cuenta los trabajos realizados previamente en el seno de la Comisión de Estudio 17 del UIT-T, así como otros estudios y publicaciones existentes en este ámbito.

Sami Al Basheer Al Morshid

Director de la Oficina de Desarrollo
de las Telecomunicaciones

RESUMEN

Con independencia del aspecto que se considere, ya sea el social, el económico, el político o el de las cuestiones que atañen a la persona, y de su denominación, ya sea ésta seguridad de la informática y de las telecomunicaciones o ciberseguridad, la seguridad de la información afecta a la del patrimonio digital y cultural de los individuos, organizaciones y países. Los problemas aparejados son complejos y su resolución exige una voluntad política de diseño e implementación de un plan de desarrollo de infraestructuras y servicios digitales (ciberservicios) que comprenda una estrategia multidisciplinar de la ciberseguridad coherente, eficaz y controlable.

La obtención de un nivel de seguridad informática suficiente para prevenir los riesgos tecnológicos e informáticos es esencial para el adecuado funcionamiento de los Estados y de las organizaciones. La adopción de las tecnologías digitales va acompañada del aumento de la dependencia de las mismas y de la interdependencia de infraestructuras críticas. Esto crea una vulnerabilidad nada despreciable en el funcionamiento de las instituciones, lo que supone un peligro potencial para las mismas llegando a menoscabar la propia soberanía del Estado.

El objetivo de la ciberseguridad es contribuir a la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos e informativos, adquiridos por las instituciones, para realizar sus objetivos. La finalidad de la seguridad informática es conseguir que ningún perjuicio pueda poner en peligro su perpetuidad. Para ello se tratará de reducir la probabilidad de materialización de las amenazas; limitando los daños o averías resultantes; y logrando que se reanuden las operaciones normales tras un incidente de seguridad, en un plazo de tiempo razonable y a un coste aceptable.

El proceso de ciberseguridad alcanza a toda la sociedad, en la medida en que todos los individuos están afectados en mayor o menor medida por su implementación. Puede facilitarse su aplicación desarrollando un cibercódigo de conducta para la utilización adecuada de las TIC y promulgando una política de seguridad genuina en la que se definan las normas que se espera cumplan los usuarios de la ciberseguridad (partes interesadas, socios y proveedores).

Al plantear el proceso de ciberseguridad es importante identificar correctamente los activos y recursos que han de protegerse, para poder definir con precisión el alcance de la seguridad para que la protección sea eficaz. Esto exige un planteamiento global de la seguridad, a la vez multidisciplinar y exhaustivo. La ciberseguridad es incompatible con un mundo anárquico, lábil e incontrolado. Hace falta un conjunto de principios fundamentales de comportamiento ético, responsabilidad y transparencia, integrado en el oportuno marco legal y un cuerpo pragmático de procedimientos y normas. Éstos deben aplicarse a nivel local, naturalmente, aunque su aplicación debe extenderse asimismo a la comunidad internacional y ser compatible con las directivas internacionales existentes.

Para evitar dar oportunidades al incremento de la delincuencia, las infraestructuras de telecomunicaciones existentes deben contar con medidas de seguridad adecuadas de naturaleza tanto técnica como jurídica. Los ataques procedentes del ciberespacio pueden adoptar diversas formas: el secuestro clandestino de un sistema, la denegación de servicio, la destrucción o robo de datos sensibles, la piratería de las redes de telecomunicaciones (*hacking*), la penetración en la protección de los programas informáticos (*cracking*) y la manipulación fraudulenta de las conexiones telefónicas (*phreaking*) (entre las que se encuentran entre otros el sabotaje y secuestro de las centrales telefónicas); todos ellos tienen consecuencias negativas para las organizaciones e individuos que los padecen.

Las telecomunicaciones consideradas como sistema (es decir tanto las infraestructuras como los servicios) plantean un problema de seguridad muy semejante al de los recursos informáticos, por lo que su resolución debe responder a los mismos imperativos de orden técnico, organizativo y humano. La protección de la información durante su transmisión es necesaria aunque no suficiente, ya que su vulnerabilidad se mantiene, e incluso aumenta, durante las fases de procesamiento y almacenamiento.

Así pues la ciberseguridad debe contemplarse desde una perspectiva integradora. Las soluciones de seguridad puramente técnicas no pueden compensar la falta de una gestión coherente y rigurosa de las necesidades, medidas, procedimientos y herramientas de seguridad. La proliferación desordenada de herramientas de seguridad dificultará su uso, complicará su explotación y degradará la calidad de funcionamiento de los sistemas informáticos. La seguridad informática es una cuestión de gestión, de modo que las herramientas y servicios asociados están relacionados con la administración operacional de los sistemas. Por ejemplo, la encriptación de los datos para protegerlos durante la transmisión carece de sentido si a continuación se almacenan de un modo no seguro. Análogamente, la instalación de un cortafuegos tendrá poca utilidad si se permite que las conexiones puedan obviar este sistema.

El desarrollo de actividades basadas en el proceso de información encaminadas a reducir la brecha digital exigirán:

- infraestructuras de información fiables y seguras (con accesibilidad, disponibilidad, fiabilidad y continuidad de servicios garantizada);
- políticas orientadas a la creación de confianza;
- un marco jurídico adecuado;
- autoridades políticas y jurídicas versadas en las nuevas tecnologías y capaces de cooperar con sus homólogos de otros países;
- herramientas de gestión del riesgo y seguridad de la información;
- herramientas de seguridad que despierten la confianza en las aplicaciones y servicios ofrecidos (transacciones comerciales y financieras, cibersalud, cibergobierno, ciberelecciones, etc.) y en procedimientos de salvaguarda de los derechos humanos, especialmente los de protección de datos personales.

La buena administración de los activos de información digital, la distribución de bienes intangibles, la explotación de contenidos y la reducción de la brecha digital constituyen ejemplos de problemas económicos y sociales que no pueden abordarse considerando exclusivamente el aspecto tecnológico de la seguridad informática. Una respuesta que tenga en cuenta las dimensiones humanas, legales, económicas y tecnológicas de las necesidades de seguridad de la infraestructura digital y de los usuarios puede contribuir a acrecentar la confianza e inducir un crecimiento económico que beneficie a toda la sociedad.

ESTRUCTURA DE ESTA GUÍA

Esta Guía ofrece una introducción a la ciberseguridad en la que se destacan los cambios provocados por las tecnologías digitales, la desmaterialización de la información y la profusión de las redes de telecomunicaciones. Se presentan ordenadamente las cuestiones de interés para la evolución de la sociedad a fin de introducir el concepto de imperativo de seguridad en la informática y en las telecomunicaciones (ciberseguridad).

La Sección I de este manual se centra en las necesidades de la ciberseguridad y bosqueja los elementos sobre los que se basarán las soluciones. Se analiza el concepto de seguridad de las infraestructuras de comunicación en el marco de las vulnerabilidades observadas y de la situación de inseguridad propia de las tecnologías de la información y las comunicaciones. Aprovechando los conocimientos extraídos del examen de las mejores prácticas, de la realidad cotidiana de la seguridad en Internet y de la experiencia adquirida por la comunidad internacional, se identifican las necesidades específicas de la ciberseguridad en los países en desarrollo.

Se analizan las dimensiones administrativa, política, económica, social, jurídica y tecnológica de la ciberseguridad. Se formulan recomendaciones genéricas para el acceso a las infraestructuras de telecomunicaciones con miras a controlar los riesgos – ya sean de origen delictivo o no – y a alimentar la confianza en los ciberservicios, que constituyen uno de los motores más importantes del desarrollo económico.

La Sección II trata de la problemática del control de la ciberdelincuencia. Se consideran los elementos que favorecen las actividades delictivas a fin de mostrar las limitaciones de las actuales soluciones de seguridad y lucha contra el delito cibernético, así como la complejidad y escala de los problemas que se plantean.

Se enumeran las diversas infracciones y delitos que pueden perpetrarse a través de Internet, haciendo hincapié en los delitos de carácter económico. Se analizan los comportamientos delictivos, el perfil de los ciberdelincuentes y las características genéricas de los ciberataques y de los programas informáticos maliciosos. Se definen pautas para hacer frente a la amenaza de la ciberdelincuencia.

En la Sección III se revisan algunos de los principios fundamentales del mundo de las telecomunicaciones y se plantea una solución funcional y un análisis crítico de las herramientas de seguridad de las infraestructuras.

La Sección IV presenta un planteamiento global de la ciberseguridad que integra los diferentes aspectos jurídicos de las tecnologías modernas y ofrece ciertas perspectivas de desarrollo para la aplicación de soluciones de seguridad a las infraestructuras de comunicación.

Al final de esta Guía de Ciberseguridad el lector encontrará un glosario de términos de seguridad y un conjunto de referencias y otros documentos de interés.

AGRADECIMIENTO

La Oficina de Desarrollo de las Telecomunicaciones de la UIT desea manifestar su agradecimiento por la colaboración de la Sra. Solange Ghernaouti–Hélie y de todos los miembros de su equipo, especialmente de Mohamed Ali Sfaxi, Igli Tashi, Sarra Ben Lagha, Hend Madhour y Arnaud Dufour (consultor de estrategias de Internet).

Este Manual se ha elaborado a partir de la información y estudios suministrados por varios organismos, especialmente por «Clusif» (Club de la sécurité informatique français) y «Cert» (*Computer Emergency and Response Team*), que merecen nuestra gratitud más sincera.

Este Manual nunca habría visto la luz sin la magnífica cooperación de los miembros de la Unidad de Ciberestrategias de la UIT, y especialmente del Sr. Alexander Ntoko. Deseamos asimismo manifestar nuestro reconocimiento a la Sra. Renée Zbinden Mocellin (División de Producción de Publicaciones de la UIT) y a su equipo, por su esfuerzo en la preparación de esta Guía.

ÍNDICE

Page

SECCIÓN I

CONTEXTO DE LA CIBERSEGURIDAD
RETOS Y SOLUCIONES

Capítulo I.1 – El ciberespacio y la sociedad de la información

I.1.1 La digitalización

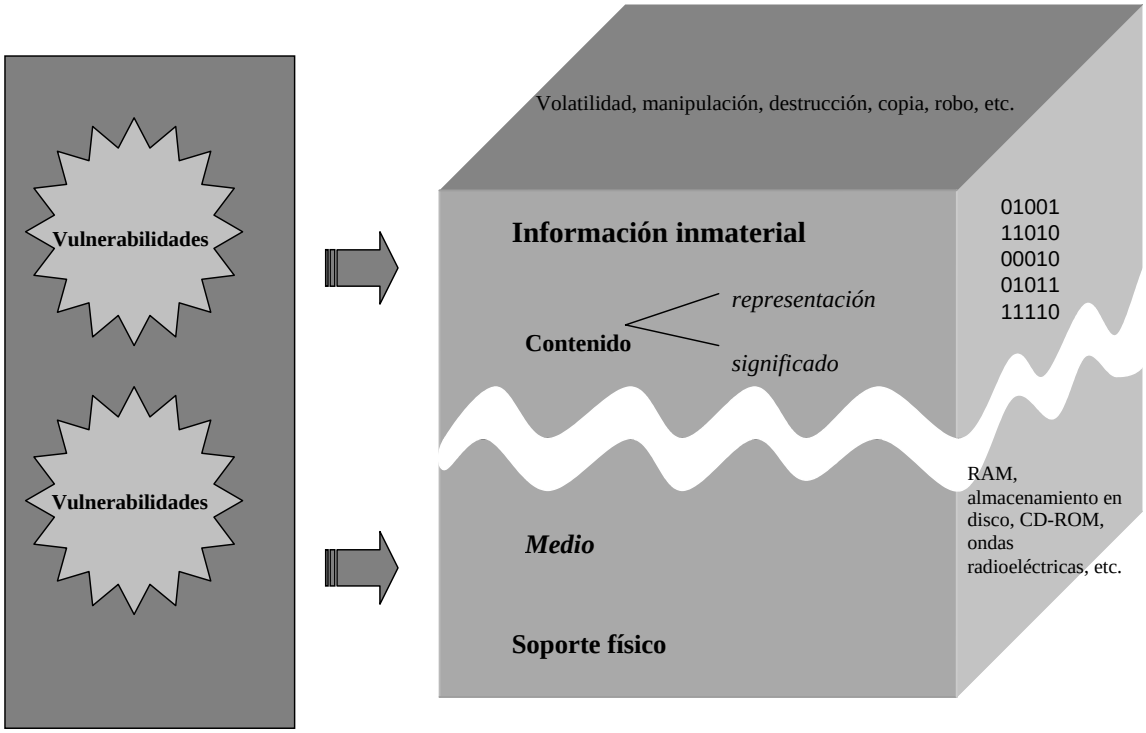
Las tecnologías informáticas transforman nuestra manera de pensar y actuar en cualquier aspecto de nuestras vidas, introduciendo importantes cambios estructurales, al permitirnos modelar *objetos* de todo tipo en forma de información, permitiendo de este modo su manipulación por medios electrónicos.

I.1.1.1 La información digital

La técnica de la digitalización permite crear una imagen digital o copia virtual de las entidades existentes. Independientemente de su naturaleza (voz, datos, imágenes), toda información es digitalizable y se puede representar de un modo homogéneo y uniforme.

La información ya no está asociada físicamente a su contenido, o sea a su soporte de representación y almacenamiento. Su valor añadido proviene directamente de la propia información (de su contenido), porque cuesta mucho menos compartirla y almacenarla que producirla (Figura I.1). Además, los datos pueden localizarse y procesarse simultáneamente en diversos puntos. La posibilidad de duplicación perfecta *ad infinitum* hace que el concepto de datos «originales» carezca de sentido, lo que puede plantear problemas para el concepto de protección de los derechos de autor.

Figura I.1 – Desmaterialización e información digital



I.1.1.2 La tecnología digital

La tecnología digital, ha permitido, gracias a la normalización de la producción, procesamiento y transferencia de los datos, la construcción de una cadena continua de información digital. Esta convergencia digital crea, junto con las técnicas de compresión de datos, oportunidades de sinergias entre la informática, las telecomunicaciones y los medios audiovisuales, de lo que es ejemplo patente el fenómeno de Internet. De este modo la revolución tecnológica real ha sido posible gracias a la digitalización de la información, y sus consecuencias sobrepasan los límites del mundo de la tele-comunicación.

Esta nueva dimensión del procesamiento de la información repercute en todas las áreas de la actividad humana y de su trabajo. En los últimos años se ha producido una evolución tanto de la determinación del valor como de los modos de producción. Esto ha dado lugar a la reorganización de las cadenas de valor entre los distintos agentes económicos.

I.1.1.3 Las infraestructuras y los contenidos

El control de la cadena de información digital, es decir de la infraestructura y del contenido, se ha convertido en el reto más importante del siglo XXI. El nuevo mercado, abierto a todos, se caracteriza por una movilización sin precedentes de todos los agentes de la economía mundial: operadores de telecomunicación, operadores de cable, fabricantes de hardware y de software, emisoras de televisión, etc.

El nuevo reto económico para las organizaciones de hoy lo constituyen la competencia desenfrenada y la redistribución de los ámbitos de actividad y de las funciones.

Cuando Gutenberg imprimió el primer libro, no pudo imaginar ni por un momento las repercusiones industriales que su invento tendría y que, a la sazón, fue el primer paso en el camino hacia la automatización industrial. Algo análogo ocurrió, a finales de los años 1960, cuando las universidades y los órganos de la Defensa, guiados cada uno de ellos por sus propias motivaciones y objetivos, aparentemente en conflicto, comenzaron a crear la red de comunicaciones que en su momento se convirtió en Internet. Como sus antecesores del siglo XV, actuaron sin ser plenamente conscientes de las consecuencias de su creación. Hoy en día, el ciberespacio anuncia la transición de la sociedad a la era de la información.

I.1.2 La revolución de la información

La revolución de la información altera en profundidad el modo de tratamiento y almacenamiento de la información. Modifica la forma en que las organizaciones, y por supuesto la sociedad en conjunto, funcionan. Aunque no se trata de la única innovación técnica ocurrida en los últimos años, reviste especial importancia por su repercusión sobre el proceso de la información y por tanto del conocimiento. Su repercusión afecta a los mecanismos de generación y transmisión del saber, por lo que cabe considerar la revolución de la información como motor de innovación en el futuro, de la que los países en desarrollo no deberían quedar excluidos en ningún caso.

La evolución de las tecnologías de la información y de la telecomunicación desemboca en una auténtica revolución de nuestro modo de pensar acerca de los intercambios económicos, sociales y culturales. Asimismo nos ofrece un nuevo modelo informático centrado en la red, en el que hay que garantizar la seguridad del flujo de la información para que se puedan desarrollar nuevas aplicaciones que incrementen la eficacia de las organizaciones. Ninguna forma de actividad económica puede subsistir sin que se produzcan intercambios e interacciones entre los diversos componentes; no es posible ningún intercambio de información sin ciertas garantías básicas de seguridad y no es posible plantear ningún servicio sin tener en cuenta la calidad del mismo. No obstante, debemos tener en cuenta que el éxito de una comunicación depende de la capacidad de dominio de las restricciones técnicas por parte de los interlocutores y de la gestión de las reglas propias de cualquier intercambio de información.

I.1.2.1 Innovación y desarrollo

Las organizaciones y los Estados deben esforzarse por adquirir capacidades de innovación y de adaptación rápidas, respaldadas por sistemas de información potentes y seguros, si desean sobrevivir y afirmarse como protagonistas en el nuevo entorno competitivo.

La diversificación de las telecomunicaciones y las posibilidades creadas por el desarrollo de la informática están abriendo nuevos ámbitos de actividad, de lo que deben beneficiarse también los países en desarrollo.

Las mejoras tecnológicas y económicas que han hecho posible el desarrollo de infraestructuras informáticas fiables permiten albergar grandes esperanzas para el ciudadano de a pie. Sin embargo, también introducen un grado de complejidad tecnológica y de gestión sin precedentes. Es necesario controlar los importantes riesgos asociados, de lo contrario dejaría de tener sentido la propia idea de evolución. El riesgo tecnológico, por ejemplo una avería de los sistemas de procesamiento de información y de las comunicaciones, provocada por un fallo de funcionamiento accidental o provocado, lleva aparejado un riesgo para el sistema de información, que puede socavar la capacidad de una organización para utilizar la información.

Un punto importante a destacar es que a pesar de que el acceso a la informática se ha generalizado y sigue creciendo, una parte nada despreciable de la población sigue ajena a la revolución informática. Los motivos por los que esto ocurre son complejos y entre ellos se cuentan factores culturales y financieros así como, en ciertos casos, problemas básicos tales como el analfabetismo. La formación y la educación son indispensables, más aquí que en cualquier otro dominio, para democratizar la tecnología de la información y combatir la infoexclusión. Será necesario replantear también las interfaces de comunicación para poder atender mejor a la población y respetar la diversidad de los contextos culturales. Los ordenadores deben adaptarse al entorno humano en el que se integran, en vez de dictar un nuevo orden en las comunicaciones.

I.1.2.2 Soporte de la revolución de la información

Las tecnologías de la información y de la comunicación, como cualquier otra técnica, se conciben y aplican en un espacio temporal y geográfico determinado, reflejando normalmente un cierto equilibrio de la sociedad. Es responsabilidad de las personas apoyar la revolución de la información dotándola de herramientas, procedimientos, legislación y una ética de seguridad que satisfaga su realización y corresponda a las expectativas y necesidades de la sociedad.

No puede negarse el hecho de la existencia de una multiplicidad de reglamentaciones incompletas de la UIT (Unión Internacional de Telecomunicaciones), la UNESCO, la ONU, la OCDE, el Consejo de Europa, etc. sobre utilización de los diferentes medios de comunicación y sobre la libertad de emisión y recepción de mensajes. Se ha generado un desfase importante entre la situación actual de desarrollo y grado de implementación de las tecnologías de la información y las comunicaciones, y el estado de los reglamentos. Debe elaborarse un marco jurídico apropiado que tenga en cuenta principalmente la desvinculación territorial de las redes como Internet y los problemas de responsabilidad, de respeto de la vida privada y de la propiedad. La evolución tecnológica debe asociarse a otra de orden social, político y jurídico. Estas someras consideraciones sobre la era de la información bastan para poner de manifiesto la importancia de las cuestiones de su control, del papel preponderante de las telecomunicaciones en su realización y de una necesidad de seguridad que no debe suponer un freno al desarrollo.

El paso a la era de la información refleja la importancia de las tecnologías de la información y de su control. Al considerar las nuevas dimensiones que estas tecnologías introducen en el plano técnico y en el socioeconómico, se pone de manifiesto la importancia primordial que adquiere la necesidad de garantizar la seguridad de los sistemas e infraestructuras informáticos y de telecomunicaciones. Esto destaca el carácter estratégico y crítico de la gestión y puesta en práctica de la ciberseguridad, tanto para los Estados y las organizaciones como para el individuo.

La importancia de los esfuerzos financieros, materiales y humanos de los Estados para crear su infraestructura informática y de telecomunicaciones, determinará la de que se doten de medios que permitan asegurarla, administrarla y controlarla.

Capítulo I.2 – La ciberseguridad

I.2.1 Contexto de seguridad de las infraestructuras de comunicación

Estamos asistiendo hoy en día a una concienciación creciente de la necesidad de controlar los riesgos informáticos operacionales debido a la utilización extensiva de las nuevas tecnologías, a la existencia de una infraestructura de información mundial y a la aparición de nuevos riesgos.

La transformación de las sociedades en sociedades de la información, gracias a la integración de nuevas tecnologías en todas sus actividades e infraestructuras, aumenta la dependencia de los individuos, de las organizaciones y de los Estados, de los sistemas de información y de las redes. Esto constituye un riesgo de primer orden que debe contemplarse como un riesgo de seguridad.

Los países en desarrollo se enfrentan a la necesidad de formar parte de la sociedad de la información asumiendo el riesgo de su dependencia de las tecnologías y de los proveedores de las mismas intentando que la brecha digital existente no dé lugar a una brecha de seguridad y menos aún a una dependencia más estrecha de entidades que controlen sus necesidades y los medios de seguridad de las tecnologías de la información[1].

Las infraestructuras de telecomunicaciones y los servicios y actividades que éstas permiten desarrollar y generar, deben plantearse, concebirse, instalarse y administrarse en términos de seguridad. La seguridad es la piedra angular de toda actividad y debe contemplarse como un servicio que permite crear otros y generar valor añadido (cibergobierno, cibersalud, ciberenseñanza, etc.) con independencia de las tecnologías[2]. Sin embargo, hasta el momento, las herramientas básicas de comunicación disponibles no cuentan con los medios suficientes ni necesarios para establecer o garantizar un nivel mínimo de seguridad.

Los sistemas informáticos conectados en red son recursos accesibles a distancia y blancos potenciales de ataques informáticos. Esto incrementa los riesgos de intrusión en los sistemas y ofrece un terreno favorable para la realización y propagación de ataques y delitos. Lo que realmente se busca es la información que se encuentra en los sistemas atacados (Figura I.2). Los ataques pueden afectar a la capacidad de tratamiento, salvaguarda y comunicación del capital de información, de los valores y materiales y de los símbolos, y al proceso de producción o de decisión de los que los poseen. Los sistemas informáticos introducen un riesgo operacional en el funcionamiento de las instituciones que los poseen.

Así pues, las redes de telecomunicaciones y la apertura de los sistemas plantean problemas de seguridad informática, complejos y multiformes, que son relativamente difíciles de controlar y que pueden tener consecuencias y repercusiones críticas sobre el funcionamiento de las organizaciones y de los Estados. De la capacidad de controlar la seguridad de las informaciones, de los procesos, de los sistemas, y de las infraestructuras dependen los factores críticos de éxito de las economías.

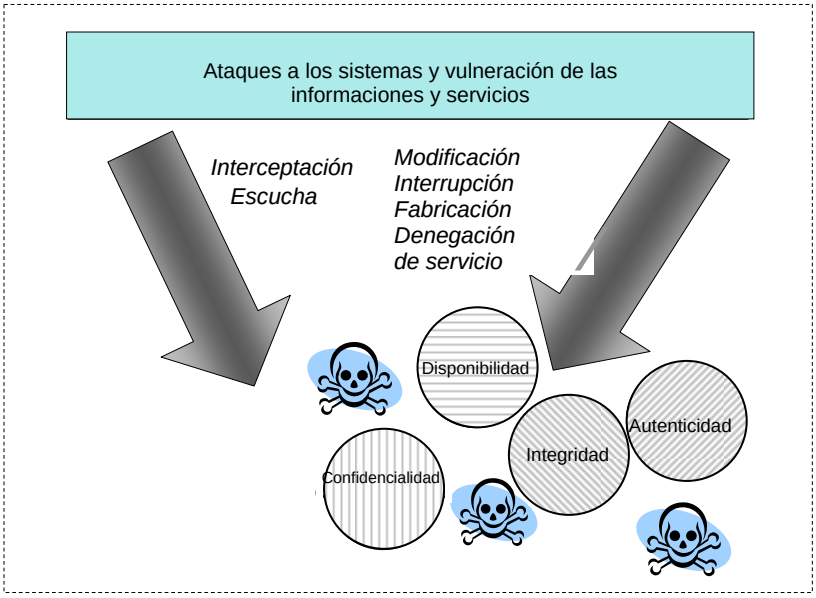
La interconexión extensiva de sistemas, la interdependencia de las infraestructuras, el aumento de la dependencia de las tecnologías digitales, las amenazas y los riesgos, exigen dotar a los individuos, las organizaciones y los Estados de medidas, procedimientos y herramientas que permitan mejorar la gestión de los riesgos tecnológicos y de la información. Los retos del dominio de los riesgos tecnológicos son propios del siglo XXI y exigen un planteamiento global a nivel internacional y su integración en el proceso de la seguridad de los países en desarrollo.

---

1 S. Ghernaouti-Hélie: «From digital divide to digital unsecurity: challenges to developp and deploy a unified e-security framework in a multidimensional context». International cooperation and the Information Society, Capítulo del Anuario Suizo de Política de Desarrollo. Iuéd publications. Ginebra, Noviembre de 2003.

2 A. Ntoko: «Mandate and activities in cybersecurity – ITU-D». Reunión temática de la CMSI sobre ciberseguridad. UIT – Ginebra, 28 de junio a 1 de julio de 2005.

Figura I.2 – Ataques a los sistemas y vulneración de la seguridad de los recursos



No basta con establecer puntos de acceso a las redes de telecomunicación, es indispensable desplegar infraestructuras y servicios informáticos fiables, susceptibles de mantenimiento, robustos y seguros, para respetar los derechos fundamentales de las personas y de los Estados. La protección de los sistemas y de la información de valor debe complementarse y armonizarse con la protección de los individuos y de su intimidad digital (*privacidad*).

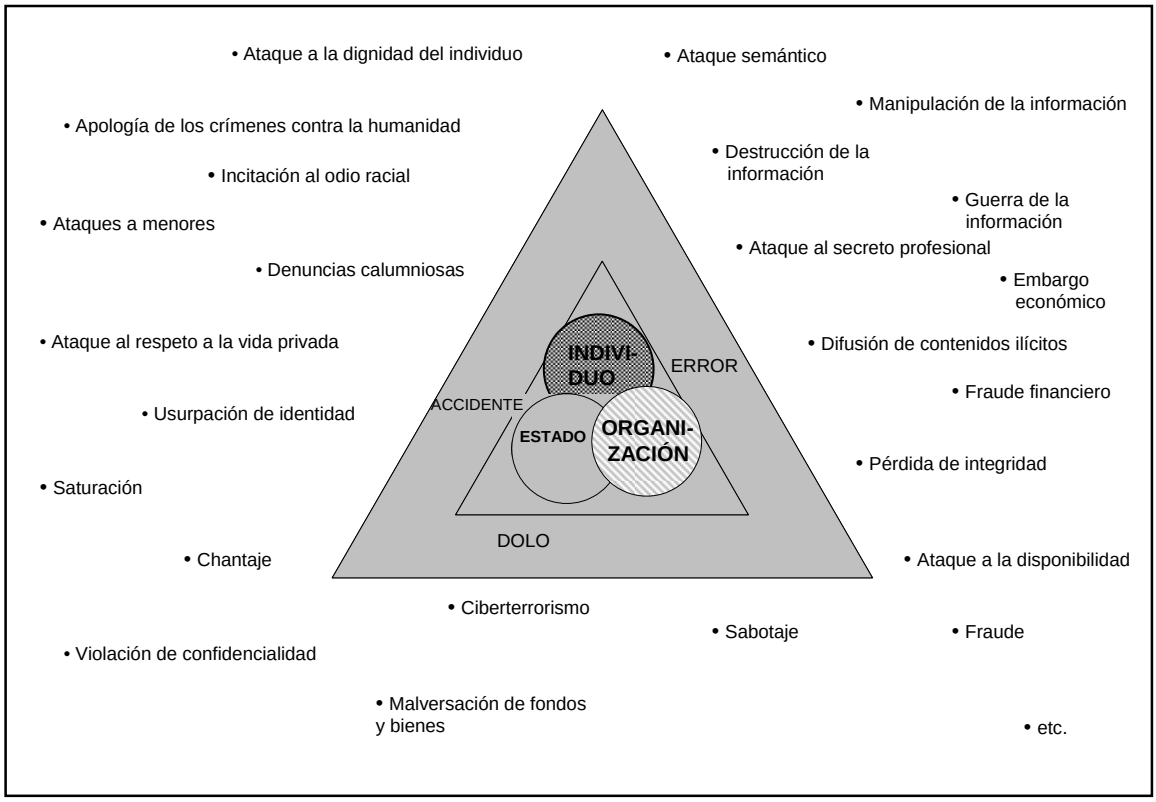
La entrada en la sociedad de la información sin un riesgo excesivo y aprovechando las experiencias obtenidas de los países en desarrollo, sin que la ciberseguridad se convierta en un factor adicional de exclusión, constituye un nuevos reto para los países en desarrollo.

I.2.2 Retos de la ciberseguridad

Se plantean retos de orden social, económico, político y humano. Con independencia de que se denomine seguridad de la informática y de las telecomunicaciones o ciberseguridad, la seguridad de la información afecta a la seguridad del patrimonio digital y cultural de los individuos, las organizaciones y las naciones (Figura I.3). Hay retos complejos cuya satisfacción exige la voluntad política de definir y realizar una estrategia de desarrollo de las infraestructuras y servicios digitales (ciberservicios) que integre una estrategia de ciberseguridad coherente, eficaz y controlable. Ésta debe inscribirse en una solución multidisciplinar, y deben aplicarse soluciones de orden educativo, jurídico, administrativo y técnico. De este modo, al ofrecer una respuesta adecuada a las dimensiones humana, jurídica, económica y tecnológica de las necesidades de seguridad de las infraestructuras digitales, puede generarse confianza y poner en marcha un desarrollo económico provechoso para todos los agentes sociales.

El control del patrimonio digital de la información, la distribución de los bienes intangibles, la valorización de los contenidos y la reducción de la brecha digital, por ejemplo, son problemas de orden económico y social cuya resolución no puede limitarse exclusivamente a la dimensión tecnológica de la seguridad informática.

Figura I.3 – Los distintos niveles de la ciberseguridad: los individuos, las organizaciones y los Estados



El desarrollo de las actividades basadas en el procesamiento de la información y encaminadas a reducir la brecha digital, exige lo siguiente:

- infraestructuras de información fiables y seguras (garantía de accesibilidad, disponibilidad, seguridad de funcionamiento y continuidad de los servicios);
- políticas de creación de confianza;
- un marco legal adaptado;
- instancias jurídicas y policiales competentes en el dominio de las nuevas tecnologías y capaces de cooperar a nivel internacional con sus homólogos;
- herramientas de gestión del riesgo de la información y de la gestión de la seguridad;
- herramientas de implementación de la seguridad que permitan infundir confianza en las aplicaciones y servicios ofrecidos (transacciones comerciales y financieras, cibersalud, ciber-gobierno, ciberelecciones, etc.) y en los procedimientos, sin perjuicio del respeto a los derechos del hombre, especialmente en lo referente a los datos de carácter personal.

El objetivo de la ciberseguridad es contribuir a preservar las fuerzas y medios organizativos, humanos, financieros, tecnológicos y de información, con las que cuentan las instituciones, para alcanzar sus objetivos.

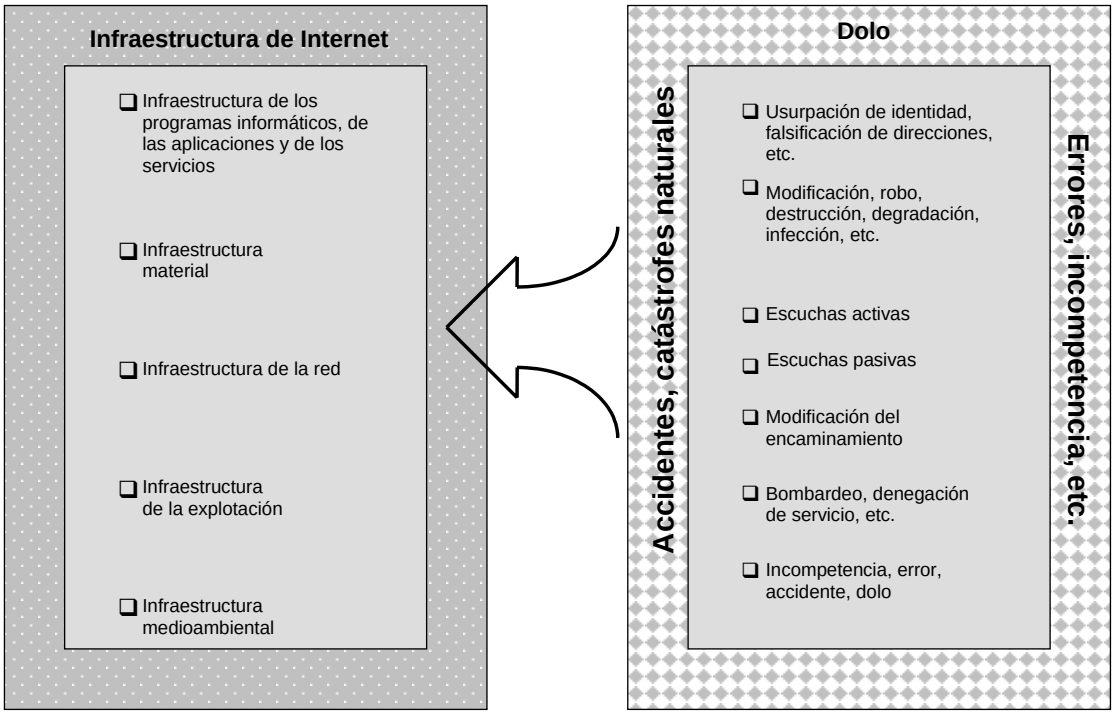
La finalidad de la seguridad informática es garantizar que ningún perjuicio pueda poner en peligro la vida de la organización. Esto equivale a reducir la probabilidad de materialización de las amenazas, limitar los ataques y los problemas de funcionamiento inducidos y permitir la vuelta a la normalidad de funcionamiento tras un siniestro, a un coste aceptable y en un plazo razonable.

El proceso de la ciberseguridad es un proyecto de la sociedad en la medida en que todos los individuos están afectados por su realización. Su validez quedará reforzada si se desarrolla una ciberética de utilización y de comportamiento en relación con las tecnologías de la información y si existe una verdadera política de seguridad que estipule sus exigencias de seguridad frente a los usuarios, agentes, asociados y proveedores de seguridad de las nuevas tecnologías.

I.2.3 Manifestación de la inseguridad digital

La inseguridad de las tecnologías de procesamiento de la información y de las comunicaciones tiene su origen en las características de las tecnologías de la información y del mundo virtual. La desmaterialización de los implicados, el acceso a distancia, el relativo anonimato, los problemas de concepción, de implementación, de gestión, de control de la informática y de las telecomunicaciones, asociados a las averías, los problemas de funcionamiento, errores, incompetencias, incoherencias e incluso a las catástrofes naturales, confieren *de hecho* un cierto nivel de inseguridad a las infraestructuras informáticas (Figura I.4).

Figura I.4 – Infraestructura de Internet y multiplicidad del origen de los problemas



En este contexto, las posibilidades de dolo y de explotación de estas vulnerabilidades son considerables[3].

La existencia de estos ataques: usurpación de identidad, burla de los sistemas, intrusión, secuestro de recursos, infección, deterioro, destrucción, manipulación, violación de confidencialidad, denegación de servicio, robo, extorsión, etc. – pone en evidencia las limitaciones de las soluciones de seguridad actuales, lo que refleja paradójicamente una cierta robustez de las infraestructuras.

Con independencia de los motivos de los agentes de la delincuencia informática, ésta tiene siempre consecuencias económicas nada despreciables y constituye, en su dimensión de cibercriminalidad, una amenaza creciente, internacional y compleja.

Las soluciones de seguridad existentes no tienen carácter universal y normalmente sólo resuelven un problema particular en una situación determinada; trasladan el problema de seguridad y transfieren la responsabilidad de seguridad. Además, necesitan asegurarse y administrarse de un modo protegido.

[3] La cibercriminalidad, los ciberataques y los ciberdelitos se exponen en la Sección II.

Es necesario aclarar que su respuesta a la dinámica del contexto en el que deben integrarse no es total. Estas tecnologías no son estables; los objetivos son móviles y los conocimientos de los delincuentes evolucionan como también lo hacen las amenazas y los riesgos. Esto hace que la vigencia de las soluciones de seguridad, y el retorno de la inversión en las mismas, no estén nunca garantizados.

En muchos casos la estrategia de seguridad se limita a la adopción de medidas de reducción de riesgos para las informaciones de valor de las organizaciones, normalmente con una única solución tecnológica. Sin embargo, el planteamiento de la seguridad debe contemplarse en todas sus dimensiones y satisfacer igualmente las necesidades de seguridad de los individuos, especialmente en lo que se refiere a la protección de su vida privada y al respeto de sus derechos fundamentales. La ciberseguridad debe estar disponible para todos y tener en cuenta la necesidad de protección de los datos de carácter personal.

Aunque existen soluciones de seguridad, suelen ser de carácter tecnológico y responder principalmente a un problema específico en una situación determinada. Sin embargo, como cualquier otra tecnología, son falibles y se pueden burlar. Suelen trasladar el problema de seguridad y la responsabilidad a otra entidad del sistema que se supone deben proteger. Además, necesitan ser protegidas y administradas de manera segura. Nunca son ni universales ni definitivas, por el carácter evolutivo del contexto de la seguridad como consecuencia de la dinámica del entorno (evolución de las necesidades, riesgos, tecnologías y conocimientos de los delincuentes, etc.). Esto plantea el problema de la vigencia de las soluciones aplicadas. Además, la diversidad y número de las soluciones existentes puede plantear el problema de la coherencia global de la solución de seguridad. Por consiguiente, no basta con disponer de la tecnología: hay que integrarla además en una estrategia de gestión.

La diversidad y pluralidad de los agentes (ingenieros, desarrolladores, auditores, integradores, juristas, investigadores, clientes, proveedores, usuarios, etc.), la diversidad de intereses, de visiones, de entornos y de idiomas dificultan la coherencia global de las medidas de seguridad. Por otra parte sólo la contemplación global y sistemática de los riesgos y de las medidas de seguridad, la asunción de la responsabilidad por parte de todos los protagonistas y participantes contribuirá a ofrecer el nivel de seguridad que cabe esperar para realizar confiadamente actividades utilizando las tecnologías de la información y las comunicaciones, y para tener confianza en la economía digital.

I.2.4 Conclusiones de orden práctico

I.2.4.1 Dirección de la seguridad

Desde principios de los años 2000, se ha generalizado la toma de conciencia de los problemas vinculados con la seguridad informática en las organizaciones, al menos en las grandes. La seguridad es cada vez menos una yuxtaposición de tecnologías heterogéneas de seguridad y debe contemplarse y administrarse como un proceso continuo.

El «gobierno» o «gobernanza» de la seguridad debe garantizar que las medidas de seguridad sean las óptimas en el espacio y el tiempo. Este concepto responde a los siguientes interrogantes simples:

- ¿Quién hace qué, cómo y cuándo?
- ¿Quiénes son los agentes que elaboran las reglas, las definen y las validan, quiénes las aplican y quiénes las controlan?

I.2.4.2 Identificación y gestión de los riesgos

La consideración del análisis de los riesgos vinculados a la informática, las telecomunicaciones y el ciberespacio, en un proceso de gestión de riesgos (*risk management*), inspira la estrategia de seguridad de las infraestructuras digitales. El riesgo de seguridad vinculado a las tecnologías de la información (riesgo informático, de información o tecnológico, no importa su denominación) debe identificarse en pie de igualdad con los demás riesgos (riesgo estratégico, social, medioambiental, etc.) que deben afrontar las instituciones.

El riesgo informático tiene carácter operacional y debe controlarse. La gestión de los riesgos constituye el punto de partida del análisis de las necesidades de seguridad, que permitirá definir la estrategia y la política de seguridad. Se plantean varias cuestiones entre las que cabe citar las siguientes:

- ¿Quién es el responsable del análisis de los riesgos y de la gestión de los mismos?
- ¿Cómo se lleva a cabo dicho análisis?
- ¿Cuáles son las herramientas y metodologías disponibles?
- ¿Cuál es el grado de fiabilidad de las mismas?
- ¿Qué importancia hay que otorgar a los resultados? ¿Cuál es su coste?
- ¿Es necesario subcontratar esta función?
- etc.

El riesgo es un peligro eventual, previsible en cierto grado, que se mide por la probabilidad de que se produzca y por las repercusiones y daños que puede provocar su materialización. El riesgo expresa la probabilidad de que un valor se pierda en función de una vulnerabilidad vinculada a una amenaza o a un peligro.

El compromiso entre el coste del riesgo y el de su reducción permite determinar el nivel de protección y las medidas de seguridad a aplicar (Figura I.5). En todo caso es necesario identificar los valores que han de protegerse y las razones para ello, en función de las limitaciones efectivas y de los medios organizativos, financieros, humanos y técnicos disponibles. Estas medidas deben ser eficaces e inscribirse en una lógica de optimización/rentabilidad.

Para cualquier organización, el control de los riesgos informáticos supone la concepción de una estrategia, la definición de una política de seguridad y su realización táctica y operacional.

Figura I.5 – Los diversos compromisos del control de los riesgos: una opción política

I.2.4.3 Definición de la política de seguridad

La política de seguridad permite traducir la percepción de los riesgos afrontados y de sus repercusiones, en medidas de seguridad a implementar. Facilita la adopción de una actitud preventiva y reactiva frente a los problemas de seguridad y permite reducir los riesgos y sus repercusiones.

Como no existe el riesgo nulo y es difícil prever todas las amenazas que se pueden presentar, hay que reducir la vulnerabilidad del entorno y de los recursos a proteger, ya que es evidente que una gran parte de los problemas de seguridad tienen su origen en ellos.

La política de seguridad especificará, entre otros, los medios, la organización, los procedimientos, los planes de defensa y de reacción que permitan controlar verdaderamente los riesgos operacionales, tecnológicos y de información.

La Norma ISO 17799 propone un código de buena conducta para la gestión de la seguridad. Esta norma puede contemplarse como un referencial que permite definir una política de seguridad, como una lista de elementos de riesgo a analizar (*lista de comprobación*), como una ayuda a la auditoría de seguridad, ya sea en el contexto de un procedimiento de certificación o no, e incluso como centro de comunicación sobre la seguridad. Se pueden realizar diversas interpretaciones e implementaciones de esta norma. Su interés reside en el hecho de que aborda los aspectos organizativo, humano, jurídico y tecnológico de la seguridad en relación con las distintas etapas de concepción, implementación y mantenimiento de la misma. En la versión de 2005 de esta norma (ISO/CEI 17799:2005)[4] se hace hincapié en la evaluación y el análisis de los riesgos, en la gestión de los valores y de los bienes y en la gestión de los incidentes. También se destaca la importancia otorgada a la dimensión de gestión de la seguridad.

Figura I.6 – La gestión de la seguridad pasa por la definición de una política de seguridad

Elementos de una política de seguridad	
Organización de la seguridad	¿Qué hay que proteger? ¿De quién? ¿De quién debe uno protegerse? ¿Por qué?
Asignación de responsabilidades a personas competentes que posean la autoridad y medios necesarios	¿Cuáles son los riesgos realmente enfrentados? ¿Son soportables estos riesgos?
Identificación de los objetivos de seguridad en cada dominio y componente del sistema de información	¿Cuál es el nivel actual de seguridad de la empresa? ¿Cuál es el nivel que se desea alcanzar?
Definición de las amenazas – Identificación de las vulnerabilidades	
Definición de las medidas de seguridad	¿Cuáles son las restricciones efectivas? ¿Cuáles los medios disponibles? ¿Cómo aplicarlos?
Definir los comportamientos de seguridad	

La eficacia de una política de seguridad no se mide por el presupuesto asignado ya que depende de la política de gestión del riesgo y de la calidad del análisis de los riesgos (Figura I.6). Los riesgos varían notablemente dependiendo del sector de actividad de la organización, de su magnitud, de su imagen, de la sensibilidad de los sistemas, de su entorno y de las amenazas asociadas, y de su grado de dependencia del sistema de información.

4 El índice de esta norma se presenta en el Anexo B de esta Guía.

La calidad de la seguridad informática depende ante todo de la identificación y de la evaluación del valor patrimonial de la información, de la implementación operacional de las medidas de seguridad adoptadas a partir de una definición correcta de la política de seguridad y de una gestión eficaz.

I.2.4.4 Implementación de las soluciones

Se pueden adoptar diversos tipos de medidas para contribuir a asegurar las infraestructuras informáticas y de telecomunicaciones. Entre ellas cabe citar las siguientes:

- educar, formar y concienciar a todos los agentes de la ciberseguridad;
- implementar estructuras que puedan funcionar como centro de alerta y de gestión de crisis a nivel nacional, agrupar los medios a implementar para utilizarlos y compartirlos para un conjunto de países o para una región;
- imponer sistemas de vigilancia y control (por analogía a los controles instalados en las carreteras);
- desarrollar las competencias de un equipo de ciberpolicía que pueda contribuir a la persecución e investigación de los delitos informáticos en el ámbito de la cooperación internacional;
- desarrollar soluciones tecnológicas en lo que se refiere a la gestión de identidades, el control de acceso, la utilización de plataformas materiales y de aplicaciones informáticas seguras, las infraestructuras de respaldo, los protocolos criptográficos y la gestión operacional.

I.2.5 El punto de vista de la gestión

I.2.5.1 La gestión dinámica[5]

El planteamiento de la seguridad en un proceso de gestión dinámico y continuo permite hacer frente al carácter dinámico del riesgo y a la evolución de las necesidades gracias a la adaptación y optimización continua de las soluciones. El nivel de seguridad ofrecido depende de la calidad de la gestión de la seguridad. La política de ciberseguridad se determina en la cúpula de mando de la estructura correspondiente. Hay tantas estrategias de seguridad, políticas de seguridad, medidas, procedimientos y soluciones de seguridad como organizaciones y necesidades de seguridad a satisfacer en un momento dado.

Como ejemplo de la dinámica del contexto en el que se inscribe la gestión de la seguridad cabe citar el proceso de descubrimiento y corrección de fallos de seguridad que se lleva a cabo mediante una publicación periódica de las medidas correctivas (*parches* de seguridad). Las circulares informativas (*newsletters*), personalizadas en cierta medida, permiten mantenerse al tanto de los fallos descubiertos y de la manera de remediarlos. Para mantener un cierto nivel de seguridad, el responsable de seguridad o el administrador de sistema, debe instalar los *parches* de seguridad conforme se van publicando. Aunque el conocimiento de los fallos y de las vulnerabilidades de los sistemas es indispensable para el responsable de la seguridad, también es cierto que facilita el trabajo de los malhechores que pueden explotarlos antes de que se corrijan. Resulta por tanto imperativo facilitar los medios de realización de una gestión dinámica que contribuya a la puesta al día de las soluciones de seguridad y al mantenimiento de la seguridad en el tiempo.

Si un sistema de publicación de parches como el descrito permite al administrador controlar el proceso de actualización (aceptar o no la instalación de los parches), el modo automatizado permite delegar implícitamente al editor la instalación periódica y sistemática de los parches. Esto plantea la cuestión del libre albedrío. ¿Cuáles son las consecuencias jurídicas de rechazar la actualización cuando aparecen problemas derivados de la explotación de un fallo no corregido? Dado que gran parte de los ataques se aprovechan de estas deficiencias, la cuestión del libre albedrío y de la responsabilidad del administrador del sistema resulta totalmente pertinente.

---

[5] Los puntos 5.1 y 5.2 son adaptaciones del artículo «Sécurité informatique, le piège de la dépendance» de A. Dufour y S. Ghernaouti-Hélie, Revue Information et Système, 2006.

La dimensión dinámica de la seguridad constituye un reto crítico tanto para los proveedores de soluciones y editores como para los administradores de sistemas y responsables de seguridad que rara vez tienen tiempo de integrar el conjunto de parches propuestos.

La capacidad de los responsables informáticos o de la seguridad y de los administradores de sistemas para acceder a todos los recursos informáticos implica además la integridad sin fallos de procedimientos estrictos de vigilancia y control de sus acciones (en proporción directa a los riesgos a los que someten potencialmente los sistemas que administran), y de su integridad moral.

I.2.5.2 Subcontratación y dependencia

Al ofrecer filtros contra los virus o contra el correo indeseado, los proveedores de servicios asumen una parte de la administración de la seguridad de sus clientes. Si se generaliza esta tendencia, se habrá iniciado una evolución del reparto de funciones y responsabilidades en materia de seguridad. La seguridad recae cada vez más en el proveedor de servicios y los intermediarios técnicos. Esta evolución no resuelve la problemática de la seguridad, ya que no hace más que trasladarla al proveedor de servicios que deberá no solamente garantizar la disponibilidad y la calidad del servicio sino también la gestión del mantenimiento de su nivel de seguridad.

Al ofrecer ciertos programas informáticos contra los virus, el editor ofrece igualmente un servicio de actualización automática. La adición de esta dimensión de servicio favorece el alquiler de los programas informáticos en la medida en que el editor deba mantenerlos durante su periodo de vigencia y contribuye además a alimentar la tendencia, cada vez más generalizada, a subcontratar las aplicaciones, con arreglo a un modelo económico que está aún por definir.

La cuestión de la subcontratación o de la delegación de toda la seguridad o de parte de ella, no viene planteada por la tecnología. Es de naturaleza estratégica y jurídica y plantea la cuestión fundamental de la dependencia de los proveedores.

La estrategia de subcontratación de la seguridad puede afectar a la definición de la política, a su aplicación, a la gestión del acceso, al cortafuegos (*firewall*), al telemantenimiento de los sistemas y de las redes, al mantenimiento de las aplicaciones informáticas por parte de terceros, a la gestión de las copias de seguridad, etc. La elección de un proveedor debe venir siempre amparada por un planteamiento de control de calidad que puede tener en cuenta, por ejemplo, la experiencia del proveedor, sus competencias internas, las tecnologías utilizadas, el tiempo de respuesta, el soporte de servicio, las cláusulas contractuales (garantía de resultados, etc.) y las responsabilidades legales compartidas.

I.2.5.3 Estrategia de prevención y respuestas[6]

La estrategia de prevención de la seguridad es, por definición, anticipada. Afecta a las dimensiones humana, jurídica, organizativa, económica (relación coste de implementación/nivel de servicio/ servicios ofrecidos) y tecnológica. Hasta el momento, en el planteamiento de la seguridad de los entornos informáticos, sólo se ha tenido en cuenta, mayoritariamente, la dimensión tecnológica. Esta manera de contemplar la seguridad informática, bajo un ángulo esencialmente tecnológico que ignora la dimensión humana, plantea un verdadero problema para el control del riesgo tecnológico de origen delictivo. En efecto, la delincuencia es ante todo una cuestión de personas y no de tecnologías, por lo que una respuesta de carácter exclusivamente tecnológico resulta inadecuada para el control de un riesgo de origen humano.

La represión de la delincuencia informática se inscribe sobre todo en una estrategia de respuesta y seguimiento que se efectúa *a posteriori*, es decir, tras la aparición del siniestro que pone de manifiesto el fallo de las medidas de protección. Resulta necesario prevenir los ciberabusos y disuadir a los que pueden cometerlos, desarrollando mecanismos legales y de investigación; también resulta

---

6 El punto 5.3 es una adaptación del libro «Sécurité informatique et réseaux» de S. Ghernaouti-Hélie, Dunod 2006.

indispensable identificar en las políticas de seguridad las medidas de respuesta a los ataques y las de persecución de sus autores. Para ello, es obligatorio concebir y realizar planes de contingencia y continuidad que tengan en cuenta las restricciones vinculadas a la investigación y persecución del delito informático, con filosofías de trabajo y objetivos diferentes, en diversas escalas temporales.

I.2.6 El punto de vista político

I.2.6.1 Responsabilidad del Estado

Sobre el Estado recaen responsabilidades importantes de realización de la seguridad digital. Esto es especialmente cierto en lo que se refiere a la definición de un marco legal adecuado, es decir unificado y aplicable. Además, no sólo se trata de favorecer y alentar la investigación y desarrollo en materia de seguridad sino también de promover una cultura de la seguridad e imponer el cumplimiento de unas normas mínimas de seguridad (la seguridad debería ser inherente a los productos y servicios), reforzando al mismo tiempo la lucha contra la delincuencia. Surge entonces la cuestión del modelo financiero subyacente a estas acciones y a la colaboración entre los sectores público y privado para la ejecución de planes de acción a nivel nacional e internacional.

A nivel estratégico, es preciso garantizar la prevención, la comunicación, la información compartida, y la gestión de alertas. Además, es necesario dar a conocer las prácticas óptimas para la gestión del riesgo y de la seguridad. Resulta igualmente importante garantizar la coordinación y la armonización de los sistemas legales. Hay que definir asimismo entre otras cuestiones, la asistencia para promover la seguridad y la protección, y las fórmulas de cooperación eventual (formal/informal, multilateral/ bilateral, activa/pasiva), tanto a nivel nacional como supranacional.

Resulta asimismo indispensable educar, informar y formar en las tecnologías del tratamiento de la información y de las comunicaciones y no solamente en la seguridad y en las medidas disuasorias. La sensibilización a los problemas de seguridad no debe limitarse a la promoción de una cierta cultura de la seguridad y de una ciberética. Además de la cultura de seguridad, debe haber una cultura de la informática.

Hay que dotar a los distintos implicados de medios para que aprendan a manejar los riesgos tecnológicos, operacionales y de información que les amenazan en función de su empleo de las nuevas tecnologías. En este contexto, el Estado debe fomentar además la denuncia de las agresiones vinculadas a los ciberdelitos e infundir confianza entre los distintos implicados del mundo económico por una parte y las instancias judiciales y policiales por otra.

Tanto las instancias judiciales y policiales, ya mencionadas, como los servicios de protección civil, los bomberos, las fuerzas armadas y las de seguridad desempeñan una misión tanto a nivel táctico como operacional en la lucha contra la delincuencia informática en funciones de protección, persecución y reparación. Debe haber centros de vigilancia, de detección y de información de los riesgos informáticos operacionales para garantizar la prevención necesaria para el control de estos riesgos.

Compete a los Estados la definición de una verdadera política de desarrollo de la sociedad de la información en función de sus valores propios y la aportación de los medios necesarios para ello. Esto concierne tanto a los medios de protección como a los de lucha contra la ciberdelincuencia.

Un control mundial, centralizado y coordinado de la delincuencia informática exige una respuesta política, económica, jurídica y tecnológica homogénea y susceptible de ser adoptada por los diversos protagonistas de la cadena digital, copartícipes de la seguridad.

I.2.6.2 La soberanía nacional

El reto de la sencillez y de la eficacia de la seguridad se opone a la complejidad de las necesidades y de los entornos, y tiende a favorecer los planteamientos de subcontratación de servicios y de la seguridad de los sistemas e informaciones a sociedades especializadas. Esta subcontratación genera

una dependencia de considerable importancia cuando no absoluta que constituye un riesgo de seguridad de primer orden. Los Estados deben procurar no depender de entidades externas que escapen a su control, en lo que afecta a la gestión estratégica, táctica y operacional de su seguridad.

Los Estados deben contribuir al cumplimiento de los siguientes objetivos:

- poder disponer de la seguridad inherente (seguridad por defecto) y de manera amistosa, comprensible, transparente, controlable y verificable;
- evitar que los individuos e instituciones se pongan en situaciones peligrosas (evitar las configuraciones permisivas, los comportamientos arriesgados, la dependencia excesiva, etc.);
- el respeto de las normas de seguridad;
- la reducción de la vulnerabilidades de la tecnología y de las soluciones de seguridad.

I.2.7 El punto de vista económico

La seguridad no permite la obtención directa de beneficios económicos aunque sí contribuye a evitar las pérdidas. Aunque el coste de la seguridad (presupuestos asociados, coste de los productos de seguridad, de formación, etc.) parece relativamente fácil de estimar, evaluar su rentabilidad resulta bastante más intrincado. Se puede pensar, subjetivamente, que las medidas de seguridad poseen intrínsecamente una eficacia «pasiva» y evitan ciertas pérdidas.

De todos modos, la determinación del coste de la seguridad en relación con los costes asociados a las consecuencias resultantes de la pérdida de valores por accidentes, errores, o dolo, resulta difícil de realizar. El coste de la seguridad es función de las exigencias de las organizaciones y depende de los valores a proteger y del coste de los perjuicios acarreados por un fallo de seguridad. Además, no existe una respuesta predefinida a las cuestiones siguientes:

- ¿Cómo evaluar la exposición de la organización a los riesgos, especialmente a los riesgos en serie que comporta la interconexión de las infraestructuras entre organizaciones?
- ¿Cómo estimar correctamente los costes indirectos de la inseguridad que resultan, por ejemplo, de una pérdida de imagen o de espionaje?
- ¿Qué puede aportar la seguridad a la organización que la implementa?
- ¿Cuál es el valor económico de la seguridad?
- ¿Cuál es el retorno sobre la inversión de la seguridad?

El valor económico de la seguridad debe contemplarse en toda su dimensión social, teniendo en cuenta las repercusiones de las nuevas tecnologías sobre los individuos, las organizaciones y las naciones. No puede reducirse, por tanto, a los costes de instalación y mantenimiento.

I.2.8 El punto de vista social

Es importante concienciar a todos los agentes del mundo de Internet sobre los beneficios del control de la seguridad y de las medidas elementales que permiten reforzar el nivel de seguridad siempre que se enuncien, definan y apliquen con claridad.

Es necesario emprender acciones de información y de educación cívica dirigidas a una sociedad de la información responsable, sobre los beneficios, riesgos y medidas preventivas y disuasivas de seguridad, para educar a todos los ciberciudadanos y que éstos adopten un planteamiento de seguridad.

Se hará hincapié en el deber de la seguridad, la responsabilidad individual y en las medidas disuasorias, así como sobre las posibles consecuencias penales del incumplimiento de las obligaciones de seguridad. De manera más general, resulta igualmente necesario educar y formar en las tecnologías del tratamiento de la información y de las comunicaciones y no solamente en la seguridad y en las medidas de disuasión. La sensibilización a los problemas de seguridad no debe limitarse a la

promoción de una cierta cultura de seguridad. Además de la cultura de seguridad debe haber una cultura de la informática, lo que corresponde al concepto de carné de conducir informático, que promueve el CIGREF (Club Informático de las Grandes Empresas Francesas)[7].

Internet debe ser un patrimonio abierto a todos de manera que los ciberciudadanos puedan beneficiarse de las infraestructuras y servicios puestos a su disposición, sin asumir riesgos de seguridad excesivos. Debe pues desarrollarse una ética de seguridad, comprendida y respetada por todos los implicados del ciberespacio.

I.2.9 El punto de vista jurídico

I.2.9.1 El factor crítico de éxito

En la legislación de ciertos países y en determinados convenios internacionales se obliga a las organizaciones a dotarse de medidas de seguridad que garanticen la conformidad jurídica. De este modo, los dirigentes de una organización y, por delegación de poderes, los responsables de seguridad, tienen una obligación con respecto a los medios de seguridad (aunque no una obligación en cuanto a los resultados). La responsabilidad de una persona jurídica que haya cometido una falta de seguridad que conlleve una infracción, puede ser penal, civil o administrativa. Esta responsabilidad se establece sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción.

Una legislación adaptada en materia de tratamiento de datos permite reforzar la confianza de los socios económicos en las infraestructuras del país, lo que contribuirá al desarrollo económico del mismo. De este modo, al contribuir a crear un contexto propicio al intercambio de datos con respeto de la legislación, se favorece la utilización por parte del público en general de servicios basados en la informática y las telecomunicaciones. La legislación y la seguridad deben considerarse pues como activadores de la economía nacional. Asociada al concepto de confianza y de calidad, la ciberseguridad constituye la piedra angular sobre la que se puede desarrollar una verdadera economía de servicios.

I.2.9.2 Refuerzo de la legislación y de los medios de aplicación de la misma

Actualmente, la ciberdelincuencia está mal controlada como lo demuestran las cifras de los sondeos anuales del CSI[8] (*Computer Security Institute*) o las estadísticas del CERT[9] (*Computer Emergency and Response Team*). Por tanto, resulta evidente que las medidas de seguridad adoptadas por las instituciones tienden a proteger un entorno dado en un contexto particular, aunque no pueden de ninguna manera impedir la ejecución de actividades delictivas por Internet. Las causas de esta situación están relacionadas principalmente con:

- las características del ciberdelito (capacidad de automatización, tecnología integrada en los programas informáticos, ejecución a distancia);
- la posibilidad que tiene el ciberdelincuente de usurpar fácilmente y sin excesivo riesgo, la identidad de los usuarios legítimos, neutralizando de este modo la capacidad de la justicia para identificar a los autores reales de una infracción;
- la determinación de las competencias para realizar una investigación;
- la escasez de recursos humanos y materiales en los servicios encargados de la represión de los crímenes y delitos informáticos;
- el carácter transnacional de la ciberdelincuencia que necesita frecuentemente de la cooperación y colaboración judicial internacional. Esto último supone demoras incompatibles con la rapidez con que se ejecutan las agresiones y con la necesidad de poner inmediatamente en funcionamiento los sistemas informáticos afectados por los ciberataques;

---

7 CIGREF: www.cigref.fr.

8 CSI: www.gocsi.com

9 CERT: www.cert.org

– la dificultad de calificar los hechos con arreglo a ciertas legislaciones penales;
– la naturaleza mal definida de la mayor parte de las pruebas informáticas y la volatilidad de las mismas.

Por todas estas causas, el sistema judicial resulta ineficaz en el contexto de Internet. Además, al igual que existen paraísos fiscales, existen paraísos legales. La causa de que el delito informático esté poco o mal reprimido no es necesariamente la falta de leyes. Hay un cierto número de crímenes y delitos informáticos que ya están calificados en las legislaciones penales existentes.

Lo que es ilegal «fuera de línea» también lo es «en línea»

Las nuevas legislaciones, nacidas de la necesidad de definir un marco jurídico apropiado para la utilización de las nuevas tecnologías, complementan o debe complementar la mayor parte de las legislaciones existentes que, como cabe subrayar, son igualmente válidas en el ciberespacio.

El refuerzo de la legislación no tiene por qué ser suficiente si faltan los medios de aplicación. Una ley será de poca utilidad si la justicia no se esfuerza en recoger pruebas y analizarlas, e identificar a los autores de comportamientos delictivos y sancionarlos. Tampoco resultará eficaz si los delincuentes saben que pueden actuar con total impunidad.

I.2.9.3 La lucha contra la ciberdelincuencia y el derecho a la intimidad digital: un compromiso difícil

Los medios de lucha contra el azote internacional de la ciberdelincuencia, cada vez mayor y más ajeno a las fronteras, pasa por la creación de un marco legal armónico y aplicable a nivel internacional y de medios eficaces de cooperación internacional de las instancias judiciales y policiales.

Sobre el Estado recaen responsabilidades importantes en la realización de la seguridad digital. Esto es particularmente cierto en lo tocante a la definición del marco legal adecuado, es decir, unificado y aplicable, para la promoción de una cultura de seguridad que respete la intimidad digital de los individuos (*privacidad*), sin perjuicio de la intensificación de la lucha contra la delincuencia.

El principal objetivo de la lucha contra la ciberdelincuencia debe ser la protección de los individuos, las organizaciones y los Estados, tomando en consideración los grandes principios democráticos.

Las herramientas de lucha contra la delincuencia pueden actuar en detrimento de los derechos del hombre y atentar contra la confidencialidad de los datos de carácter personal. Efectivamente, la implementación de la seguridad pasa por la vigilancia, control y filtrado de los datos. Es esencial la creación de barreras que eviten los abusos de poder, de situación dominante y todo tipo de derivas totalitarias a fin de garantizar el respeto de los derechos fundamentales y, muy especialmente, el respeto a la intimidad digital y a la confidencialidad de los datos personales.

Además de la Directiva Europea de 1995, cabe señalar las diversas legislaciones nacionales que existen desde hace tiempo, referentes a la protección de los datos personales:

Alemania: Ley de 21 de enero de 1977
Argentina: Ley de protección de datos personales – 1996
Austria: Ley de 18 de octubre de 1978
Australia: Ley de la vida privada – 1978
Bélgica: Ley de 8 de diciembre de 1992
Canadá: Ley de protección de las informaciones personales – 1982
Dinamarca: Ley de 8 de junio de 1978
España: Ley de 29 de octubre de 1992
Estados Unidos: Ley de protección de las libertades individuales – 1974; Ley de bases de datos y de la vida privada – 1988
Finlandia: Ley de 30 de abril de 1987
Francia: Ley de informática y libertades del 6 de enero de 1978 – modificada en 2004
Grecia: Ley de 26 de marzo de 1997
Hungría: Ley de protección de datos personales y de comunicación de datos públicos – 1992

Irlanda: Ley de 13 de julio de 1988
Islandia: Ley relativa a la grabación de datos personales – 1981
Israel: Ley de protección de la vida privada – 1981, 1985 y 1996; Ley de protección de los datos en la administración – 1986
Italia: Ley de 31 de diciembre de 1996
Japón: Ley de protección de datos informatizados de carácter personal – 1988
Luxemburgo: Ley de 31 de marzo de 1979
Noruega: Ley de registros de datos personales – 1978
Nueva Zelandia: Ley de información oficial – 1982
Países Bajos: Ley de 28 de diciembre de 1988
Polonia: Ley relativa a la protección de datos personales – 1997
Portugal: Ley de 29 de abril de 1991
República Checa: Ley de protección de datos personales de los sistemas informatizados – 1995
Reino Unido: Ley de 12 de julio de 1988
Rusia: Ley Federal de información, informatización y protección de las informaciones
Eslovenia: Ley de protección de datos – 1990
Suecia: 11 de mayo de 1973
Suiza: Ley Federal de protección de datos – 1992
Taiwán: Ley de protección de datos – 1995

I.2.9.4 Reglamentación internacional en materia de ciberdelincuencia

La primera reglamentación internacional que contempla la dimensión internacional de la ciber-delincuencia es el Convenio sobre ciberdelincuencia[10] – Budapest 23 de noviembre de 2001, adoptado bajo los auspicios del Consejo de Europa y en vigor desde julio de 2004 (tras su ratificación por cinco Estados como mínimo (de los cuales tres al menos tenían que formar parte del Consejo de Europa). En este Convenio se abordan los puntos siguientes:

- Disposición de derecho penal material que contempla:
  - las infracciones de la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos;
  - las infracciones informáticas;
  - las infracciones relacionadas con los ataques a la propiedad intelectual y derechos afines;
- Disposición de derecho procesal que afecta a lo siguiente:
  - al almacenamiento rápido de los datos informáticos y de los relativos al tráfico y a su divulgación rápida a las autoridades competentes;
  - a la conservación y protección de la integridad de los datos durante el tiempo necesario para permitir a las autoridades competentes obtener su divulgación;
  - al mandato de presentación;
  - a la captura y registro de los datos almacenados;
  - a la recogida de datos en tiempo real;
  - a la protección adecuada de los derechos humanos y libertades;
- Los Estados deben adoptar las medidas legislativas y de otra índole, necesarias para establecer como infracción penal, sin perjuicio de las leyes nacionales:
  - el acceso deliberado e ilegítimo a todo un sistema o parte del mismo;
  - la interceptación deliberada o ilegítima de los datos durante su transmisión no pública, con destino a un sistema, procedente de éste o en el interior del mismo;

[10] http://www.conventions.coe.int/Treaty/EN/Treaties/Html/185-SPA.htm

- el hecho deliberado e ilegítimo de dañar, borrar, deteriorar, alterar o suprimir datos;
- la obstaculización grave deliberada e ilegítima del funcionamiento de un sistema;
- la producción, venta, obtención para su uso, importación, difusión u otras formas de aprovechamiento de dispositivos concebidos o adaptados para realizar alguna de las infracciones citadas;
- la introducción, alteración, borrado o supresión deliberada e ilegítima de datos, generando datos falsos, con la intención de que sean considerados o utilizados para fines legales como si fueran realmente auténticos;
- el hecho deliberado e ilegítimo de ocasionar un perjuicio patrimonial a un tercero por la introducción, alteración, borrado o supresión de datos y toda forma de ataque al funcionamiento de un sistema con intención, dolosa o delictiva, de obtener ilegítimamente un beneficio económico para sí mismo o para un tercero;
- se considera infracción penal la complicidad en las acciones mencionadas así como la tentativa deliberada de perpetrarlas.

– Los Estados deben establecer sus competencias respecto a toda infracción penal siempre que ésta se haya cometido:
  - en su territorio;
  - a bordo de un barco con bandera de dicho Estado;
  - por uno de sus ciudadanos, si la infracción es punible penalmente allí donde se haya cometido o si la infracción no incumbe a la competencia territorial de ningún Estado;
– Reglas que afectan a la cooperación internacional en materia de:
  - extradición;
  - colaboración con fines de investigación;
  - procedimientos relativos a las infracciones penales relacionadas con los sistemas y datos informáticos;
  - la recogida de pruebas de infracciones penales en formato electrónico;
– Creación de una red de colaboración:
  - 24 horas al día, 7 días a la semana;
  - servicio de información nacional;
  - asistencia inmediata para las infracciones.

A nivel internacional existe ciertamente la voluntad reglamentaria de poder controlar la ciber-delincuencia. La causa de que se explote Internet con fines delictivos no es en ningún caso la falta de leyes o directrices como las enunciadas por la OCDE (Organización de Cooperación y Desarrollo Económico) «Directrices de la OCDE para la seguridad de sistemas y redes de información – hacia una cultura de seguridad – 2002[11]» (Figura I.7) sino la dificultad y complejidad de los trabajos a realizar y los medios necesarios para alcanzar los objetivos de la lucha no solamente contra la ciberdelincuencia sino también contra el crimen organizado.

[11] www.oecd.org/dataoecd/16/22/15582260.pdf. Estas directivas se reproducen en el Anexo al presente documento.

Figura I.7 – Directrices de la OCDE en materia de seguridad informática (julio de 2002)

Sensibilización	Las partes interesadas deben concienciarse de la necesidad de garantizar la seguridad de los sistemas y redes de información y de las acciones que pueden adoptar para reforzar la seguridad
Responsibilidad	Las partes interesadas son responsables de la seguridad de los sistemas y de las redes de información
Reacción	Las partes interesadas deben actuar con rapidez y con ánimo de cooperación para prevenir, detectar y responder a los incidentes de seguridad
Ética	Las partes interesadas deben respetar los intereses legítimos de las demás partes interesadas
Democracia	La seguridad de los sistemas y de las redes de información debe ser compatible con los valores fundamentales de una sociedad democrática
Evaluación de riesgos	Las partes interesadas deben evaluar los riesgos
Concepción y aplicación de la seguridad	Las partes interesadas deben integrar la seguridad como elemento esencial de los sistemas y redes de información
Gestión de la seguridad	Las partes interesadas deben adoptar una solución global de gestión de la seguridad
Revaluación	Las partes interesadas deben examinar y revaluar la seguridad de los sistemas y redes de información así como introducir las modificaciones adecuadas en sus políticas, prácticas, medidas y procedimientos de seguridad

I.2.10 Fundamentos de la ciberseguridad

Las soluciones de seguridad deben contribuir a la satisfacción de los criterios básicos de la seguridad, a saber: disponibilidad, integridad y confidencialidad (criterios DIC). A los tres criterios citados se añaden los que permiten demostrar la identidad de las entidades (concepto de autenticación) y las acciones o acontecimientos que han tenido lugar (conceptos de no rechazo, de imputabilidad y de rastreo) (Figura I.8).

I.2.10.1 Disponibilidad

La disponibilidad de servicios, sistemas y datos se obtiene, por una parte, por el adecuado dimensionamiento, con un cierto grado de redundancia, de los elementos constitutivos de las infraestructuras y, por otra, por la gestión operacional de los recursos y de los servicios.

La disponibilidad se mide a lo largo del periodo de tiempo durante el que el servicio ofrecido está operativo. El volumen potencial de trabajo aceptable durante el periodo de disponibilidad de un servicio, determina la capacidad de un recurso (por ejemplo, de un servidor o de una red). Por otra parte, la disponibilidad de un recurso no se puede disociar de su accesibilidad.

I.2.10.2 Integridad

El respeto a la integridad de los datos, procesamientos y servicios permite garantizar que no se modifiquen, alteren ni destruyan, ni deliberada ni accidentalmente. Esto contribuye a garantizar su exactitud, fiabilidad y perdurabilidad.

Conviene protegerse anticipadamente de la alteración de los datos cerciorándose de que no se han modificado durante su almacenamiento ni durante su transmisión.

La integridad de los datos sólo quedará garantizada si se protegen de escuchas activas que puedan interceptarlos y modificarlos. Esta protección puede realizarse por la implementación de mecanismos de seguridad tales como:

– un control de acceso riguroso;
– la encriptación de los datos;
– medios de protección contra virus, gusanos y troyanos.

Figura I.8 – Elementos fundamentales de la ciberseguridad

Capacidad de un sistema para:	Objetivos de la seguridad	Medios de seguridad
Poder utilizarse	• Disponibilidad • Perdurabilidad • Continuidad • Confianza	• Dimensionamiento • Redundancia • Procedimientos de explotación y de copia de seguridad
Ejecutar acciones	• Seguridad de funcionamiento • Fiabilidad • Perdurabilidad • Continuidad • Exactitud	• Concepción • Prestaciones • Ergonomía • Calidad de servicio • Mantenimiento operacional
Permitir el acceso de entidades autorizadas (ningún acceso ilícito)	• Confidencialidad (preservación del secreto) • Integridad (ninguna modificación)	• Control de acceso • Autenticación • Control de errores • Control de coherencia • Encriptación
Demostrar las acciones	• No rechazo • Autenticidad (ninguna duda) • Ninguna contestación	• Certificación • Grabación, rastreo • Firma electrónica • Mecanismos de prueba

I.2.10.3 Confidencialidad

La confidencialidad consiste en guardar el secreto de las informaciones, flujos, transacciones, servicios y acciones realizadas en el ciberespacio. Se trata de proteger los recursos contra su divulgación no autorizada.

La confidencialidad puede implementarse por medio de mecanismos de control de acceso o de encriptación.

La encriptación de los datos (criptografía), contribuye a garantizar la confidencialidad de las informaciones durante su transmisión o almacenamiento, transformándolos de modo que resulten ininteligibles para las personas que no dispongan de los medios de desencriptación adecuados.

I.2.10.4 Identificación y autenticación

La autenticación debe permitir disipar cualquier duda sobre la identidad de un recurso. Esto supone la correcta identificación de todas las entidades (recursos materiales, programas informáticos y personas) y la posibilidad de que determinadas características sirvan de prueba para su identificación. Es necesario que todos los mecanismos de control de acceso lógico a los recursos informáticos efectúen la identificación y autenticación de las entidades.

Los procesos de identificación y autenticación tienen por objeto contribuir a:

- la confidencialidad e integridad de los datos: sólo los derechohabientes identificados y autenticados pueden acceder a los recursos (control de acceso) y modificarlos si están habilitados para ello;
- el no rechazo y la imputabilidad (ciertas entidades identificadas y autenticadas han realizado determinada acción), la prueba de origen de un mensaje o de una transacción (cierta entidad identificada y autenticada ha efectuado determinada emisión), la prueba de destino (cierta entidad identificada y autenticada es la destinataria de determinado mensaje).

I.2.10.5 No rechazo

En ciertos casos, es necesario demostrar la realización de ciertos eventos (acciones o transacciones). Al no rechazo se asocian los conceptos de responsabilidad, imputabilidad, rastreo y, en su caso, de auditabilidad.

El establecimiento de la responsabilidad exige la existencia de mecanismos de autenticación de los individuos y de imputabilidad de sus acciones. Es especialmente importante poder registrar la información a fin de «rastrear» la ejecución de acciones, cuando se trata de reconstruir un histórico de los acontecimientos, especialmente cuando se trata de investigaciones en medios informáticos para recuperar eventualmente, por ejemplo, la dirección del sistema desde el que se han enviado datos. Debe guardarse (registro por diario) la información necesaria para un análisis posterior que permita realizar la auditoría de un sistema. En esto consiste la capacidad de un sistema para ser auditado (concepto de auditabilidad).

I.2.10.6 Seguridad física

Deben protegerse físicamente los entornos donde se encuentran los puestos de trabajo, los servidores, las zonas de explotación informática y de logística (aire acondicionado, cuadros de control de alimentación eléctrica, etc.) contra accesos indebidos y catástrofes naturales (incendio, inundación, etc.). La seguridad física representa el control más fundamental y vigente de los sistemas informáticos.

I.2.10.7 Soluciones de seguridad

Considerando los problemas de seguridad cotidianos de la mayor parte de las infraestructuras, sabiendo que sobran soluciones de seguridad y que el mercado de la seguridad se comporta satisfactoriamente, nos permitimos plantearnos las cuestiones siguientes:

- ¿Están adaptadas las soluciones de seguridad a las necesidades?
- ¿Están implantadas y gestionadas correctamente?
- ¿Pueden aplicarse y adaptarse a un entorno en constante cambio?
- ¿Pueden atenuar el excesivo poder otorgado a los administradores de los sistemas?
- ¿Cómo pueden afrontar los problemas de seguridad cuyo origen debe buscarse en la negligencia, la incompetencia, los fallos de diseño, de implementación o de gestión de las tecnologías y soluciones de seguridad?
- etc.

SECCIÓN II

CONTROL DE LA CIBERDELINCUENCIA

Capítulo II.1 – La ciberdelincuencia

II.1.1 Concepto de delito informático y de ciberdelito

Las vulnerabilidades y el insuficiente control de las tecnologías digitales les confieren un cierto nivel de inseguridad. De este estado de inseguridad se aprovechan sobre todo los delincuentes. Por otra parte, cada tecnología introduce potencialidades delictivas y ofrece oportunidades para cometer infracciones. Internet no es excepción a esta regla y el mundo de la delincuencia ha invadido el ciberespacio.

La OCDE definió en 1983 la infracción informática como todo comportamiento ilegal, inmoral o no autorizado que afecta a la transmisión o al procesamiento automático de datos.

Un delito informático (*computer-related crime*) es aquél cuyo objeto o medio de realizarlo es un sistema informático, está relacionado con las tecnologías digitales y se integra en los propios de la delincuencia de cuello blanco. El ciberdelito (*cybercrime*) es una forma del delito informático que recurre a las tecnologías de Internet para su comisión, refiriéndose por tanto a todos los delitos cometidos en el ciberespacio.

El mundo virtual confiere al delito la capacidad de automatización, permitiendo su ejecución a gran escala (ciberepidemia), su comisión a distancia *a través de las redes* (ubicuidad del delincuente en el tiempo y en el espacio) y, en su caso, con efecto retardado (Figura II.1).

Figura II.1 – Características del delito informático

- Delincuencia de cuello blanco
- Delito cometido a distancia a través de las redes, escondidos detrás de una pantalla
- Ubicuidad del delincuente en el espacio y en el tiempo
- Conocimientos técnicos del delincuente integrados en el software
- Comisión automatizada de delitos a gran escala

Las tecnologías de Internet facilitan todo tipo de infracciones (robo, sabotaje de información, ataques a los derechos de copia, al derecho de autor, a la violación del secreto profesional, de la intimidad digital, de la propiedad intelectual, difusión de contenidos ilegales, ataques contra la competencia, espionaje industrial, violación de los derechos de las marcas, difusión de informaciones falsas, denegación de servicio, fraudes diversos, etc.).

Los acontecimientos que han contribuido a la evolución de la percepción de la amenaza ciberdelincuente son, además del virus del año 2000 que ha permitido tomar conciencia de la fragilidad de los programas informáticos y de la dependencia de la informática, los ataques de denegación de servicio contra sitios tales como Yahoo (10 de febrero de 2000) y el famoso virus «I love you» (4 de mayo de 2000). Desde entonces, gracias a la cobertura mediática de los ataques de los virus (el virus *Code red* de julio de 2001 o el *Nimda* de septiembre de 2001) o de denegación de servicio (ataque a los principales servidores de DNS el 21 de octubre de 2002), por no citar más que algunos ejemplos, el público en general toma conciencia en mayor o menor medida de la realidad de las amenazas que se materializan a través del mundo de Internet. La actualidad abunda en noticias de nuevos problemas relacionados con la informática.

II.1.2 Factores que favorecen la expresión de la delincuencia por Internet

II.1.2.1 El mundo virtual y la desmaterialización

La desmaterialización de las transacciones y la facilidad de comunicación asociada a las soluciones de encriptación, de taquigrafía y de anonimato, permiten establecer vínculos entre los delincuentes de distintos países sin contacto físico, de manera flexible y segura, con toda impunidad. De este modo, pueden organizarse en equipos, planificar acciones lícitas y ejecutarlas ya sea del modo tradicional, ya por medio de las nuevas tecnologías. La cobertura internacional de Internet permite a los delincuentes actuar a nivel mundial, a gran escala y con toda rapidez.

Por otra parte, las facilidades propias del mundo digital y de las telecomunicaciones, los problemas de concepción, implementación, gestión y control de la informática asociados a las averías, los problemas de funcionamiento, los errores, incompetencias e incluso las catástrofes naturales, y la interdependencia de las infraestructuras, confieren de hecho un cierto grado de inseguridad a las infraestructuras digitales.

Las posibilidades de explotación de las vulnerabilidades con fines malintencionados son numerosas y se traducen en lo siguiente:

> usurpación de identidad, falsificación de direcciones, accesos indebidos, explotación fraudulenta de recursos, infección, deterioro, destrucción, modificación, divulgación, robo de datos, chantaje, extorsión, intimidación, denegación de servicio, etc.

lo que pone en evidencia la insuficiencia del control del riesgo informático de origen delictivo por parte de las organizaciones y las limitaciones de las soluciones de seguridad existentes.

El ciberespacio, donde las acciones se ejecutan amparadas en el anonimato de una pantalla y a distancia a través de una red, favorece los comportamientos delictivos. Esto facilita a algunos el paso a la ilegalidad sin tener, muchas veces, conciencia real de la dimensión delictiva de los actos perpetrados.

Además, los delincuentes pueden organizarse en equipos, planificar acciones ilícitas y realizarlas ya sea del modo tradicional, ya por medio de las nuevas tecnologías. La cobertura internacional de Internet permite a los delincuentes actuar a nivel mundial, a gran escala y con toda rapidez.

II.1.2.2 Conexión en red de los recursos

La generalización de la conexión en red de los recursos informáticos y de información, los convierte en blancos interesantes para la comisión de delitos económicos gracias a las nuevas tecnologías. Las distintas formas de ataques informáticos existentes tienen por denominador común la asunción relativamente escasa de riesgos para su autor y la posibilidad de consecuencias negativas y daños muy superiores a los recursos necesarios para su ejecución. La usurpación electrónica de identidad, las posibilidades de anonimato y el control de ordenadores, por ejemplo, facilitan la ejecución de acciones ilegales sin riesgos excesivos.

II.1.2.3 Disponibilidad de herramientas y existencia de fallos

La disponibilidad de herramientas de explotación de los fallos y vulnerabilidades de los sistemas, de bibliotecas de ataques y de programas informáticos que capitalizan los conocimientos técnicos delincuentes en un programa, facilita la ejecución de ataques informáticos. Esta disponibilidad asociada a la desmaterialización de las acciones, favorece el comportamiento doloso de los informáticos con pocos escrúpulos y de los delincuentes con conocimientos informáticos. El ciberespacio facilita a algunos el paso a la ilegalidad sin tomar muchas veces conciencia real de la dimensión delictiva de los actos perpetrados.

II.1.2.4 Vulnerabilidad y fallos

La delincuencia aprovecha las vulnerabilidades y fallos de la organización y de las técnicas de Internet, la inexistencia de un marco jurídico armónico entre los Estados y la falta de coordinación eficaz de las políticas. Puede tratarse de la delincuencia tradicional (comisión de los delitos tradicionales con nuevas tecnologías: blanqueo de dinero, chantaje, extorsión, etc.) o generar nuevos tipos de delitos basados en las tecnologías digitales: intrusión en sistemas, robo de tiempo del procesador, robo de código fuente, de base de datos, etc. En todos los casos se efectúa en condiciones excepcionalmente óptimas (riesgos mínimos, cobertura importante y rentabilidad máxima).

La Figura II.2 resume las fuentes de vulnerabilidad de una infraestructura Internet.

Figura II.2 – Características principales del mundo de Internet explotadas con fines delictivos

II.1.2.5 Problemas para identificar a los autores de un delito

El delito informático es sofisticado y se suele cometer a nivel internacional a veces con efecto retardado. Los rastros que quedan en los sistemas son inmateriales y difíciles de recoger y almacenar. Se trata de informaciones digitales memorizadas en cualquier tipo de soporte: memorias, periféricos de almacenamiento, discos duros, disquetes, memorias USB, componentes electrónicos diversos, etc. Se plantea entonces la cuestión de su captura en el curso de una investigación informática. Las cuestiones siguientes, entre otras, demuestran hasta qué punto cuesta establecer el concepto de prueba digital:

- ¿Cómo identificar los datos pertinentes?
- ¿Cómo localizarlos?
- ¿Cómo preservarlos?
- ¿Cómo constituir una prueba que se pueda presentar ante un tribunal?
- ¿Cómo recuperar ficheros borrados?
- ¿Cómo demostrar el origen de un mensaje?
- ¿Cómo remontarse hasta la identidad de una persona basándose únicamente en un rastro digital, dada la dificultad de establecer una correspondencia segura entre una información digital y su autor (desmaterialización) y de la frecuencia con la que se usurpan las identidades?
- ¿Cuál es el valor de un rastro digital como prueba para establecer la verdad ante un tribunal (concepto de prueba digital) sabiendo que los soportes de memoria de los que se han sacado los rastros pueden fallar (los conceptos de fecha y hora son variables de un sistema informático al otro y fáciles de modificar)?
- etc.

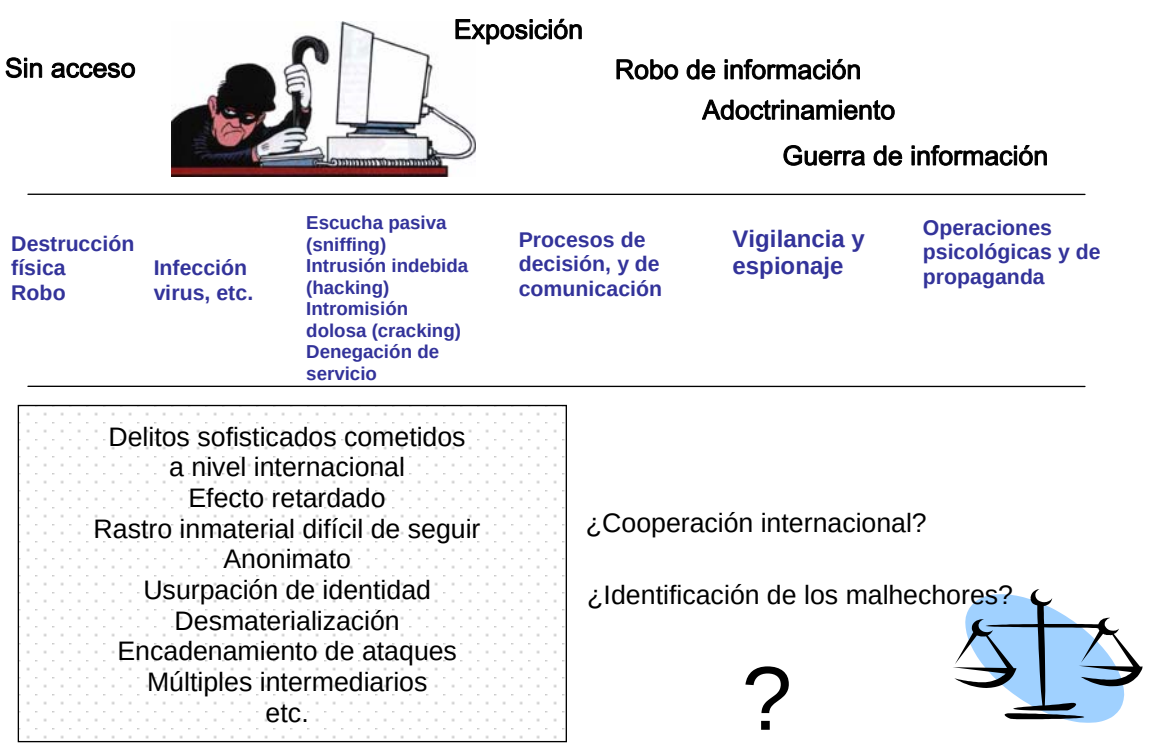
Los rastros informáticos son aún más difíciles de obtener cuando se encuentran en varios sistemas de distintos países. Su obtención depende de la eficacia de la colaboración judicial internacional y de la rapidez de la intervención. La eficacia de su explotación para identificar a los individuos depende de lo que tarde en tramitarse la solicitud de obtención, que puede llevar un cierto tiempo y que puede llegar a imposibilitar cualquier identificación.

La Figura II.3 muestra los diversos tipos de problemas inducidos por un comportamiento malintencionado tal como la destrucción física o el robo de material que impida el acceso a los sistemas y datos, la infección de recursos, la exposición de los procesos de decisión y de comunicación por ataques de denegación de servicio (o como consecuencia del espionaje o intrusión en grandes sistemas), la apropiación ilegal o la manipulación de informaciones (adoctrinamiento, guerra de información). En esta figura se destacan igualmente las principales características del ciberdelito que dificultan la identificación de los malhechores.

Por lo demás, en la mayor parte de los Estados, existe un desequilibrio significativo entre las aptitudes de los delincuentes para cometer delitos de alta tecnología y los medios a disposición de las fuerzas judiciales y policiales para perseguirlos. El grado de adopción de nuevas tecnologías por parte de las instancias de justicia y de la policía a nivel nacional e internacional sigue siendo escaso y muy dispar de un país a otro.

En la mayor parte de los casos, la policía y las autoridades judiciales recurren a los métodos convencionales de investigación utilizados en los delitos ordinarios a fin de perseguir a los ciber-delincuentes, identificarlos y arrestarlos.

Figura II.3 – Problemas de identificación del malhechor



II.1.2.6 Desvinculación territorial y paraísos digitales

El mundo de la delincuencia se aprovecha de la desvinculación territorial de Internet, de la inexistencia en ciertos Estados de leyes que repriman el delito informático y de las múltiples jurisdicciones que afectan a Internet.

Análogamente a los paraísos fiscales, los paraísos digitales permiten a los delincuentes alojar los servidores, difundir contenidos ilícitos y realizar acciones ilícitas con toda impunidad. La instalación de servidores en Estados débiles responde a la necesidad de crear refugios para operaciones transnacionales.

La falta de reglamentos internacionales y de control y la ineficacia de la cooperación internacional en materia de investigación y de procedimientos judiciales hace que Internet se comporte como una capa aislante que protege a los delincuentes.

En el momento actual, no existe una solución idónea ni en el plano jurídico ni en el técnico para controlar los distintos delitos favorecidos por Internet, entre los que cabe citar los siguientes:

- la industria paralela, muy organizada, de copia en serie de programas informáticos, de películas, de música, etc., que ha alcanzado en el ciberespacio una dimensión sin precedentes;
- los ataques a los derechos editoriales, derechos de autor, la violación del secreto profesional, de la intimidad digital y de la propiedad intelectual;
- los ataques contra la propiedad, la apropiación ilegal de los bienes de un tercero, los daños o la destrucción de los bienes de un tercero y la intromisión en la propiedad de un tercero (concepto de violación de domicilio virtual);
- la difusión de contenidos ilegales;
- los ataques a la competencia, el espionaje industrial, los ataques a los derechos de marca, la difusión de informaciones falsas y los ataques de denegación de servicio encargados por la competencia.

II.1.3 La delincuencia tradicional frente a la ciberdelincuencia

La ciberdelincuencia es la heredera natural de la delincuencia tradicional. Hoy en día, las actividades delictivas se realizan a través del ciberespacio, por medios distintos a los habituales, y de modo complementario a la delincuencia tradicional.

Internet no sólo ofrece condiciones excepcionales para la proliferación de nuevas empresas y actividades ilícitas sino que además permite la comisión habitual de fraudes y delitos con herramientas informáticas.

Internet ofrece oportunidades que favorecen la búsqueda y generación de ingresos que suponen nuevas capacidades para el mundo de la delincuencia. La explotación eficaz de las nuevas tecnologías permite a los delincuentes cometer delitos garantizando unos beneficios máximos y exponiéndose a un nivel de riesgo aceptable.

II.1.4 Ciberdelincuencia, delincuencia económica y blanqueo

El delito económico a través de Internet no queda reservado únicamente a la delincuencia organizada, las herramientas informáticas y las telecomunicaciones lo acercan a individuos aislados que pueden constituirse o no en grupos de diversa importancia.

Los delincuentes pueden organizarse para intercambiar información gracias a las tecnologías de la información. Las redes de personas o de conocimientos permiten la constitución de organizaciones delictivas desmaterializadas.

El alto grado de conocimientos económicos de profesionalidad necesarios para la comisión del delito económico, hacen que éste se vea facilitado por las tecnologías de la información.

Internet contribuye a la adquisición de información y a un mejor conocimiento de los mercados, leyes, técnicas, etc., necesario para la comisión de delitos económicos, facilitando igualmente la identificación de oportunidades delictivas.

El delito económico está sometido a la influencia de las nuevas tecnologías que se han convertido en un factor de producción de las organizaciones delictivas y coloca la información en el corazón de sus estrategias y procesos de decisión.

Las nuevas tecnologías facilitan todo tipo de robos, modificaciones, sabotaje de información y fraudes. Los fenómenos de chantaje, extorsión, intimidación, y solicitud de rescates, ya han aparecido en Internet.

Efectivamente los recursos informáticos se convierten en los rehenes potenciales de los ciber-delincuentes. Los chantajistas se han apropiado del ciberespacio y cualquiera puede ser objeto de intentos de chantaje, desinformación y ciberpropaganda. Además, la explosión del fenómeno de usurpación de identidad a partir de 2003, demuestra que los delincuentes han entendido en toda su amplitud los beneficios que podían extraer, no solamente de las capacidades de anonimato que ofrece Internet sino también de la apropiación de identidades falsas para evitar ser perseguidos o considerados responsables de acciones delictivas o terroristas. La usurpación de identidad, fácil de realizar en Internet, favorece la ejecución de actividades ilícitas.

Como todos los delincuentes que se aprovechan de las infraestructuras tecnológicas existentes, los blanqueadores de dinero recurren cada vez más a Internet para poder utilizar legalmente los capitales generados por actividades delictivas tales como el tráfico de drogas, la venta ilegal de armas, la corrupción, el proxenetismo, la pedofilia, el fraude fiscal, etc.

Aunque no se suele hablar mucho de ello y es mal conocido, el blanqueo de dinero por Internet está cobrando auge. Internet ofrece un potencial excepcional tanto por la desmaterialización (anonimato, mundo virtual, rapidez de transferencia) como por la desvinculación territorial (fenómeno transnacional, conflictos de competencias y jurisdicciones), características explotadas sobremanera por los protagonistas tradicionales del blanqueo. Internet permite reinsertar con toda impunidad dinero negro en los circuitos económicos por medio de transferencias de fondos, inversiones y capitalización.

Las operaciones bursátiles en línea, los casinos en línea, el comercio electrónico – venta de productos y servicios ficticios contra pago reales, generando beneficios justificados, son actividades incontrolables e imposibles de perseguir judicialmente. La banca electrónica, las transacciones de capital inmobiliario y de bienes inmuebles a través de la red, la creación de sociedades virtuales «pantalla» y los monederos electrónicos se utilizan para cometer el delito de los delitos que es el blanqueo. Gracias a la utilización de ciertos servicios desmaterializados, el internauta puede favorecer inconscientemente el desarrollo del blanqueo de dinero. Asimismo, las empresas pueden implicarse fortuitamente en este proceso y sufrir por ello consecuencias judiciales y comerciales que pueden llegar a ser importantes. Así pues, esto constituye un riesgo de gran importancia para las empresas.

En la actualidad existen pocos medios eficaces para controlar este fenómeno del blanqueo que utiliza las nuevas tecnologías.

II.1.5 Generalización de la ciberdelincuencia y extensión de la delincuencia

La ciberdelincuencia se suele realizar a través de delitos ordinarios, prácticamente invisibles pero muy reales y eficaces, gracias a la conexión en red de los recursos y de las personas. Las empresas pero sobre todo sus recursos informáticos y de información son los blancos preferidos de las organizaciones delictivas en busca de beneficios. Se trata pues de una amenaza estratégica en la medida en que el dinero se encuentra en los sistemas informáticos, en las grandes empresas, fondos de pensiones, etc., y no solamente en los bancos.

El carácter abierto de Internet propio de los servidores web, portales y mensajería electrónica expone a la empresa a riesgos de origen delictivo y permite la intromisión de los delincuentes. Internet es una herramienta de comunicación pero también un entorno caótico, complejo, dinámico y hostil que puede convertirse en una herramienta de desestabilización y de comisión de delitos. Así pues, Internet puede considerarse como una zona en la que florece la delincuencia. Por otra parte, la necesidad de que las instituciones estén presentes en Internet nos plantea la cuestión de su posible contribución en mayor o menor medida a la extensión de la delincuencia en Internet.

Hoy en día la seguridad interna de un país se enfrenta a amenazas delictivas relacionadas con las tecnologías de la información. Las tecnologías de Internet se encuentran en el corazón de la guerra de la información (infoguerra, *infowar*) cuyos objetivos son principalmente de índole económica y cuya repercusión es importante para el buen desarrollo de las actividades. Internet no sólo permite manipular la información sino que además es una herramienta privilegiada para responder a los rumores o a cualquier forma de intoxicación o campaña de desestabilización. Asimismo, se favorecen las actividades de espionaje y de inteligencia, debido a la facilidad actual de interceptación de la información que se transmite por Internet.

II.1.6 Ciberdelincuencia y terrorismo

La ciberdelincuencia puede tener una dimensión terrorista en la medida en que los sistemas atacados estén implicados en infraestructuras críticas. Efectivamente, las infraestructuras esenciales para el buen funcionamiento de las actividades de un país (energía, agua, transportes, logística alimentaria, telecomunicaciones, bancos y entidades financieras, servicios médicos, funciones gubernamentales, etc.) ven aumentada su vulnerabilidad por depender cada vez más de las tecnologías de Internet.

Es necesario subrayar la importancia de los sistemas de producción y distribución de electricidad ya que condicionan el funcionamiento de la mayor parte de las infraestructuras. El control de infraestructuras críticas parece ser uno de los objetivos del ciberterrorismo, prueba de ello es el recrudecimiento de los *scans* (pruebas de sistemas informáticos para descubrir sus vulnerabilidades a fin de poder penetrar en ellos con posterioridad) dirigidos contra los ordenadores de las organizaciones que gestionan estas infraestructuras.

Hoy en día, la definición del ciberterrorismo no está clara. Qué duda cabe de que lo más sencillo sería considerar el ciberterrorismo como el terrorismo aplicado al ciberespacio. Ahora bien, en su sentido ordinario, el terrorismo se refiere al empleo sistemático de la violencia para alcanzar un fin político.

Cabe preguntarse si la suspensión eventual de Internet o de una parte de la misma, como consecuencia de actos dolosos, podría provocar el terror en el seno de la comunidad de los internautas, de determinados agentes económicos particulares, o de la población.

¿No se trataría más bien de terrorismo económico dirigido a infringir daños a las organizaciones que realizan actividades a través de Internet?

El término «ciberterrorismo» debe usarse con prudencia sobre todo a partir de su difusión desde el 11 de septiembre de 2001. Efectivamente, conviene recordar que las primeros ataques de denegación de servicio distribuidos (DDOS) de las que se informó ampliamente en los medios de comunicación, fueron obra de un adolescente de 15 años (Mafia Boy) el de 10 febrero de 2000. Identificado y detenido varios meses más tarde, aunque sus motivos no se han hecho públicos, cabe pensar que en ningún caso eran políticos.

¿Si este mismo ataque hubiese sido perpetrado después del 11 septiembre de 2001 no se habría calificado de ciberterrorismo?

En ausencia de elementos concretos, sin reivindicación ni presunto autor de un ataque, es difícil calificar al mismo como ciberterrorista.

La palabra ciberterrorismo refleja una realidad bastante ambigua en el repertorio de las nuevas amenazas y es difícil suponer a priori los motivos y objetivos de un agresor o de un grupo de agresores desconocidos. Efectivamente, a veces resulta difícil distinguir, en función del blanco únicamente, los motivos de un delincuente, de un terrorista, de un mercenario, de un militante, de un estafador o incluso de un inmaduro.

El tipo de agresión informática no basta para definir con certeza la motivación ni los objetivos del malhechor. Esto constituye una de las dificultades de la lucha contra el delito informático ya que es necesario disponer de informaciones complementarias para caracterizar la intención delictiva.

Con independencia de que sea a través de procesos de desestabilización económica, de la amenaza de infraestructuras críticas, de la propagación de ideologías o de la manipulación de información, el ciberterrorismo constituye una nueva forma de amenaza que debe considerarse muy seriamente. Más allá de los sistemas informáticos y del mundo virtual que simboliza Internet, la vida puede verse amenazada al poner en peligro indirectamente la integridad de las personas.

II.1.7 Los ciberdelincuentes

La determinación de la motivación del ciberdelincuente y de su competencia tecnológica, permite evaluar la gravedad de un ataque para poder contrarrestarlo mejor. Para asegurar un sistema de información es necesario saber de quién se le debe proteger. Hoy en día se observan dos grandes tipos de ciberdelincuentes, a saber, por una parte los profesionales cuyas actividades son directamente rentables, y por otra, los aficionados que suelen estar animados por una gran necesidad de reconocimiento social (Figura II.4).

Los profesionales son generalmente:

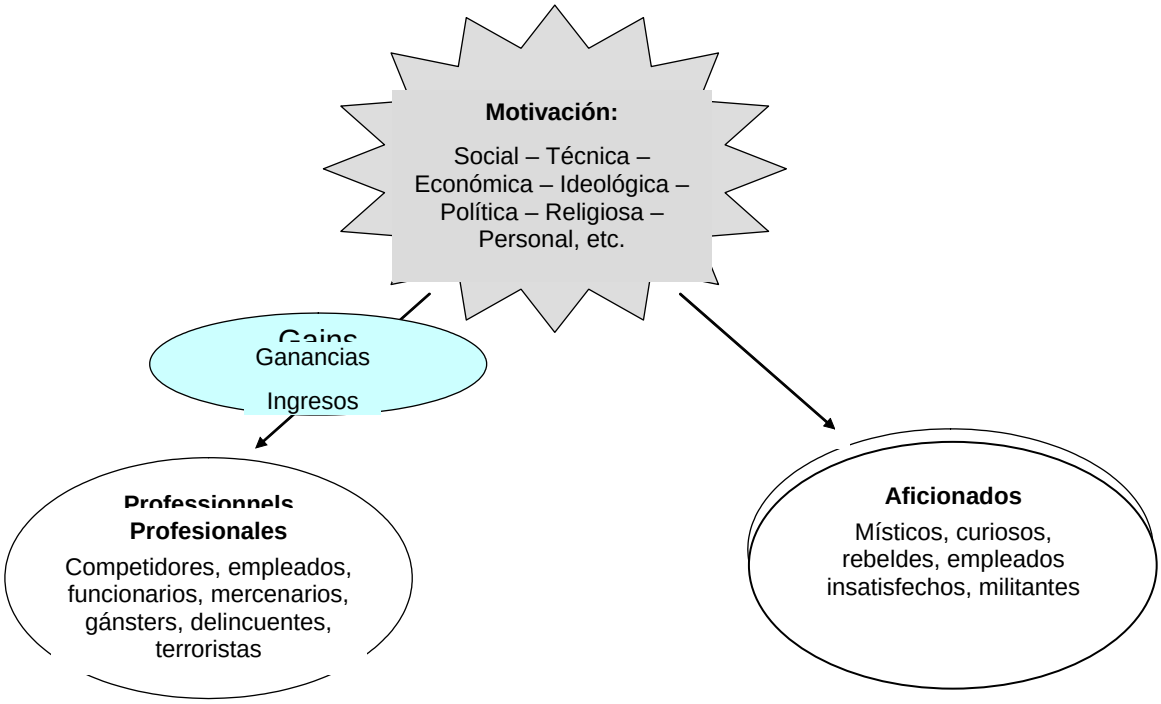
- competidores directos de la organización objetivo;
- funcionarios al servicio del Estado;
- mercenarios (que pueden actuar por encargo de instituciones tanto privadas como públicas);
- malhechores de cualquier tipo.

Entre los aficionados, destacan:

- los técnicos, sucesores de los primeros aficionados, piratas informáticos de los primeros tiempos, cuya motivación esencial era el deseo de dominar cada vez más las tecnologías;
- los curiosos;
- los inmaduros: que se suelen denominar «script-kiddies» o «kiddiots». Suelen acaparar una gran publicidad cuando son detenidos. El hecho de que sean atrapados por las fuerzas de orden público no significa necesariamente que sean los únicos ciberdelincuentes;

– los psicópatas;
– los militantes, movidos por ideologías o religión, que además se suelen encontrar a mitad de camino entre los aficionados y los profesionales.

Figura II.4 – Las dos grandes familias de ciberdelincuentes



Las motivaciones básicas de estas personas están relacionadas con componentes de orden social, técnico, político, financiero o estatal.

La motivación social radica en la necesidad de reconocimiento del individuo por sus iguales, y está relacionada generalmente con una estructura de banda. Quiere demostrar su valor al grupo refiriéndose a criterios culturales internos. Se trata de un fenómeno análogo al de los «*taggers*» que está vinculado a una visión muy primaria de las relaciones sociales. Suele aparecer entre los inmaduros para quienes el «*hacking*» les confiere un sentimiento de superioridad y de control de las instituciones a las que creen estar sometidos en su vida diaria.

La motivación técnica es poco habitual. Tiene como objetivo principal la investigación de los límites de la tecnología, a fin de sacar a la luz los límites y debilidades y comprender mejor los puntos fuertes.

La motivación política consiste en crear un evento destinado a alertar a los medios de comunicación, para llamar su atención sobre un problema grave esperando provocar una toma de conciencia colectiva que conduzca a su resolución. Debe observarse aquí que la frontera con el terrorismo puede ser bastante difusa, por lo menos desde un punto de vista conceptual. Se debe subrayar igualmente que un buen número de personas disimulan su motivación social detrás de un objetivo político.

La motivación financiera puede llegar a ser muy fuerte y engendrar muchas acciones ilícitas. El afán de ganancias, permite a los delincuentes de cuello blanco (ladrones, estafadores, competidores desleales, etc.) expresarse a través de la red de Internet.

Por último, cabe distinguir una motivación gubernamental. Con independencia de que se trate de guerra de información o de espionaje, afecta a servicios administrativos que actúan por encargo de los poderes del Estado.

Los delincuentes han sabido adaptarse a las nuevas tecnologías para que sus actividades tradicionales sigan dando fruto. Hay sobrados motivos de preocupación, viendo hasta qué punto pueden ser creativos cuando se trata de inventar nuevos usos para estas tecnologías.

II.1.8 Programas indeseables o maliciosos

II.1.8.1 El correo indeseado

El correo indeseado (*spam*) consiste en el envío masivo de mensajes electrónicos no solicitados cuya finalidad es en principio de carácter comercial y publicitario, a fin de incitar a los internautas a adquirir un producto o servicio.

El correo indeseado, a pesar del despliegue de medios técnicos y de las cantidades invertidas por los proveedores de servicios para bloquearlo, a pesar igualmente de la declaración de las autoridades en el sentido de querer combatir esta plaga y de las condenas a los responsables de la proliferación de correos indeseados, continúa siendo una auténtica molestia. En septiembre de 2003, el correo indeseado representó el 54% del tráfico total de los mensajes electrónicos intercambiados. En 2005 en Estados Unidos, según IDC, el número de correos electrónicos enviados sobrepasó los 12 mil millones de mensajes, lo que equivale al 38,7% del tráfico total.

Llevado a un extremo, el fenómeno del correo indeseado puede asimilarse a un ataque por bombardeo o inundación de mensajes (*email bombing*) sobrecargando desmedidamente los servidores de mensajería, los buzones de los usuarios y con muchas inconveniencias. Esto puede llevarse a cabo por la inscripción del usuario, sin su conocimiento, en listas de distribución de información (*list linking*). Al usuario no le queda otra solución que darse de baja en dichas listas o, si eso le parece muy engorroso, cambiar de dirección electrónica. Esta alternativa, aunque eficaz es igualmente molesta en la medida en que es necesario avisar a todos los interlocutores del cambio de dirección.

El envío de mensajes no solicitados, inadecuados, y a veces de contenido impropio, en cantidad masiva puede considerarse un ataque a la esfera privada del internauta (concepto de *junk email*). No obstante, parecer ser que, cada vez más, el correo indeseado se utiliza para propagar programas maliciosos, lo que le confiere un grado de peligrosidad sin precedentes.

II.1.8.2 Programas maliciosos

Los principales observadores de la seguridad informática, ya sea el CERT[12], el FBI, o incluso el Clusif, declaran en sus informes anuales sobre delincuencia informática, que hay un aumento de los programas maliciosos e indeseables que se ejecutan con desconocimiento del usuario.

Se trata de los programas informáticos siguientes:

- Descargadores e instaladores (*downloaders*) que permiten la descarga de datos (acceso remoto y descarga de programas o recuperación de datos).
- Programas registradores de pulsaciones de teclado (*keyloggers*) que capturan la información introducida por el usuario a través del teclado. Existen igualmente periféricos materiales, (registradores de pulsaciones materiales) indetectables por los programas informáticos que graban los datos.
- «Bots» (abreviatura de robots) que son programas que permiten apoderarse a distancia del control de los sistemas a fin de formar una red de ataques disimulada. Cada día se descubren de 25 a 50 nuevos robots. Sirven para retransmitir correos indeseados, programas de usurpación de identidad y para distribuir programas informáticos de intromisión de publicidad (*adware*). En octubre de 2005, la policía holandesa arrestó a tres hombres sospechosos de dirigir una red de 100 000 ordenadores – robots que se proponían realizar ataques de denegación de servicio y se interesaban en las cuentas de PayPal e Ebay de sus víctimas.[13]
- Programas informáticos de publicidad (*adware* – software publicitario) que permiten, entre otras cosas, la personalización de las transacciones comerciales.

---

12 CERT: *Computer Emergency Response Team*; www.cert.org – Estadísticas 1998 – 2005 www.cert.org/stats/cert_stats.html

13 Fuente: Clusif Panorama de la cybercriminalité rapport 2005: www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k5-fr.pdf

– Programas informáticos espía (*spyware* – software de espionaje) que, como su nombre indica, graban datos sin conocimiento del usuario. Según el fabricante de programas informáticos Webroot INC., hay más de 100 000 programas espía distintos en la red y más de 300 000 sitios de Internet que albergan estos programas. Un PC conectado a Internet posee un promedio de 28 programas espía instalados sin que su usuario lo sepa. Más del 80% de los ordenadores de una empresa contienen como mínimo un programa espía. Estos programas son responsables del 70% de los ataques.

A este software hay que añadir los virus y sus derivados (gusanos, troyanos y bombas lógicas).

Los virus son programas maliciosos introducidos en los sistemas sin conocimiento de los usuarios, que tienen la capacidad de reproducirse, ya sea de manera idéntica, ya sea modificándose (virus polimórficos), para atacar entornos en los que se ejecutan, y contaminar a aquellos con los que se relacionan. Se distinguen distintos tipos de virus en función de su signatura, de su comportamiento, de su tipo de reproducción, de la infección, de los problemas de funcionamiento ocasionados, etc.

El objetivo de un virus informático, a semejanza del biológico, es reproducirse y propagarse de un ordenador a otro, incrustándose en todo tipo de programas, fundamentalmente en los mensajes electrónicos y generalmente con intervención humana. La activación de un virus puede atacar la integridad de los recursos informáticos contaminados. Algunos de ellos pueden resultar simplemente molestos mientras que otros son claramente destructivos, y pueden ocasionar pérdidas de disponibilidad y de confidencialidad.

La palabra virus designa genéricamente a todo programa informático capaz de ocasionar molestias (infección, destrucción, desvío de recursos, etc.), reproducirse y propagarse.

En 2005 circularon 50 000 virus nuevos[14]. El virus HTML_NETSKY.P, por ejemplo, registrado por el *World Virus Tracking Center*, ha infectado cerca de 855 244 máquinas en todo el mundo desde abril de 2004. El coste para las empresas infectadas por virus en el año 2004, según el *Computer Security Institute*, viene a ser del orden de 42 millones de USD. Según F-secure.com cada día hay 4 000 virus en circulación.

Los gusanos, los troyanos y las bombas lógicas son códigos maliciosos de la familia genérica de los virus.

Los gusanos son programas que se difunden a través de la red, casi siempre sin intervención humana y que, por lo general, pretenden acaparar los recursos (memoria, ancho de banda de transmisión) socavando de este modo el criterio de disponibilidad o favoreciendo la toma de control a distancia de los sistemas infectados.

Los programas maliciosos calificados de troyanos (*Troyan horse*) se introducen subrepticiamente en los sistemas, a menudo al socaire de programas inocuos o de ayuda, para controlarlos a fin de robar tiempo de procesador, alterar, modificar y destruir datos y programas, provocar anomalías de funcionamiento, efectuar escuchas ilícitas y también para provocar otros daños y servir de enlace a ataques posteriores.

Las bombas lógicas (*logical bomb*) son virus que se activan con ocasión de determinados acontecimientos (cumpleaños, por ejemplo) para atacar los sistemas en los que se encuentran.

Por contra, un *bug*, palabra de origen inglés, consiste en un error de programación. Por extensión se aplica a los defectos de concepción o de implementación que se manifiestan como anomalías de funcionamiento.

En principio, los virus se propagan y se ejecutan si el usuario los activa ejecutando los programas en los que aquellos residen. Hasta el momento, la mayor parte de los virus se propagan gracias a los ficheros adjuntos a los mensajes electrónicos (*email attachement*) y se activan cuando los usuarios pulsan dos veces sobre ellos para abrirlos.

---

14 Fuente: IPA/ISEC Computer virus incident report.

Hay un gran número de programas maliciosos camuflados como herramientas de ayuda a la navegación, a la conexión, a la personalización de servicios, etc. pero que en realidad son mayoritariamente herramientas de captura de información (robo de información, captura de contraseñas y de tráfico), de apropiación de recursos y de ataque. Permiten difundir y manejar herramientas de ataque de denegación de servicio distribuido (DDoS). Actualmente hay varios miles en circulación que tienen como fin la obtención de beneficios económicos.

Los ataques de denegación de servicio (DoS, *Denial of Service*) y los de denegación de servicio distribuidos (DDoS, *Distributed Denial of Service*) son los que afectan a la disponibilidad de recursos. Suelen realizarse solicitando de modo abusivo los servicios normalmente ofrecidos por un servidor, forzando la imposibilidad de que el sistema preste el servicio para el que está concebido (de ahí el nombre de denegación de servicio). Debido al carácter «normal» de la demanda de servicio, los ataques de denegación de servicio son muy difíciles de contrarrestar (ya que lo que perjudica a la infraestructura es la gran cantidad de peticiones) y resultan aún más difícil de contrarrestar cuando se realizan desde varios puntos o sistemas (concepto de ataque de denegación de servicio distribuido).

El vector de introducción de un programa informático malicioso puede ser un programa informático gratuito o de prueba, un sitio pornográfico o de juegos, el correo electrónico, el correo indeseado o un foro de debate.

Su uso se desvirtúa con independencia del modo de introducción, e incluso si se han instalado con el consentimiento inicial o el acuerdo implícito del usuario, lo que puede ocurrir cuando se trata de *adware* aunque en ningún caso con el *spyware*. Con frecuencia, se ejecutan sin el consentimiento de los usuarios. Estos programas informáticos capturan datos y los transfieren sin conocimiento del usuario (observación de los hábitos de navegación para realizar publicidad personalizada) y pueden servir de intermediarios para la realización de actividades ilegales (reenvío de correo indeseado o de programas de usurpación de identidad, por ejemplo) a fin de procurar el enriquecimiento de la entidad de la que proceden. La detección y desinstalación de estos programas informáticos resulta a veces difícil. El internauta no suele tener los conocimientos ni las herramientas necesarias para controlar este riesgo.

La suplantación de identidad (*phishing*) consiste en utilizar la mensajería electrónica para engañar e incitar a los internautas a entregar información sensible que se explotará acto seguido con fines maliciosos (estafa o malversación de información). En septiembre 2005 había más de 5 259 sitios de suplantación de identidad activos que afectaban a más de 110 marcas según el Journal du net del 26.01.2005[15].

La expresión «suplantación de identidad» se utiliza para designar una técnica consistente en engañar a los internautas (a menudo por medio de un mensaje electrónico) a fin de incitarlos a entregar información sensible o de carácter personal, (generalmente solicitándoles que se conecten a un sitio web que se asemeja al propio de la entidad que conocen y a cumplimentar los formularios que se encuentran a disposición de los malhechores).

La información comunicada por el internauta, especialmente su identidad virtual, se utilizará acto seguido con fines maliciosos, estafas, fraudes, etc. bajo el nombre de los internautas engañados.

Por analogía a la pesca con caña (*fishing*) que se realiza con anzuelo y cebo, la pesca electrónica de datos sensibles se realiza por medio de un cebo que induce al usuario a entregar voluntariamente la información codiciada por los malhechores.

Aunque la mayor parte del tiempo las tentativas de usurpación de identidad se realizan mediante la recepción de un mensaje que parece auténtico y que se supone ha sido emitido por una entidad real con la que el internauta está en contacto (correos, banco, comercio o sitio de subastas, por ejemplo), puede realizarse por teléfono o directamente por una persona e incluso a través del teléfono móvil o mediante una aplicación de mensajería instantánea (*Instant Messaging*, IM).

---

15 www.journaldu net.com

II.1.8.3 Tendencias

Hoy en día, los virus ya no tienen por objetivo principal la destrucción masiva y gratuita de datos. Se han vuelto más pragmáticos y se orientan a la obtención de beneficios. Su finalidad es mucho más inteligente que la original y el capital invertido les permite realizar fraudes. Los virus son vectores que permiten realizar delitos financieros que suelen estar al servicio de la delincuencia organizada y constituyen medios de enriquecimiento para sus autores.

En lo que se refiere, por ejemplo, al aumento del correo indeseado e inconveniencias asociadas, el CLUSIF[16] ha publicado que AOL filtró 500 mil millones de mensajes de correo indeseado en 2003 y que el emisor de correo indeseado más prolífico del mundo, descubierto en diciembre de 2003 por la Asociación anticorreo indeseado Spamhaus[17] llegó a enviar 70 millones de mensajes electrónicos en un solo día.

También según el CLUSIF, en mayo de 2003, «*Buffalo spammer*» fue condenado en Estados Unidos a pagar una multa 16,4 millones de USD al proveedor de servicios de Internet Earthlink, por haber enviado 825 millones de mensajes no solicitados. Según Ferris Research el correo indeseado costó al mundo de los negocios en 2003, 2,5 millones de USD en Europa y 8,9 millones de USD en Estados Unidos. Si esto se añade a los 500 millones de USD invertidos por los proveedores de servicios para bloquear el correo indeseado, se puede calificar a este abuso de la mensajería electrónica de verdadero problema que en ningún caso se debe ignorar.

Además de las pérdidas directas ocasionadas por los fraudes, es necesario considerar los costes generados por la interrupción del servicio que conlleva la discontinuidad de las operaciones, la pérdida de volumen de ventas, los daños colaterales, la pérdida de imagen y de reputación, etc., así como los costes de recuperación del estado operacional de los sistemas. Esto representa sumas nada despreciables para las organizaciones que han sido víctimas de ataques informáticos.

Se observa, pues, que el número de ataques no cesa de crecer y que los virus informáticos constituyen auténticas pandemias. Los fenómenos de usurpación de identidad se prodigan cada vez más y son cada vez más sofisticados, como también ocurre con los fraudes, las estafas y diversas formas de chantaje que son ya realidades cotidianas del ciberespacio. Esto afecta a todo el mundo e incide en todos los sectores de actividad superando las barreras geográficas y temporales.

Todos: sistemas, plataformas materiales y programas informáticos, así como todos los sistemas de explotación se ven afectados, sin olvidar los sistemas que permiten la movilidad de los usuarios (ordenadores portátiles y teléfonos móviles).

II.1.9 Principales delitos favorecidos por Internet

II.1.9.1 Estafa, espionaje y actividades de inteligencia, tráficos varios y chantaje

Todos los crímenes y delitos «comunes» (intimidación, trata de seres humanos, estafa, robo, etc.) cometidos por las organizaciones delictivas, son beneficiarios potenciales de las nuevas tecnologías de información y principalmente de Internet. A grandes rasgos, el servicio de comunicación que ofrece Internet favorece cualquier tipo de tráfico, ya sea el de armas o el de seres humanos, y de estafa (ataques contra la propiedad, ataques contra los sistemas de infraestructuras informáticas, robo de datos, ataques a los derechos de autor, etc.).

Internet permite a los estafadores hacer estragos de diversas maneras. Por una parte están los que usurpan una identidad a fin de disfrutar de prestaciones sin pagar por ellas. Su herramienta de trabajo suele ser un programa informático de suplantación de tarjetas de crédito «*carding*» que permite crear números de tarjetas de crédito perfectamente válidos sin correspondencia alguna con números de cuenta reales, que les permite efectuar compras en línea y ordenar la entrega en una determinada

---

16 CLUSIF – Club de la Sécurité des Système d'Information Français: www.clusif.asso.fr

17 Asociación Spamhaus: www.spamhaus.org

dirección de conveniencia de un solo uso. El coste lo soportará el sistema bancario o el comerciante. El usuario final también queda afectado cuando el número de su tarjeta de crédito haya sido entregado por un carterista o un comerciante poco escrupuloso a una red especializada.

Otra familia de estafadores es la constituida por los que ofrecen prestaciones inexistentes (venta de diplomas, pasaportes diplomáticos de Estados imaginarios, subastas de productos inexistentes, etc.).

También se facilitan las actividades de espionaje y de inteligencia debido a la facilidad existente hoy en día para interceptar ilegalmente la información transmitida por Internet.

Cabe observar que la utilización sistemática de medios de comunicación y de seguridad de información, como el encriptado, por parte de terroristas profesionales, permite mejorar también su propia seguridad y limitar la cantidad de información que la policía puede recuperar.

Internet es un potente medio que favorece la difusión de métodos que permiten cometer crímenes y delitos, lo que facilita a algunos el paso a la ilegalidad.

II.1.9.2 Ataques contra las personas

Internet permite que se constituyan comunidades virtuales clandestinas para entregarse a prácticas rigurosamente castigadas por la ley. Puede tratarse de pornografía, pedofilia o de películas *snuff* (películas que muestran escenas de violencia y tortura realizadas sobre víctimas, y que en algunos casos suponen la muerte de las personas maltratadas). Este tipo de actividad suele estar relacionado con la trata de seres humanos, especialmente mujeres y niños. El intercambio de películas y fotos es mucho menos fácil de interceptar por la policía. Cada vez más, el hecho de que los servidores estén instalados en países donde no hay fuerzas de policía o donde éstas están desbordadas, así como el de la utilización de la encriptación, de servidores IRC (*Internet Relay Chat*) privados, activos durante periodos muy limitados y de intercambios P2P (*peer to peer*), confieren más libertad de acción a los delincuentes.

Estas actividades ilícitas entran en el ámbito del derecho común. Cabe preguntarse entonces si su comisión casi industrializada y a gran escala, gracias a Internet y a la movilidad de personas y bienes, no las convierten en auténticos delitos contra una parte de la humanidad.

En lo que se refiere a los ataques a la personalidad, cabe citar por ejemplo: los ataques a la vida privada, a la representación de la persona, al secreto profesional y a los derechos de la persona, resultantes de ficheros o procesos informáticos. En lo que se refiere a los ataques a menores, cabe citar la difusión de mensajes pornográficos susceptibles de ser vistos por aquellos.

I.1.9.3 Falsificaciones

La facilidad con que la información digital puede reproducirse, ha contribuido a la aparición de un mercado de copias ilícitas. Esto representa unas ventas no realizadas de varias decenas de miles de millones de USD para los distintos editores en los sectores de los programas informáticos, la música e incluso los vídeos domésticos, entre otros.

Por otra parte, se constata un aumento muy importante del número de trabajos escolares y universitarios realizados por simple copia de documentos de la web.

Las infracciones del código de la propiedad intelectual pueden ser numerosas: falsificación de obras originales (incluidos los programas informáticos), de diseños, modelos, marcas, etc.

II.1.9.4 Manipulación de la información

La manipulación puede adoptar diversas formas, como por ejemplo la difusión de documentos internos de una empresa de manera que se provoque su desestabilización, el envío de correos electrónicos instando a los destinatarios a realizar entregas de dinero en sitios falsos, etc.

Internet es una herramienta excelente para propalar rumores y cualquier forma de intoxicación. Favorece igualmente las infracciones de prensa, la instigación de crímenes y delitos, la apología de delitos contra la humanidad, la apología del terrorismo e incitación al mismo, la incitación al odio racial, el negacionismo, las difamaciones, injurias, etc.

En la Figura II.5 se presentan algunos ejemplos de delitos facilitados por Internet.

Figura II.5 – Ejemplos de delitos facilitados por Internet

Crímenes y delitos contra las personas – Ataques a la personalidad – Ataques a la vida privada – Ataques a la representación de la persona – Denuncias calumniosas – Ataque al secreto profesional – Ataque a los derechos de la persona resultante de ficheros o procesos informáticos – Ataques a menores, etc.
Crímenes y delitos contra los bienes – Estafa – Ataques a los sistemas informáticos – Infracciones de prensa
Incitación al crímenes y al delito – Apología de los delitos contra la humanidad – Apología del terrorismo e incitación al mismo – Incitación al odio racial – Negacionismo – Difamación – Injurias
Infracción del código de la propiedad intelectual – Falsificación de invenciones (incluidos los programas informáticos) – Falsificación de diseños y modelos – Falsificación de marcas – Participación en la explotación de casas de juegos de azar (cibercasino)

II.1.9.5 Función de las instituciones públicas

Las instituciones públicas necesitan más que nunca desempeñar su función tradicional de persecución y represión de los fraudes y delitos. Asimismo deben ser activas en materia de sensibilización y de información de la población. Sería extremadamente útil poder disponer de elementos de referencia relativos a la protección de las personas y bienes cuando se utiliza Internet.

Cada vez será más peligroso permitir que las fuerzas de orden queden retrasadas en el dominio tecnológico. Efectivamente, un eventual esfuerzo de puesta al día tras varios años no solamente tendría un coste financiero directo, consecuencia de las inversiones en nuevas infraestructuras, sino también y sobre todo un coste social por el auge de la influencia de las estructuras mafiosas o asimiladas sobre la sociedad, con todos los riesgos de desestabilización que ello comporta.

Sin embargo, el crecimiento excesivo de la presencia policial en la red no es forzosamente deseable, ya que puede entrar en conflicto con la necesidad de confidencialidad de los intercambios y de respeto a la esfera privada de los individuos.

II.1.10 Incidentes de seguridad y cifras ocultas de la ciberdelincuencia

Conviene destacar la escasez de estadísticas sobre ciberdelincuencia. Se trata de un nuevo ámbito de expresión de la delincuencia en el que se denuncian pocos asuntos a la policía. Además, estas infracciones se perpetran a nivel mundial, pero como las legislaciones penales son nacionales resulta a veces difícil refundir estadísticas de delitos cuya calificación varía entre los diversos países. Por ejemplo, cuando se utiliza un sistema informático para una transacción financiera fraudulenta tras la usurpación de los parámetros de conexión de un usuario: ¿Se trata de un delito informático o financiero?

Sin embargo, la creación en Estados Unidos de equipos de investigación informática y valoración de amenazas a las infraestructuras (CITA, *Computer Investigation and Infrastructure Threat Assessment*) descentralizados y coordinados por el Centro Nacional de Protección de las Infraestructuras (NIPC, *National Infrastructures Protection Center*) pone de manifiesto indirectamente la magnitud de la ciberdelincuencia.

El número de incidentes de seguridad denunciados al CERT[18] continúa creciendo desde comienzos de los años 2000 y el número de ataques declarados a las instancias judiciales tiende igualmente a aumentar a lo largo de los años, lo que contribuye al mejor conocimiento y toma de conciencia de la delincuencia informática. En el año 2003 se produjo un aumento significativo del volumen de correo indeseado, que ya no se limitó a Internet sino que afectó igualmente a los SMS. También se consiguió detener y arrestar a varios emisores de correo indeseado. Hubo operaciones policiales de envergadura, tanto en Estados Unidos (operación E-Con en mayo de 2003 y Cyber-Sweep en octubre de 2003) como en Europa (España, Italia, Francia, Reino Unido, etc.), lo que demuestra que las autoridades reaccionan y se adaptan a este nuevo contexto delictivo. El arresto y condena de algunos autores de virus y de correo indeseado son prueba manifiesta de la voluntad de represión de estas nuevas formas de agresión. Sin embargo, el número de condenas sigue siendo pequeño en relación con la importancia cuantitativa del correo indeseado y de los virus que circulan diariamente[19].

Las cifras ocultas de ciberdelincuencia son difíciles de estimar. Se calcula que sólo el 12% de los ciberdelitos llegan a ser conocidos por las instancias judiciales y policiales y por el público en general[20]. Resulta verdaderamente difícil obtener una estadística real de la delincuencia informática, y esto constituye un verdadero obstáculo para el análisis del fenómeno y contribuye al desconocimiento de su magnitud.

La ausencia de estadísticas oficiales se debe en parte al hecho de que las organizaciones:

- no desean necesariamente comunicar los ataques sufridos;
- ignoran que son víctimas de ataques, especialmente de los pasivos (desvío transparente de datos, de flujos, escuchas clandestinas, intromisión no detectada en sistemas, etc., o sólo se enteran a posteriori cuando toda acción de respuesta carece de sentido;
- no saben gestionar una situación de crisis;
- no tienen suficiente confianza en las instancias judiciales y policiales ni en su competencia para abordar este tipo de problemas;
- prefieren tomarse la justicia por su mano.

Los conocimientos técnicos de los atacantes, la sofisticación y eficacia de los ataques, las herramientas informáticas de que disponen y los instrumentos de los ataques así como el número de éstos, no cesan de crecer. Este dinamismo supone una complejidad creciente del fenómeno a controlar. Sin una voluntad política decidida, la asunción de responsabilidad por parte de todos los agentes a nivel internacional y una colaboración eficaz de los sectores público y privado, toda medida de seguridad, ya sea de orden tecnológico o legislativa, sólo constituirá una solución insuficiente y fragmentaria de la seguridad que resultará por consiguiente ineficaz para controlar la delincuencia informática.

---

18 CERT Coordination Center, Carnegie Mellon University (http://www.cert.org)

19 La Information Technology Promotion Agency Information Security Center (IPA/ISEC – Japón) ha censado 85 059 virus en diciembre de 2003 – «Computer Virus Incident Reports». 2004. www.ipa.go.jp/security/english/virus/press/200401/virus200401-e.html

20 Vladimir Gobulev «Computer crime typology» – 9 de enero de 2004 – Computer Crime Research Center www.crime- research.org/articles/Golubev1203/

II.1.11 Prepararse para la amenaza de la ciberdelincuencia o el deber de protegerse

Es necesario prepararse para la amenaza de la ciberdelincuencia que antes o después se cumplirá.

Se trata de organizar la protección y defensa de los valores tomando en consideración la amenaza de riesgo delincuente cuando se define la estrategia de seguridad. Resulta difícil identificar a los agentes de la ciberdelincuencia, su modo de actuar y sus motivos, pero se sabe que las organizaciones delictivas suelen actuar de manera oportunista y atacan preferentemente a los elementos vulnerables. La organización podrá evitar convertirse en blanco prioritario de la ciberdelincuencia en la medida en que proteja eficazmente, es decir mejor que los demás, su infraestructura informática y rechace la filosofía de que la seguridad consiste en tener el mismo grado de inseguridad que la competencia. El riesgo ciberdelictivo se transforma entonces en un incentivo para implementar una seguridad de calidad.

Por contra, si los agentes tradicionales de la delincuencia consideran a la organización como una fuente de riqueza o un símbolo a destruir, la señalará como objetivo a atacar. En este caso, se puede contemplar la posibilidad de que la organización quede destruida como consecuencia de actos terroristas. Así pues, hay que implementar una estrategia de protección y de defensa adecuada. Sin embargo, los instrumentos tradicionales de seguridad y de gestión de riesgos tienen escasa eficacia para afrontar los riesgos de origen delictivo, ya que algunos de ellos son inevitables salvo que se suspenda la conexión con Internet.

El riesgo delictivo tiene una dimensión mundial y afecta en su integridad a las instituciones (accionistas, dirigentes, empleados, herramientas de producción, etc.). Éstas deben saber preservar su integridad frente al riesgo delictivo, del mismo modo que saben protegerse de los riesgos de corrupción, por ejemplo. Deben ser rentables y compensar las ventas no realizadas debido al riesgo ciberdelictivo y el coste de las medidas a adoptar para controlarlo. Debe diseñarse pues un modelo económico que soporte de la mejor manera posible el coste de protección de las infraestructuras, de la seguridad de los sistemas, redes, datos y servicios, en detrimento del desarrollo económico, a cargo de los que comparten el valor creado por las organizaciones.

La toma de conciencia de la fragilidad del mundo digital y de la falta de control total, no solamente de las tecnologías e infraestructuras informáticas y de telecomunicaciones, sino también de las soluciones de seguridad comercializadas, nos obliga a plantearnos la cuestión fundamental de la dependencia de tecnologías que escapan a nuestro control.

Se trata de preguntarse hasta qué punto es deseable depender de un proveedor, de un país o de un administrador.

El primer paso para el control del riesgo ciberdelictivo pasa por:

- el replanteo de la relación con las nuevas tecnologías y los proveedores;
- la exigencia de una garantía de seguridad;
- la responsabilidad del conjunto de los agentes.

Antes de adoptar las medidas de seguridad tradicionales con un planteamiento preventivo, proteccionista y defensivo, debemos proteger los recursos sensibles y críticos de la organización replanteando antes que nada su relación con las nuevas tecnologías.

Se debe exigir:

- la utilización de productos de calidad cuyo nivel de seguridad pueda ser controlable y verificable;
- que la seguridad ya no se realice en la oscuridad sino que sea transparente;
- que la seguridad no dependa únicamente de la responsabilidad de los usuarios sino también de los intermediarios técnicos – responsabilidad jurídica de los profesionales (diseñadores de programas, proveedores de acceso, etc.);
- que se integre un mínimo de seguridad en modo nativo en las soluciones tecnológicas (concepto de productos seguros).

Independientemente de la preocupación de las organizaciones por la sinergia y la convergencia del delito organizado, del delito económico y del ciberdelito, se debe ofrecer una respuesta completa, multilateral y transnacional para reforzar la confianza de los agentes económicos en las tecnologías de la información y disminuir las oportunidades delictivas.

Esta respuesta debe satisfacer las necesidades de la seguridad del Estado, de las organizaciones y de los individuos. Debe contribuir asimismo a limitar hasta un nivel aceptable la ciberdelincuencia, a infundir confianza en el mundo digital y a reducir al mínimo el riesgo de corrupción y de amenaza de los poderes públicos.

Capítulo II.2 – Los ciberataques

II.2.1 Características de los ciberataques

Hay varios modos de explotar fraudulentamente las posibilidades ofrecidas por las tecnologías de Internet. Suelen basarse en la usurpación de los parámetros de conexión, de las contraseñas de los usuarios legítimos, y también en el engaño y la explotación de los fallos y vulnerabilidades de las tecnologías.

II.2.2 Apropiación de las contraseñas de los usuarios para penetrar en los sistemas

Los principales medios que permiten la obtención de los parámetros de conexión de los usuarios legítimos para introducirse en los sistemas son los siguientes:

- Obtención directa: la contraseña es evidente (nombre de la persona, de su cónyuge, de sus hijos, fechas de nacimiento, etc.), el usuario entrega directamente la contraseña al malhechor.
- Obtención por engaño del usuario (concepto de ingeniería social): el estafador se hace pasar por un administrador y solicita las contraseñas a los usuarios aduciendo razones de índole técnica, por lo que éstos las entregan en la mayor parte de los casos.
- Obtención por escucha de tráfico: el malhechor intercepta y escucha los datos no codificados transmitidos por los protocolos de comunicación (escucha pasiva (*sniffing*), vigilancia del tráfico de la red (*monitoring*)).
- Obtención por medio de un programa informático: se introduce un «troyano» en la estación de trabajo del usuario que graba sin su conocimiento sus parámetros de conexión a sistemas remotos.
- Obtención por acceso al fichero de contraseñas.
- Obtención por desencriptación de las contraseñas encriptadas (*cracker*).
- Obtención por observación de los usuarios gracias a la activación de periféricos multimedios que graban sus parámetros de conexión.

Una vez en posesión de las claves de acceso a los sistemas (identificación de la combinación usuario, contraseña), resulta fácil penetrar en ellos y efectuar todo tipo de operaciones de lectura y escritura. El objetivo para el pirata informático consiste entonces en no dejarse detectar ni dejar rastros de su presencia en los sistemas visitados.

II.2.3 Ataque de denegación de servicio

Puede realizarse un ataque que provoque la denegación o rechazo del servicio, solicitando abusivamente los recursos. Como no disponen de la capacidad de procesar tal flujo de demandas, los sistemas atacados, sobrecargados por un número excesivo de peticiones, se caen y quedan no disponibles. Se pueden perpetrar estos ataques aprovechando los fallos del sistema operativo y utilizando por ejemplo las características internas, principalmente las de gestión en ciertas zonas de memoria intermedia (ataques por desbordamiento de la memoria intermedia, *buffer overflow attack*) lo que comportará graves problemas de funcionamiento que pueden provocar la parada total de los sistemas.

Un ataque por inundación de mensajes (bombardeo de correo electrónico), consistente en la inundación del buzón de correo electrónico de un usuario, puede provocar una denegación de servicio.

II.2.4 Ataques por modificación de la página web

Los ataques por modificación de la página de bienvenida de un sitio web (*defacement attack*) se realizan sustituyendo la página web de un sitio por otra cuyo contenido (pornográfico, político, etc.) varía según la motivación de los atacantes. Una variante de este tipo de ataques consiste en redireccionar al usuario hacia un sitio falso, copia exacta de aquél al que se pretendía conectar, a fin de obtener, por ejemplo, el número de su tarjeta de crédito. Este tipo de ataque es el que se realiza en las operaciones de suplantación de identidad (*phishing*).

Los contenidos de los sitios de información pueden modificarse igualmente con fines de desinformación (para influir en el desarrollo de acontecimientos, desestabilizar, manipular a la opinión pública, etc.). Los ataques semánticos (*semantic attack*) que afectan al propio sentido de las informaciones, entran en la categoría de infoguerra (*infowar*).

II.2.5 Ataques basados en el engaño y en la alteración del modo operativo de los protocolos

Todos los protocolos de la familia TCP/IP (*Transmission Control Protocol/Internet Protocol*) pueden alterarse para atacar la seguridad de los sistemas. Lo mismo ocurre con los protocolos y mecanismos que contribuyen al encaminamiento de los datos a través de la red. Así por ejemplo, en una sesión de trabajo entre un cliente y un servidor, puede producirse un robo de sesión TCP.

Efectivamente el protocolo TCP (*Transmission Control Protocol*) establece, para ejecutarse, una conexión lógica entre los dos corresponsales y soporta el intercambio de datos de la aplicación entre estos últimos. Ahora bien, para conectar las aplicaciones distribuidas, TCP utiliza «números de puerto» (*port numbers*) que no son sino identificadores lógicos de las aplicaciones. Algunos son específicos, están reservados a programas concretos y son bien conocidos de los usuarios; otros sin embargo se asignan dinámicamente en la conexión con arreglo a un algoritmo determinado. El ataque por número de puerto TCP consiste en adivinar o predecir los próximos números de puertos afectados para el intercambio de datos a fin de utilizarlos en lugar del usuario normal, suplantando al mismo. De este modo, se pueden «atravesar» los cortafuegos y establecer una conexión «segura» entre dos entidades (la entidad pirata y el objetivo). Ciertamente, la entidad original, que ha sido sustituida, no podrá comunicarse con la entidad remota; bastará entonces con enviarle un mensaje indicándole, por ejemplo, que el sistema solicitado está inactivo.

El protocolo de datagrama de usuario (UDP, *User Datagram Protocol*) es un protocolo de nivel 4 (transporte) que se ejecuta en modo no conectado. Constituye una alternativa al protocolo TCP para la transferencia rápida de un volumen pequeño de datos. Las comunicaciones UDP no están sometidas a mecanismos de control. El protocolo UDP no controla la identificación ni el flujo ni los errores, por lo que no importa que pueda utilizar la dirección IP de un interlocutor autorizado a conectarse a un sistema y aprovecharse de ello para penetrar en éste. Pueden producirse asimismo robos de sesión UDP sin que los servidores de aplicaciones se enteren de ello.

Además, resulta bastante fácil, cuando se conoce el modo operativo de los diferentes protocolos, que es público, manipular su uso, generar paquetes falsos para sobrecargar la red por ejemplo e inundarla para provocar denegaciones de servicio. De este modo, se llega al criterio de seguridad relativa a la disponibilidad de la red y de los servicios.

Los delincuentes informáticos saben aprovechar perfectamente las ventajas de los protocolos y sus limitaciones para:

- paralizar la red;
- reencaminar los paquetes IP hacia un destino falso (el de ellos, por ejemplo);
- aumentar considerablemente la carga de los sistemas obligándoles a procesar en vano un gran número de mensajes sin importancia;
- impedir que un emisor envíe datos;
- controlar el flujo de emisión de paquetes, lo que tiene igualmente consecuencias para el tráfico soportado por la red y afecta a su rendimiento (fiabilidad, seguridad de funcionamiento).

Generalmente, los ataques a nivel del encaminamiento se basan en la confusión de los encaminadores, de las pasarelas y de los destinatarios, al facilitarles informaciones de direccionamiento falsas que permiten desviar los datos.

Utilizando, por ejemplo, ciertas facilidades opcionales del protocolo IP que permiten definir el trayecto, es decir especificando las direcciones de los sistemas intermedios por los que debe pasar un determinado paquete, y falsificando dichas direcciones, el malhechor puede redireccionar fácilmente los paquetes hacia el destino que elija.

Los atacantes no sólo saben aprovechar el modo de funcionamiento de los protocolos de comunicación sino que además saben cómo sacar partido de las características de los sistemas de explotación y de su modo de funcionamiento. De este modo, los desbordamientos de capacidad de ciertas zonas de memoria intermedia en los sistemas (ataques por desbordamiento de memoria intermedia, *buffer overflow attack*) comportan disfunciones graves que pueden provocar su detención. Los blancos de este tipo de ataque son, por supuesto, todos los sistemas que desempeñen un papel importante en la realización de servicios, ya sea para el encaminamiento de datos, como los encaminadores, o para la gestión de nombres y direcciones, como los servidores de nombre, por ejemplo. La mayor parte de los ataques contra los sitios web los dejan fuera de servicio y se basan en la explotación de los fallos de su sistema operativo.

II.2.6 Ataques contra las infraestructuras críticas

Las infraestructuras críticas esenciales para el buen funcionamiento de la sociedad (energía, agua, transportes, logística alimentaria, telecomunicaciones, bancos y servicios financieros, servicios médicos, funciones gubernamentales, etc.), resultan más vulnerables por su creciente utilización de las tecnologías de Internet que permiten el acceso a las mismas desde la red de redes.

Además, es necesario subrayar la importancia particular de la vulnerabilidad de los sistemas de producción y distribución de electricidad. Éstos constituyen una infraestructura vital, y por lo tanto, crítica, en la medida en que condiciona el funcionamiento de la mayor parte de las demás infraestructuras. La complejidad y el carácter distribuido de las relaciones entre las distintas infraestructuras críticas es a la vez causa de fuerza y de vulnerabilidad.

Es fundamental asegurar las pasarelas hacia Internet de las redes de gestión de estas infraestructuras y crear, ya sea a nivel regional o nacional, organismos encargados de la protección de las infraestructuras críticas cuya misión principal sea la de coordinar la concepción y actualización de los planes de protección de cada una de estas infraestructuras. Efectivamente, la coherencia y compatibilidad de estos planes y soluciones de seguridad es primordial en caso de crisis que afecte simultáneamente a varias de ellas.

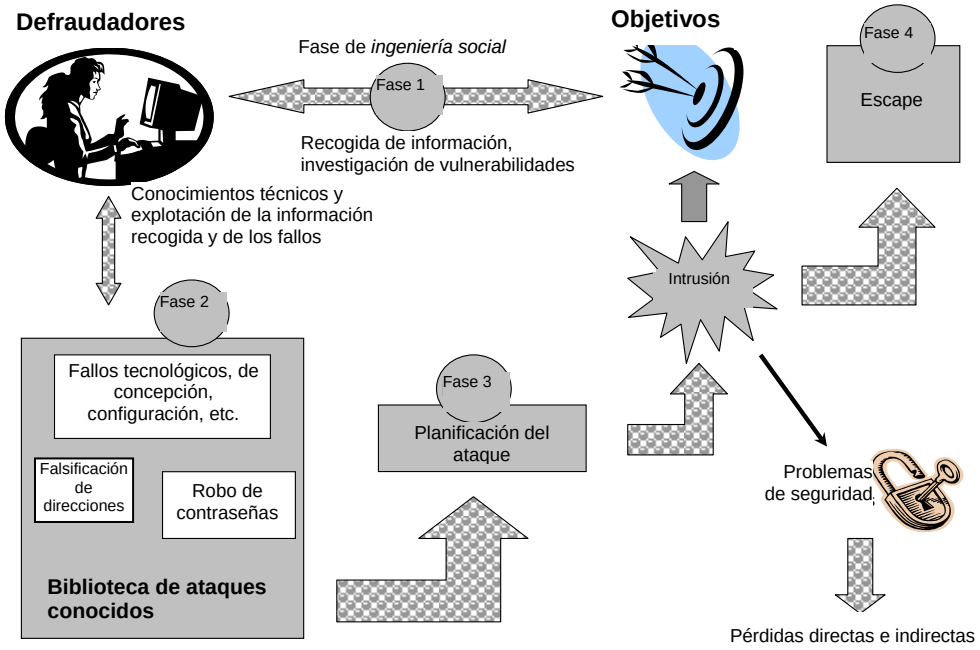
II.2.7 Modelo de desarrollo de un ciberataque

En la Figura II.6 se presentan las distintas fases de desarrollo de un ataque[21].

La primera fase, recogida de información e investigación de la vulnerabilidad de un sistema, tiene por objeto recoger el máximo de información sobre el sistema objetivo a fin de explotarla. Consiste en conocer los mecanismos y niveles de seguridad vigentes relativos a la identificación, autenticación, control de acceso, criptografía, vigilancia y a identificar los fallos técnicos, organizativos, humanos y medioambientales. El atacante se aprovechará sobre todo de la ingenuidad y de la credulidad de los usuarios para sonsacarles información que facilite la ejecución del ataque (concepto de *ingeniería social*).

[21] Reproducción del libro «Sécurité informatique et télécoms: cours et exercices corrigés»; S. Ghernaouti-Hélie; Dunod 2006.

Figura II.6 – Fases características del desarrollo de un ataque



Además, el defraudador intentará detectar y explotar los fallos de seguridad conocidos sin resolver (no *parcheados*) y utilizar las herramientas disponibles (concepto de biblioteca de ataques o de caja de herramientas de ataque) para introducirse en los sistemas. La fase de escape tiene por objeto principal evitar que el ataque sea detectado y que el atacante deje rastros que puedan servir para su identificación. Para contribuir a esto, intentará permanecer en el anonimato, utilizar alias (seudónimos), usurpar la identidad digital de los usuarios e incluso borrar las pistas pasando por varios sistemas intermedios o de enlace.

SECCIÓN III

PLANTEAMIENTO TECNOLÓGICO

Capítulo III.1 – Infraestructuras de telecomunicación

III.1.1 Características

La gran cobertura geográfica de la red telefónica la ha convertido en una red preferente que da servicio a un gran número de usuarios. Su infraestructura permite utilizarla hoy en día no sólo para transportar datos vocales sino también datos informáticos. De este modo es posible, siempre que se disponga de interfaces adaptadas, comunicar los ordenadores a través de la red telefónica. Además, en estos últimos años se han desarrollado puntos de acceso a Internet, continúan abriéndose nuevos cibercafés y cada vez son más los países que disponen de una infraestructura de transporte accesible y eficaz. A veces se despliegan redes de cable para la transmisión de canales de televisión.

A las infraestructuras fijas de telecomunicación hay que asociar las inalámbricas, que permiten la movilidad de los usuarios y utilizan tecnologías que aprovechan las infraestructuras de los satélites, las espaciales y los sistemas radioeléctricos terrenales. Así por ejemplo, la telefonía móvil ofrece, desde hace pocos años, sus servicios en muchos países en desarrollo.

La norma GSM (*Global System for Mobile Communication*, sistema mundial para comunicaciones móviles) para la transmisión de voz y ocasionalmente de pequeños volúmenes de datos, se ha impuesto ya en varios continentes. La nueva generación de redes móviles con arreglo a las especificaciones de la norma UMTS (*Universal Mobile Telecommunication System*, sistema de telecomunicaciones móviles universales) ofrece mejores características de transmisión y permite aprovechar mejor los teléfonos móviles multimedios. Sin embargo, la evolución de las redes GSM que integran el servicio GPRS (*General Packet Radio Service*, servicio general de radiocomunicaciones por paquetes) permite aumentar la velocidad de transmisión a fin de satisfacer mejor las necesidades de las aplicaciones informáticas en las redes móviles.

Por otra parte, la aparición de tecnologías tales como el GSM supone una mutación tanto tecnológica como comportamental y económica. Efectivamente, el mundo de los teléfonos móviles constituye un dominio en plena expansión que se inscribe en un contexto de competencia mundial desenfrenada. Ya es posible además penetrar en el mercado de las telecomunicaciones, que hasta ese momento estaba reservado a los operadores, con un nuevo servicio, el radioteléfono, construyendo al mismo tiempo una infraestructura que puede utilizarse para cualquier transferencia de datos.

Con independencia de la tecnología utilizada para desplegar los teleservicios, las infraestructuras de telecomunicaciones de los países en desarrollo deben permitir lo siguiente:

– el interfuncionamiento digital generalizado (voz, datos, imagen) de un cierto conjunto de servicios de base fácilmente realizables, mantenibles y con una cobertura geográfica adaptada (tanto nacional como internacional), dentro de un planteamiento de calidad total (oferta permanente, estable y granular cuya selección pueda ser reversible con el mínimo coste técnico y económico) y de seguridad óptima;
– la armonización técnica y comercial; la protección contra la posible constitución de un cártel, para un desarrollo armónico de las infraestructuras y servicios, con garantía de regulación activa de los abusos de las posiciones dominantes.

III.1.2 Principios fundamentales

Una red de telecomunicación está constituida por un conjunto de recursos informáticos y de transmisión concomitantes que ofrece servicios de comunicación. Estos servicios permiten acceder a distancia y compartir recursos informáticos interconectados, relacionar aplicaciones y personas, ejecutar programas a distancia y transferir informaciones.

Para el éxito de las actividades económicas resulta imperativo disponer de una estructura de comunicación eficaz, que relacione y haga posible la cooperación entre toda clase de equipos, aplicaciones informáticas y personas, con independencia de la distancia a cubrir, el lugar y la naturaleza de los flujos de informaciones a transferir.

Las redes se suelen caracterizar por diversos criterios entre los cuales cabe destacar la cobertura geográfica, la topología[22], la tecnología de implementación y las aplicaciones soportadas, el modo de funcionamiento, el tipo de soporte de transmisión (alámbrico o no), su carácter privado o público, etc.

Las redes más antiguas son las de larga distancia[23] (redes telefónicas, télex, Transpac, Internet, etc.). Con la llegada de los microordenadores (a principios de los años 80) aparecieron las redes locales[24].

En los últimos años, estas distinciones tienden a difuminarse en la medida en que las redes se interconectan entre sí. Por ejemplo, una red local puede conectarse con otras para convertirse en una red extensa. Por otra parte, las redes ya no están dedicadas al soporte de un solo tipo de aplicación sino que permiten la transferencia simultánea de voz, datos informáticos e imágenes de vídeo (concepto de red multimedios).

Una red puede ser privada, propia de una organización que se reserva el derecho exclusivo de utilización de la misma, o pública. En este último caso, los servicios de telecomunicación se ofrecen a personas o instituciones diferentes, con arreglo a diversas modalidades de abono.

Las principales tecnologías de transmisión utilizadas para la implementación de redes de área extensa son las tecnologías TCP/IP, la retransmisión de tramas (*Frame Relay*) y el ATM (*Asynchromous Transfer Mode*, modo de transferencia asíncrono). En lo que se refiere al mercado de las redes locales de empresa, la tecnología predominante se basa en Ethernet y sus versiones de alta velocidad (*Fast Ethernet* o Ethernet de alta velocidad y Ethernet conmutada).

En el ámbito de las telecomunicaciones, el transporte óptico y la tecnología de conmutación ATM han marcado un hito en la evolución de las infraestructuras y de los medios de transmisión. Permiten transferencias de alta velocidad y calidad, atribución dinámica de ancho de banda, caudal variable y multiusos.

III.1.3 Elementos constitutivos de las redes

III.1.3.1 Soportes de interconexión

Para conectar los ordenadores entre sí y ponerlos en red, hacen falta soportes de transmisión. Dependiendo de su naturaleza se distingue entre soportes materiales (pares de hilos trenzados, cables coaxiales y fibras ópticas) y soportes inmateriales (haces hercianos y ondas de infrarrojos). Estos soportes tienen características específicas que determinan su fiabilidad y su capacidad para transmitir cantidades de información más o menos importantes, a distintas velocidades.

El caudal permitido por un soporte de interconexión es la cantidad de información transferida durante un periodo de tiempo determinado. Se expresa en kilobits, megabits e incluso terabits por segundo (100 Mbit/s, por ejemplo). Es proporcional a la anchura de banda del soporte de transmisión (*bandwith*) que representa la gama de frecuencias que el soporte deja pasar sin modificación.

---

22 La organización de los enlaces de interconexión y el modo de interconectar los elementos de la red identifican su topología.

23 La red de área extensa o WAN (*Wide Area Network*) interconecta los ordenadores distribuidos por un territorio geográfico más o menos amplio (mayor de 100 km), e incluso mundial.

24 Se dice que una red es local o LAN (*Local Area Network*) cuando interconecta ordenadores en un entorno geográfico limitado a pocos kilómetros (una decena). Una red metropolitana o MAN (*Metropolitan Area Network*) interconecta redes locales que pueden pertenecer a entidades diferentes y cuya dimensión geográfica no sobrepasa los 100 km. Hay una nueva tecnología de reciente aparición para identificar los diversos tipos de recursos interconectados en red e incluso para distinguir un dominio de una cierta aplicación. Por ejemplo, en la literatura especializada se encuentran las siglas siguientes: HAN (*Home Area Network*, red de área doméstica) que interconecta los equipos de un hogar controlados por mando a distancia (horno, vídeo, dispositivos de iluminación y de calefacción, etc.), CAN (*Car Area Network*, red de área del automóvil), SAN (*Storage Area Network*, red de área de almacenamiento), etc.

III.1.3.2 Elementos de conectividad

El tipo de conexión o elemento de conectividad a instalar entre un soporte de transmisión y un ordenador para asociar ambos elementos, depende del tipo de soporte y del modo de transmisión utilizado. Esta caja de empalmes o interfaz de red resuelve los problemas de conectividad y adapta la señal emitida o recibida por el ordenador a la señal que se puede transmitir por el soporte Por ejemplo, un *módem* (MOdulador/DEModulador) hace de interfaz entre un ordenador, que es una máquina digital que trata señales digitales, y un soporte de transmisión tal como una línea telefónica analógica que transmite señales de forma continua[25]. Cualquier elemento electrónico puede conectarse, en teoría, a la red siempre que disponga de una interfaz de conexión material y lógica apropiada.

III.1.3.3 Máquinas especializadas y servidores de información

Además de los sistemas de los usuarios que permiten acceder a una red y los ordenadores dedicados a la gestión y al procesamiento de las aplicaciones (máquinas anfitrión o *host* y servidores de información), hay ordenadores de procesamiento de las comunicaciones que constituyen la infraestructura de transporte de la red. Se encargan de una o varias funciones propias de la gestión e implementación de las telecomunicaciones (optimización y compartición de recursos, encaminamiento de datos, gestión de direcciones, de nombres, interconexión, etc.). Se trata, por ejemplo, de los encaminadores, multiplexadores, concentradores, conmutadores y pasarelas de interconexión.

Para comunicarse, es preciso transmitir la información de modo fiable de acuerdo con las modalidades de intercambio satisfactorias para los corresponsales. Efectivamente, los sistemas interconectados por las redes de telecomunicaciones son en principio diferentes. Para que puedan dialogar es preciso que utilicen el mismo referencial de comunicaciones, es decir el mismo idioma, y que respeten reglas comunes de intercambio.

Análogamente, dos individuos de lengua materna distinta que deseen intercambiar información se pondrán de acuerdo sobre el idioma a utilizar. Tal vez uno de ellos intente hablar la lengua del otro o bien ambos utilicen una lengua conocida de ambos.

Si a esta conversación inicial se incorpora una tercera persona, después una cuarta y luego una quinta, etc., hablando diversos idiomas, el intercambio de datos resultará probablemente difícil de realizar si hay que traducir una lengua a otra para cada par de interlocutores. Resulta entonces preferible hablar una lengua común adoptada por todas las entidades comunicantes.

De manera semejante, los ordenadores en red deben respetar protocolos de comunicación idénticos y cumplir las mismas reglas de diálogo a fin de poder comunicarse. Estos protocolos se integran en los paquetes informáticos de comunicaciones y permiten entre otras cosas realizar el encaminamiento correcto de los datos y el interfuncionamiento de las aplicaciones y de los sistemas remotos.

Hay organismos reconocidos por toda la comunidad industrial que definen normas internacionales y normas de hecho. La ISO (*International Organization for Standardization*, Organización Internacional de Normalización) y la UIT (Unión Internacional de Telecomunicaciones) son organismos internacionales de normalización que proponen normas internacionales (por ejemplo, las normas de la serie X.400).

Una «norma de hecho» es aquella que no ha sido publicada por estos organismos aunque haya sido adoptada mayoritariamente por el mercado. Se trata pues de una norma de referencia, es decir de una norma de hecho. Así por ejemplo, todos los protocolos que provienen de la comunidad de Internet son normas de hecho.

---

[25] La información que sale de un ordenador para trasnmitirse por dicho soporte debe modularse. La información transportada de forma analógica debe demodularse a su recepción y presentarse en forma digital al ordenador de destino. Un mismo dispositivo, el módem, modula y demodula la información emitida y recibida por el ordenador.

Las normas definen, entre otras cosas, la naturaleza de los servicios a ofrecer por los protocolos de comunicación y especifican el modo de realizarlos. Esto permite concebir soluciones informáticas que se comuniquen entre sí. De este modo, gracias a la utilización de los mismos tipos de protocolos en máquinas diferentes (o heterogéneas), resulta posible la comunicación entre ellas. La universalidad de la red de Internet radica en la integración de los protocolos de la familia Internet en el conjunto de las máquinas conectadas.

III.1.4 Infraestructura de telecomunicaciones y autopistas de la información

Se denomina infraestructura de telecomunicaciones al conjunto de medios de transmisión a partir de los cuales pueden desarrollarse servicios de comunicaciones. Efectivamente, se disocian las vías y las técnicas de encaminamiento de las soluciones y servicios de telecomunicaciones ofrecidos a los clientes. Así por ejemplo, resulta posible explotar una infraestructura existente sin ser propietario de la misma y ofrecer, a partir de ésta, facilidades de transporte para aplicaciones particulares.

La disponibilidad de equipos multimedios, de infraestructuras de comunicación eficaces, así como la convergencia de los mundos audiovisual, informático y de las telecomunicaciones, contribuyen a realizar el concepto de cadena de información totalmente digitalizada. Esto representa la continuidad digital existente, tanto a nivel de la infraestructura de transporte como al del contenido, entre todas las fuentes de información y sus usuarios.

El concepto de autopista de la información integra la puesta a disposición del público en general, gracias a infraestructuras de comunicación eficaces, de un conjunto de servicios de interés general o de servicios comerciales que se supone contribuyen al bienestar de los individuos y pueden estar relacionados con la sanidad, la educación, la cultura, la ordenación del territorio, la administración o la prensa, entre otros. Debido a la naturaleza de ciertos servicios ofrecidos por Internet, este medio de comunicación puede considerarse una autopista de la información.

III.1.5 Internet

III.1.5.1 Características generales

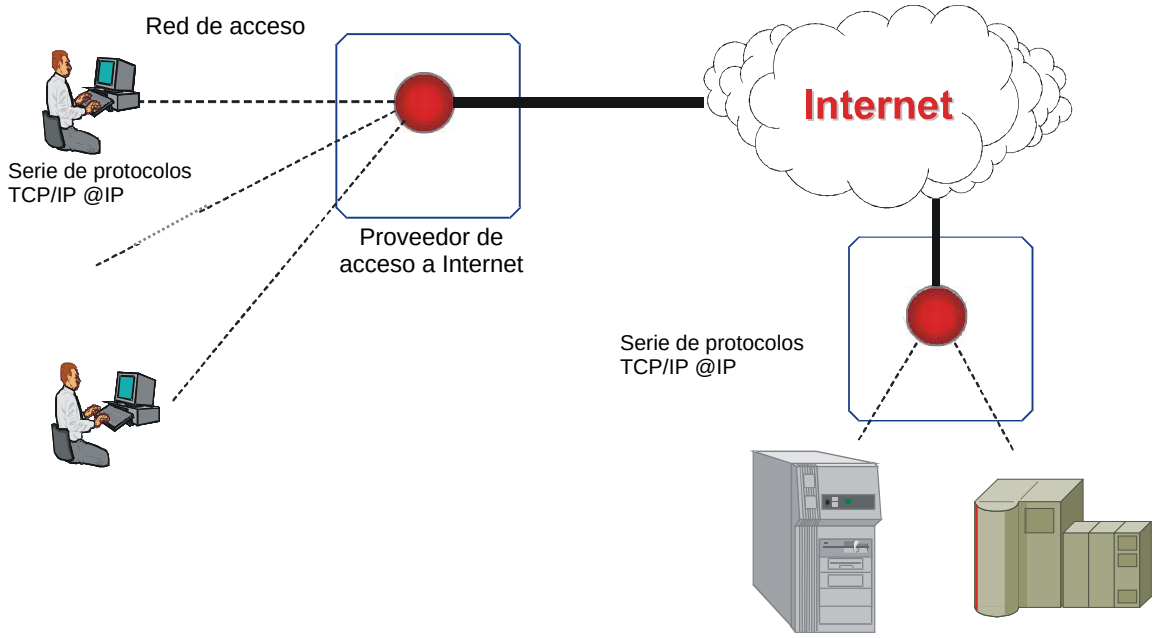
Internet se ha desplegado progresivamente desde Estados Unidos, conectando paulatinamente, sistemas informáticos así como redes de ordenadores. Este desarrollo reticular continúa y determina la estructura de la red que no es sino una red integrada a su vez por otras redes. El control mundial del conjunto de infraestructuras instaladas de este modo, extremo a extremo, resulta imposible en la medida en que son independientes y pertenecen a organismos distintos.

Desde el punto de vista material, Internet, como cualquier otra red de telecomunicaciones, está constituida por sistemas informáticos, elementos de conectividad y soportes de transmisión. Entre los sistemas informáticos cabe distinguir los que permiten acceder a la red y que permiten el diálogo con el usuario final (microordenador, teléfono móvil, buscapersonas, agenda electrónica, etc.), los que soportan las aplicaciones (servidor web, servidor de base de datos, etc.) y los dedicados a los procesamientos de la «red» (encaminadores, pasarelas de interconexión, etc.).

El intercambio de datos entre ordenadores se efectúa por los soportes de transmisión que los conectan físicamente. Cuando el acceso a la infraestructura de Internet se efectúa desde un sistema que permite la movilidad del usuario, tal como el teléfono móvil, se habla de la Internet móvil.

La transferencia de datos, su encaminamiento y la comunicación entre procesos informáticos distribuidos y usuarios humanos, se realizan mediante protocolos de comunicación de la familia TCP/IP[26]. Este software de intercambio, normalizado en el mundo de Internet, constituye una interfaz de comunicación que permite la interoperabilidad de sistemas de naturaleza diferente. Para comunicarse en el entorno de Internet un ordenador debe disponer de estos protocolos de comunicación así como de una dirección IP que lo identifique de manera única (Figura III.1).

Figura III.1 – Acceso a Internet a través de un proveedor de servicios, una serie de protocolos TCP/IP y una dirección IP

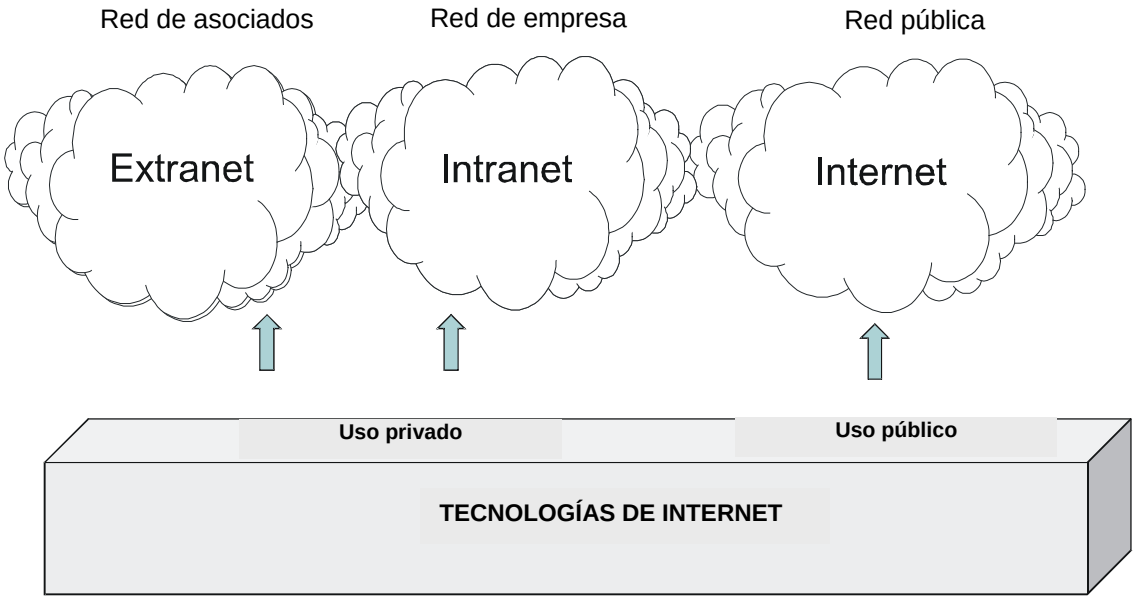


Se denomina Internet a la infraestructura de comunicación en su conjunto, puesta a disposición del público para comunicarse. Cuando una organización desea utilizar de manera privada y restrictiva esta infraestructura crea una red privada virtual (VPN, *Virtual Private Network*). Por necesidades de orden interno, puede asimismo implementar las tecnologías de Internet y construir una red privada o Intranet. Cuando la Intranet se abre además a un cierto número de asociados (clientes, proveedores, etc.), se denomina *Extranet* (Figura III.2).

La web (*World Wide Web*) es, junto con la mensajería electrónica, la aplicación más importante de Internet. A partir de la navegación web, se ha desarrollado una infinidad de servicios. La navegación web es posible gracias a un software cliente, el navegador o *browser*, implantado en la estación de trabajo del usuario que le permite acceder a distancia a los servidores web. Esto permite buscar información, consultarla, transmitirla e incluso ejecutar programas. El concepto de exploración o navegación por la red proviene del hecho de que los documentos accesibles a través de la aplicación web son hiperdocumentos. Esto significa que se han concebido, estructurado y formateado de manera que se permite la lectura no secuencial de los mismos en función de rótulos y enlaces determinados durante su concepción. Activando un enlace se accede a otra parte del documento o a otro documento, situado o no en un ordenador remoto. De este modo es posible desplazarse de sitio en sitio activando estos hiperenlaces.

26 TCP/IP: Transmission Control Protocol/Internet Protocol.

Figura III.2 – Internet – Intranet – Extranet



III.1.5.2 Direcciones IP y nombres de dominio

El acceso a Internet se realiza por medio de puntos de acceso gestionados y controlados por empresas especializadas que reciben el nombre de proveedores de acceso a Internet (ISP, *Internet Service Provider*). Cada proveedor de acceso está a su vez conectado a Internet mediante líneas de telecomunicación permanentes que comparte con sus diversos clientes. Más allá de este servicio básico suele ofrecer un servicio de gestión de mensajería electrónica y puede asimismo albergar sitios web de los clientes.

Para comunicarse por Internet hay que disponer de una dirección de Internet (dirección IP). Se trata de una serie binaria de 32 bits que identifica sin ambigüedad a cada máquina que se comunica por Internet[27].

Una dirección IP se representa, en formato decimal, mediante cuatro números decimales separados por puntos, por ejemplo, la dirección 128.10.2.30 corresponde al valor binario 10000000.00001010.00000010.00011110. Como es imposible recordar de memoria las series de números, incluso los decimales, se suelen utilizar nombres (más o menos mnemotécnicos) o direcciones lógicas, para identificar los recursos del entorno de Internet. Estas direcciones IP y los nombres correspondientes se almacenan y administran en directorios electrónicos denominados servidores de nombres, que en la práctica se conocen con las siglas DNS (*Domain Name Server*, servidor de nombres de dominio).

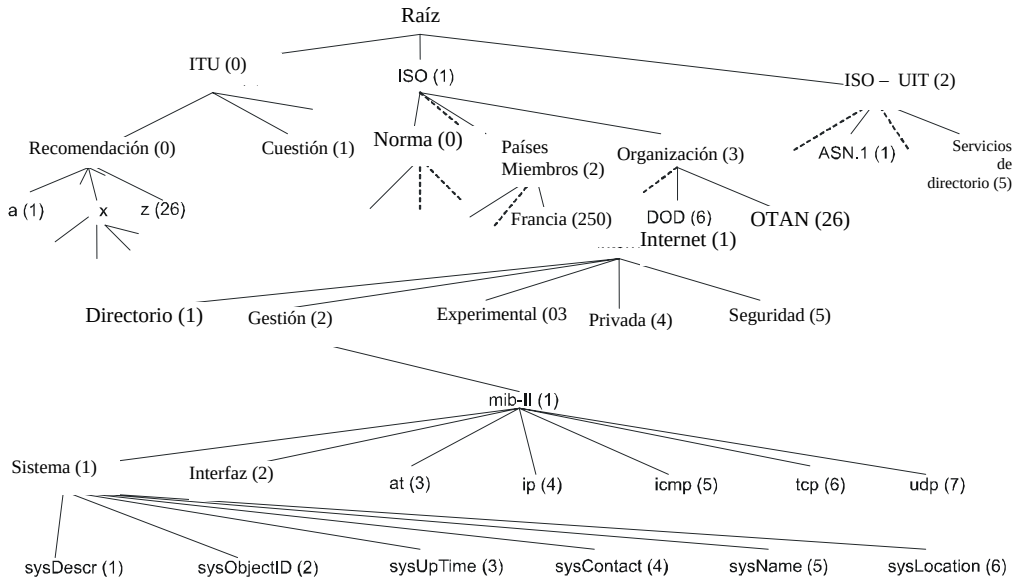
Para implementar las comunicaciones en entornos abiertos es necesario atribuir un identificador único a un dominio de denominación determinada. Se trata de poder identificar los integrantes de la comunicación (direcciones, sistemas, procesos de aplicación, entidades, objetos de gestión, etc.) así como las herramientas utilizadas para realizarlos (protocolos). Para garantizar la unicidad de los nombres a nivel internacional existen procedimientos de inscripción en las autoridades competentes que tienen por objeto la asignación de un identificador no ambiguo y único al objeto que se desea identificar.

[27] La dirección IP es única; puede asignarse de manera permanente (dirección IP fija) o no (dirección IP temporal).

En la norma ISO 9834 se indican las autoridades de registro, organizadas con arreglo a una estructura jerárquica arborescente. Desde la raíz del árbol arrancan tres ramas que terminan en nudos distintos del primer nivel que representa el dominio de denominación de la UIT, la ISO y de un Comité Mixto ISO-UIT que constituyen las autoridades internacionales de registro. El nivel inmediatamente inferior al de la ISO autoriza entre otros, el registro:

- de las diversas normas ISO (norma 0);
- de los miembros de la ISO (miembro-cuerpo 2) en el que se encuentran AFNOR (208) y ANSI (310);
- de organizaciones (organización (3)) de las que dependerá, por ejemplo, el Departamento de Defensa Norteamericano (DOD) (6) (Figura III.3).

Figura III.3 – Autoridades y árbol de registro



Los nombres de dominio de Internet genéricos se inscriben en esta estructura lógica de registro. Sólo resulta interesante la parte del árbol de registro cuyo nudo constituye la raíz de los nombres de dominio más elevados, denominados dominios de nivel superior (TLD, *top-level domains*), que identifican principalmente países indicados por dos letras (fr, it, uk, ch, nl, de, etc.) y dominios funcionales tales como:

- .com organizaciones comerciales;
- .edu instituciones académicas norteamericanas;
- .org organizaciones, ya sean institucionales o no;
- .gov gobierno norteamericano;
- .mil organizaciones militares norteamericanas;
- .net operadores de red;
- .int entidades internacionales;
- .biz negocios;
- .info cualquier uso;
- .name individuos;

- .museum establecimientos que recogen y clasifican colecciones de objetos para su conservación y presentación al público;
- .aero industria aérea y transporte;
- .coop cooperativas;
- .pro profesiones.

Dentro de estos grandes dominios de designación existen subdominios correspondientes a grandes empresas o a instituciones importantes.

La IANA (*Internet Assigned Number Authority*, Agencia de asignación de números de Internet)[28] con base en el ICANN (*Internet Corporation for Assigned Names and Numbers*, Cooporación de Internet para la asignación de nombres y números)[29] se encarga de la asignación de nombres y direcciones y debe garantizar su unicidad. La responsabilidad de gestión de los nombres puede delegarse en un subdominio que, desde el punto de vista jerárquico, cae bajo su autoridad.

La inscripción de un nombre de dominio consiste en insertar una entrada en un directorio de designaciones. Esto equivale a crear un nuevo arco en el árbol de registros gestionado por una organización habilitada. Existen varios de éstos a nivel internacional, principalmente en lo que se refiere a los dominios .biz, .com, .info, .name, .net y .org.

En Francia, por ejemplo, la AFNIC[30] es la autoridad de registro acreditada (*Accredited Registrar Directory*) por la ICANN (*Internet Corporation for Assigned Names and Numbers*).

La autoridad para la asignación y gestión de direcciones está encomendada a una asociación norteamericana, con sede en Estados Unidos, que se rige por el derecho norteamericano[31]. Controla por tanto el acceso a Internet. Esto plantea un problema de dependencia de las organizaciones y de los Estados de una superestructura extranjera que pretende estar abierta a todo el mundo pero en la que la representación no norteamericana es poco importante.

El criterio de seguridad relativo a la disponibilidad (de infraestructuras, servicios y datos) que pasa por la accesibilidad a Internet no debe estar controlado ni dominado por las organizaciones. Éstas son tributarias, para su acceso a Internet, de la asignación de direcciones IP y de nombres de dominio, por parte de entidades que les son ajenas.

Los directorios de registro de nombres de dominio pueden contemplarse como bases de datos gestionadas por servidores DNS. Hay aproximadamente 15 servidores raíz DNS (*root servers*) coordinados por el ICANN, la mayor parte de los cuales está en territorio norteamericano. Gestionan los nombres de dominio y las direcciones IP de más alto nivel (*top-levels domains*). Esto incluye todos los dominios anteriormente citados (.org, .com, etc.) así como los 244 nombres de dominio de los distintos países (.cn (China), .ga (Gabón), .lk (Sri Lanka), .pf (Polinesia Francesa), etc.). Hay servidores DNS locales llamados de resolución (*resolvers*) en los que se guarda una copia de las informaciones contenidas en lo servidores raíz. Suelen estar asociados a puntos estratégicos de acceso a la red o vinculados a proveedores de servicios de Internet (*Internet Service Providers* – ISP), permiten responder a las solicitudes de los usuarios sobre traducción de nombres de dominio a direcciones IP (Figura III.4)[32].

---

28 IANA: www.iana.org/

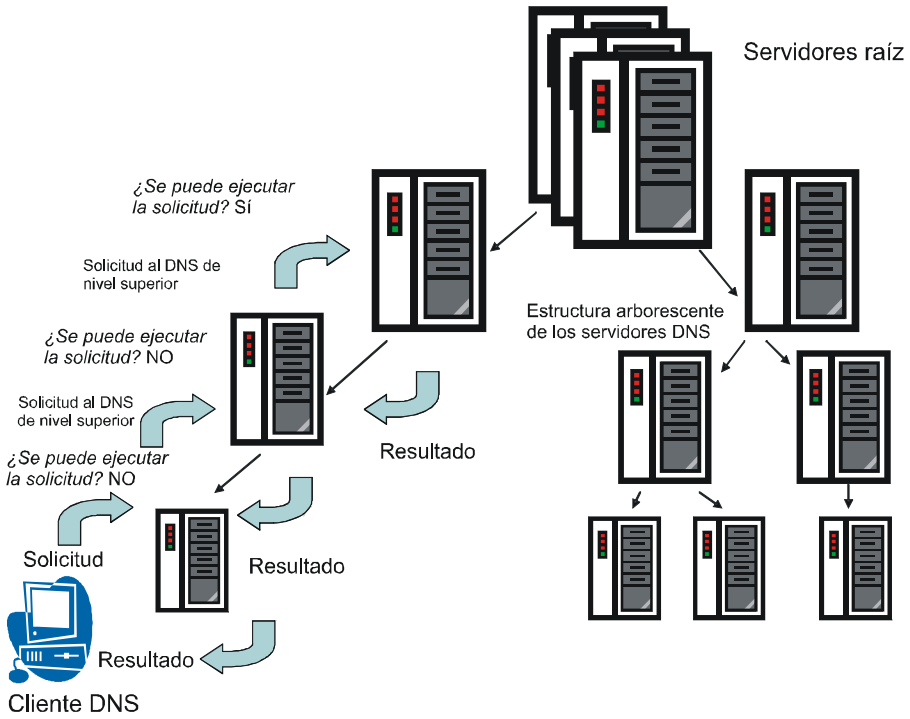
29 ICANN: www.icann.org/index.html

30 AFNIC: www.nic.fr

31 Según ICANN: «… *La corporación de Internet para la asignación de nombres y números (ICANN) es una entidad sin ánimo de lucro con carácter internacional que tiene la responsabilidad de la asignación del espacio de direcciones del protocolo Internet (IP), de la asignación de identificadores de protocolo, la gestión del sistema de nombres de dominio del nivel superior genérica (gTLD) y de códigos de país (ccTLD) y las funciones de gestión del sistema servidor raíz. Estos servicios los prestaba inicialmente la Autoridad de Asignación de Números de Internet (IANA, Internet Assigned Numbers Authority), entre otras entidades, en virtud de un contrato del Gobierno de EE.UU. En la actualidad ICANN realiza las funciones de IANA*».

32 Reproducción del libro «Sécurité informatique et télécoms: cours et exercices corrigés»; S. Ghernaouti-Hélie; Dunod 2006.

Figura III.4 – Estructura arborescente de los servidores DNS



Es muy importante que las direcciones, procesos y sistemas implicados en la gestión de nombres y direcciones y en el encaminamiento de datos estén disponibles y sean integrables, fiables y seguros. Corresponde a las entidades responsables de las infraestructuras de transporte, proteger y gestionar eficazmente sus entornos de comunicación.

III.1.5.3 El protocolo IPv4

La versión 4 del protocolo Internet (IPv4)[33], que existe desde los comienzos de Internet, sigue siendo muy utilizada. Este protocolo tiene por objeto la encapsulación (empaquetado) de los datos a transmitir en paquetes IP que se encaminan por Internet hasta su destino. Cada paquete contiene, entre otros, la dirección IP del sistema de origen o emisor y la dirección IP del sistema de destino.

El encaminamiento se realiza gradualmente a través de cada sistema intermedio (encaminador) que se atraviesa con arreglo a la interpretación de las direcciones de los paquetes y el algoritmo de encaminamiento de los encaminadores.

El protocolo IPv4 no integra ninguna función ni ningún mecanismo que permita ofrecer un servicio de seguridad. Efectivamente, el IPv4 no permite efectuar la autenticación del origen ni del destino de un paquete, ni verificar la confidencialidad de los datos que transporta, ni la de las direcciones IP implicadas en la transferencia de información entre dos entidades. Además, al ejecutarse el protocolo en el modo sin conexión, no se garantiza:

- la entrega de los datos (posible pérdida de datos);
- la entrega de los datos al destinatario correcto;
- el orden correcto (secuencia) de los datos.

33 IPv4: RFC 0791 – www.ietf.org/rfc/rfc0791.txt IPv4 y principales protocolos de la serie TCP/IP: TCP: RFC 0793 – www.ietf.org/rfc/rfc0793.txt – UDP: RFC 0768 – www.ietf.org/rfc/rfc0768.txt – FTP: RFC 0959 – www.ietf.org/rfc/rfc0959.txt – HTTP version 1.1: RFC 2616 – www.ietf.org/rfc/rfc2616.txt – Telnet: RFC 0854 – www.ietf.org/rfc/rfc0854.txt

El protocolo IP de nivel 3 de la arquitectura OSI ofrece un servicio no fiable de entrega de paquetes IP. Funciona en el modo sin garantías «*best effort*», es decir que se comporta del mejor modo posible dadas las circunstancias, por lo que la entrega de paquetes no está garantizada. De hecho, no hay ninguna calidad de servicio garantizada y por tanto no hay recuperación de errores. De este modo, los paquetes pueden perderse, modificarse, duplicarse, falsificarse o enviarse desordenadamente sin que el emisor ni el destinatario se enteren de ello. La ausencia de un enlace lógico previamente establecido entre emisor y destinatario significa que el primero envía sus paquetes sin advertir al destinatario de que pueden perderse, seguir caminos diferentes o llegar desordenadamente a su destino.

La consideración de esta falta de calidad de servicio ha desembocado en la implantación en los sistemas de extremo del protocolo TCP (protocolo de control de la transmisión) que ofrece un servicio de transporte fiable en modo conectado (nivel 4 de la arquitectura OSI). El protocolo TCP no ofrece servicio de seguridad propiamente dicho.

Capítulo III.2 – Herramientas de seguridad

La implantación de la seguridad de las informaciones, servicios, sistemas y redes consiste en implementar la disponibilidad, integridad, confidencialidad de los recursos así como el no rechazo de ciertas acciones, o la autenticidad de acontecimientos o de recursos.

La seguridad de las informaciones sólo tiene sentido cuando se aplica a datos y procesos de cuya exactitud no se tiene certeza absoluta (concepto de calidad de datos y de procesos) con objeto de que sean perdurables en el tiempo (concepto de perdurabilidad de los datos y de continuidad de los servicios).

Las principales soluciones de seguridad se basan en la implementación de técnicas de encriptación, aislamiento de entornos, redundancia de recursos, procedimientos de vigilancia, de control, de gestión de incidentes, de mantenimiento, de control de acceso y de gestión de sistemas.

La seguridad informática y de las telecomunicaciones se obtiene mediante una serie de barreras (las medidas de protección) que incrementan el nivel de dificultad que los atacantes potenciales deben superar para acceder a los recursos. No solucionan un problema de seguridad sino que lo trasladan y hacen recaer la responsabilidad de la seguridad en otras entidades. Las soluciones de seguridad han de ser protegidas y aseguradas para que puedan ofrecer un cierto nivel de seguridad (recursividad de la seguridad).

III.2.1 Encriptación de los datos

La aplicación de técnicas de encriptación permite implementar la confidencialidad de los datos, verificar su integridad y autentificar las entidades.

Existen dos grandes tipos de sistemas de encriptación de datos: la encriptación simétrica (con una clave secreta) y la asimétrica (con una clave pública).

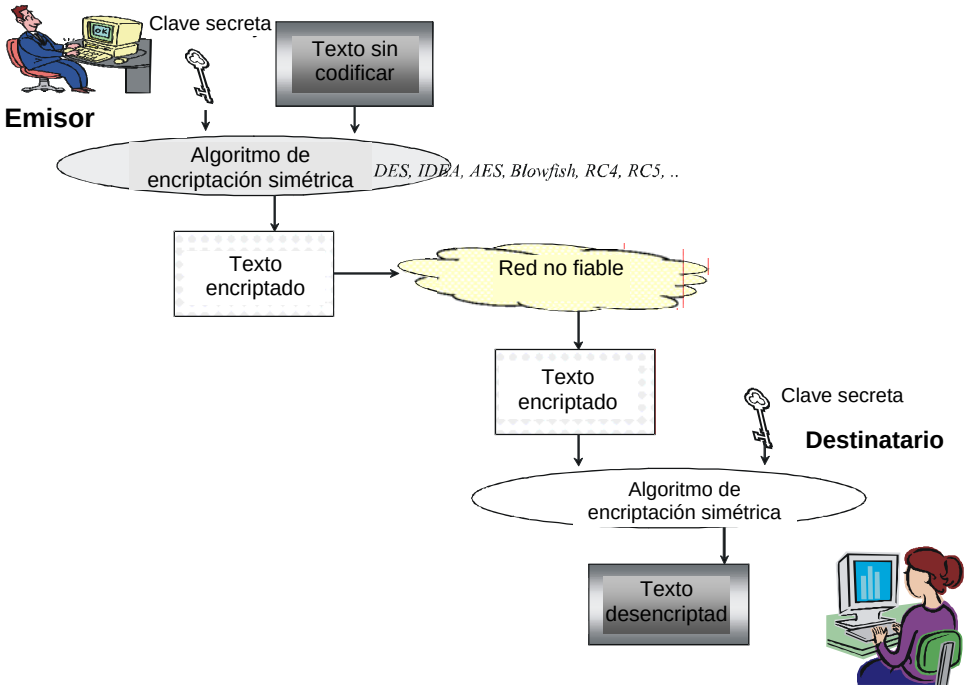
Hay diversos algoritmos de encriptación. Con independencia de su modo operativo (simétrico o asimétrico) se basan en la utilización de claves. Normalmente su grado de robustez depende de la capacidad de gestionar las claves de encriptación de manera segura, de la longitud de la clave (la longitud mínima de la clave es función del tipo de algoritmo) y de la seguridad de la plataforma material y lógica en la que los algoritmos de encriptación se implantan y ejecutan.

III.2.1.1 La encriptación simétrica

Para encriptar o desencriptar un texto, es necesario poseer una clave y un algoritmo de encriptación. Cuando la clave es la misma para ambas operaciones, el sistema de encriptación se denomina simétrico. El emisor y el receptor deben poseer y utilizar la misma clave secreta para que los datos sean confidenciales y poder descifrarlos, lo que plantea el problema de la gestión y difusión de las claves secretas (Figura III.5).

Los principales algoritmos de encriptación simétrica son los siguientes: DES, RC2, RC4, RC5, IDEA y AES[34].

Figura III.5 – La encriptación simétrica



III.2.1.2 La encriptación asimétrica o encriptación con clave pública

Un sistema de encriptación simétrica se basa en la utilización de un par único de claves, calculadas cada una de ellas en función de la otra. Esta doble clave está constituida por una clave pública y otra privada. Sólo la clave pública puede ser conocida por todos, mientras que la privada debe ser confidencial y considerada secreta.

El emisor encripta el mensaje con la clave pública del destinatario del mensaje y el destinatario lo desencripta con su clave privada (Figura III.6).

Los principales algoritmos de encriptación con clave pública llevan el nombre de sus inventores y suelen utilizar fundamentalmente claves de longitud variable de 512 a 1 024 bits, e incluso de hasta 2 048 bits. Los principales algoritmos de encriptación son los siguientes: RSA[35] (por R. Rivest, A. Shamir y L. Adelman), Diffie-Hellman[36] y El Gamal[37].

III.2.1.3 Las claves de encriptación

Las claves de encriptación son doblemente secretas. Las claves secretas de los sistemas de encriptación deben ser gestionadas confidencialmente.

---

34 Referencias:

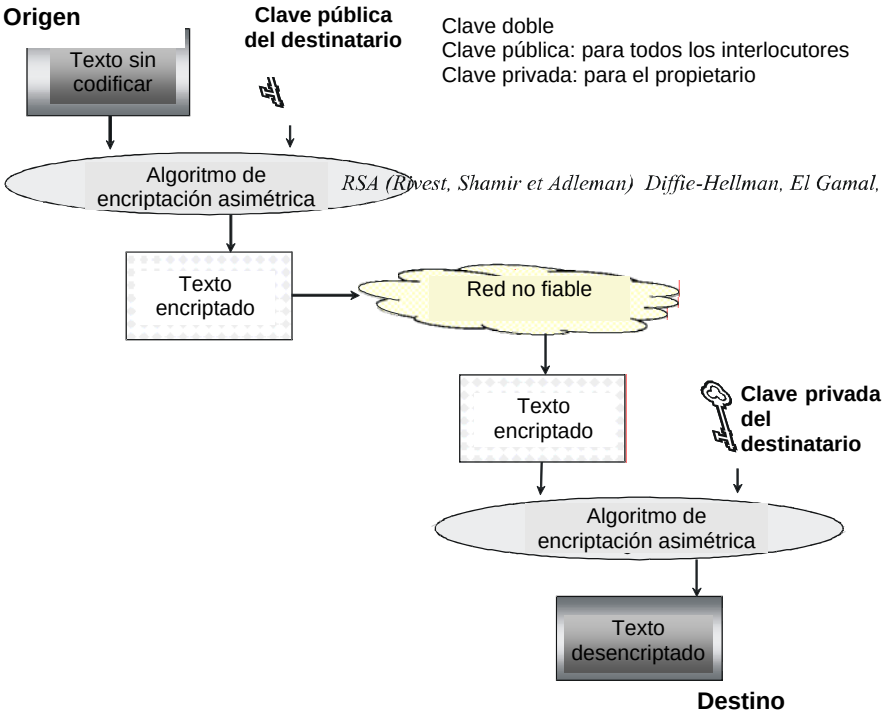
35 RSA: Schneier B, «Applied cryptography» 1996. Segunda Edición 1996.

36 Diffie-Hellman: www.ietf.org/rfc/rfc2631.txt

37 El Gamal: Schneier B, «Applied cryptography» 1996. Segunda Edición 1996.

La seguridad de los procesos de encriptación se basa en gran medida en la confidencialidad y en la longitud de las claves utilizadas, en la robustez de los algoritmos y en la seguridad de las plataformas físicas y lógicas que las soportan.

Figura III.6 – La encriptación asimétrica



III.2.1.4 La infraestructura de gestión de claves

La infraestructura de gestión de claves – IGC (PKI – *Public Key Infrastructure*) permite utilizar sistemas de encriptación asimétrica. Las principales funciones soportadas son las siguientes:

- generación de un par único de claves (clave privada – clave pública), atribución a una entidad y salvaguarda de la información necesaria para su gestión, archivo, procedimientos de recuperación en caso de pérdida por el usuario y solicitud de entrega a las autoridades judiciales;
- gestión de certificados digitales, creación, firma, emisión, validación, revocación y renovación de los certificados;
- difusión de las claves públicas a las entidades solicitantes habilitadas para su obtención;
- certificación de las claves públicas (firma de certificados digitales).

III.2.1.5 El certificado digital

Un certificado digital constituye el carné de identidad digital de una entidad (persona física o jurídica) o de un recurso informático al que pertenezca. Contiene, entre otros, la identificación de su propietario, la clave pública asignada al mismo así como la identificación del organismo emisor.

La norma X.509 «*Directory authentification framework*» «El Directorio: marco para los certificados de claves públicas y de atributos» propone un marco de arquitectura para la implementación de un servicio de autenticación basado en la utilización de certificados digitales y especifica la estructura y formato de los certificados digitales. Sobre esta estructura normalizada se basan muchas de las soluciones comercializadas (Figura III.7).

Figura III.7 – Principales parámetros de un certificado digital según la norma X.509v3

Versión del certificado
Número de serie
Algoritmo utilizado para firmar el certificado
Nombre del organismo que genera el certificado El par número de serie/nombre del organismo debe ser único
Periodo de validez
Nombre del propietario del certificado
Clave pública del propietario
Informaciones adicionales relativas al propietario o a los mecanismos de encriptación
Firma del certificado Algoritmo y parámetros utilizados para la firma y firma propiamente dicha

Para validar el certificado recibido, el cliente debe obtener la clave pública del organismo que ha creado el certificado relativo al algoritmo utilizado para firmar el certificado y descifrar la firma contenida. Con la ayuda de estas informaciones calcula el valor del resumen (*hash*) y compara el valor resultante con el contenido en el último campo del certificado, si ambos valores concuerdan, el certificado queda autenticado. A continuación se cerciora de que el periodo de validez del certificado es correcto.

El control de acceso basado en certificados digitales permite la conexión de un número importante de usuarios a un servidor determinado. El control se basa en las informaciones contenidas en el certificado digital del cliente. El servidor confía entonces en la veracidad de los certificados y en su modo de emisión, lo que constituye una brecha de seguridad de los sistemas, puesto que es posible corromper un servidor de certificación e incluso falsificar un certificado digital. Por otra parte, el control de validez de un certificado resulta difícil de ejecutar. Efectivamente, la revocación de los certificados es una tarea bastante ardua puesto que la información debe transmitirse a todas las partes e inscribirse en el CRL (*Certificate Revocation List*, lista de revocación del certificado). Esta revocación debe realizarse cuando se produzca cualquier cambio en el contenido de un certificado (por ejemplo cuando la información del certificado quede obsoleta, la clave privada del usuario haya sido corrompida, el usuario ya no pertenezca a la empresa, etc.). La consulta sistemática de esta base de datos sobrecarga aún más el control de acceso y reduce la disponibilidad de los servidores incluso para los usuarios autorizados.

III.2.1.6 Tercero de confianza

Con independencia de su denominación, tercero de confianza, autoridad de registro o autoridad de certificación, el organismo que crea una infraestructura con clave pública tiene como misión principal la producción de certificados que establezcan el valor de las claves públicas asignadas a las entidades (concepto de certificado cliente).

El cliente, emite una solicitud de registro (solicitud de certificación) ante una autoridad de certificación (inscripción del cliente a través de un servicio web). El servidor de registro puede solicitar pruebas de la identidad del cliente con arreglo a los procedimientos de identificación y autenticación empleados por la autoridad. Tras la validación de los datos, el servidor de certificación genera las claves de encriptación y construye un certificado digital a nombre del cliente, firma con su clave privada el certificado (certificación del certificado digital) y envía el certificado al cliente. Este último utilizará la clave pública de la autoridad para garantizar que el certificado ha sido emitido efectivamente por la autoridad en cuestión.

La autoridad de certificación es un tercero de confianza que entrega certificados digitales y permite verificar la veracidad de determinadas informaciones.

III.2.1.7 Inconvenientes y límites de las infraestructuras de gestión de claves

La multiplicidad de autoridades de certificación plantea el problema de su reconocimiento recíproco, su interoperabilidad, la compatibilidad de los certificados y su ámbito de validez. Sin embargo, no conviene disponer de una única autoridad mundial de certificación por el amplio y excesivo poder que se le conferiría de hecho y por la importancia de la infraestructura a crear. Hay realmente una falta de confianza de los usuarios en las autoridades de certificación, sobre todo si son extranjeras (¿Valor de los certificados? ¿Garantía de seguridad? ¿Protección de datos personales?, etc.).

Las limitaciones intrínsecas de las infraestructuras de gestión de las claves residen en:

- la complejidad y el coste de desarrollo y gestión de la infraestructura;
- el alto nivel de seguridad necesario para la implementación de los servicios de infraestructura de gestión de claves;
- la validez, vida útil, y restricción de los certificados.

Entre las cuestiones relativas a la implementación de los servicios ofrecidos por la infraestructura de gestión de claves que pueden plantear problemas, cabe citar las siguientes:

- Problemas políticos: la mayor parte de las infraestructuras PKI – Autoridades de certificación, pertenecen a entidades norteamericanas (EE.UU.). Esto plantea la cuestión del rendimiento y la de la confianza en estas entidades debido a los servicios ofrecidos: creación de claves privadas y públicas y salvaguarda y distribución de las mismas, datos de identificación, notarización de los acontecimientos; así como por la falta de garantía de uso no abusivo de datos, y los medios de recurso en caso de litigio con la autoridad de certificación.
- Problemas tecnológicos: Los sistemas de encriptación tradicionales pueden violarse, hay certificados digitales que no tienen ningún valor de seguridad y no garantizan nada, se pueden cometer fraudes, la seguridad de las infraestructuras está garantizada por medios de seguridad tradicionales que pueden burlarse. Además, el empleo de una infraestructura de gestión de claves traslada el problema de la seguridad de los intercambios pero no lo resuelve en sentido estricto.
- Problemas organizativos: Interoperabilidad de las infraestructuras, despliegue, gestión, mantenimiento, seguridad, complejidad, etc.

III.2.1.8 Firma y autenticación

El emisor encripta los mensajes con su clave privada. Cualquier entidad que conozca la clave pública de este emisor descifrará sus mensajes, lo que validará su correcta creación, con la clave privada correspondiente.

Los documentos pueden firmarse electrónicamente (concepto de firma digital) mediante un algoritmo de encriptación con clave pública. Se ejecutan en este caso las acciones siguientes:

- creación de un mensaje de declaración de identidad consistente en la firma (por ejemplo «Me llamo Alpha Tango Charlie») que se encripta con la clave privada del emisor y se asocia al mensaje a transmitir;
- el mensaje y la firma se encriptan con la clave pública del destinatario y se transmiten;
- el destinatario desencripta el mensaje con su clave privada y separa la firma para descifrarla con la clave pública del emisor.

Es importante destacar que nada impide volver a utilizar la firma digital de un mensaje haciéndose pasar por el emisor real, y que se puede crear asimismo una firma digital haciéndose pasar por un tercero tras haberle robado su clave privada… Para aumentar el grado de seguridad de la firma digital ésta debe construirse a partir del contenido del mensaje, lo que permite determinar su integridad y realizar la autenticación del emisor del mensaje.

III.2.1.9 Integridad de los datos

Se puede verificar que los datos no han sido modificados durante la transmisión asociándoles un resumen (compendio) que se emite simultáneamente con los mismos. Éste se obtiene de aplicar a los datos una función de cálculo. El destinatario vuelve a calcular con la misma función el valor del resumen a partir de los datos recibidos. Si el valor obtenido es diferente, puede inferir que los datos se han modificado. El resumen puede venir a su vez encriptado antes de que los datos se emitan o se guarden.

Tanto los sistemas de encriptación con clave simétrica como los de clave asimétrica permiten averiguar si los datos transmitidos se han modificado, porque en tal caso su desencriptación resulta imposible. Esto contribuye a implementar un control de integridad aunque sin asegurar que los datos no hayan sido destruidos por completo.

Para mejorar la eficacia del control de integridad se aplica al mensaje original una función que lo transforma en una breve serie aleatoria de bits que constituye en alguna medida su huella digital (*compendio – resumen – extracto*).

La función denominada *compendio* (o *función de troceado unidireccional*), genera un mensaje *compendio*, es decir su huella digital que es más corta que el mensaje original e ininteligible. Éste se encripta a continuación con la clave privada del emisor y se asocia al mensaje a transmitir. Al recibir el mensaje y su huella, el destinatario desencripta esta última con la clave pública del emisor y a continuación recalcula la huella con la misma función de *troceo* a partir del mensaje recibido, y la compara con la recibida. Si el resultado obtenido es idéntico, el destinatario da por verificada la identidad del emisor y se cerciora de la integridad del mensaje. Efectivamente, si el mensaje ha sufrido modificaciones, incluso pequeñas, su huella se habrá modificado considerablemente.

Para garantizar la integridad de los datos se pueden marcar los mensajes utilizando conjuntamente las técnicas de encriptación, firma y huella digital. Estos procedimientos consumen tiempo de procesador y ralentizan significativamente el rendimiento del entorno de ejecución.

III.2.1.10 No rechazo

El servicio de no rechazo consiste en prevenir el rechazo o la negación de que un mensaje haya sido emitido o recibido o de que una acción o transacción haya tenido lugar. Esto permite demostrar, por ejemplo, que cierta entidad está vinculada a una acción o evento.

El no rechazo se fundamenta en una firma única o en una identificación que demuestra la autoría del mensaje. Para realizar este servicio se puede recurrir a un algoritmo de encriptación con clave pública. Se puede igualmente acudir a un tercero de confianza para que asuma las funciones de cibernotario.

III.2.1.11 Limitaciones de las soluciones de seguridad basadas en la encriptación

La confianza en las soluciones de encriptación comercializadas sólo puede ser relativa, en la medida en que no se ofrecen garantías ni medios de verificación (¿Existen puertas falsas (*back door*) en los programas informáticos? ¿Existen claves duplicadas o divulgadas?, etc.). Por otra parte, no hay pruebas de que los algoritmos que actualmente se consideran fiables lo sigan siendo en un futuro próximo.

III.2.2 El protocolo IP seguro

La consideración de las necesidades de seguridad ha llevado a la revisión de la versión 4 del protocolo Internet. Asimismo, la necesidad de poder disponer de una gama de direcciones más amplia y de incrementar el número de direcciones de Internet disponibles, por una parte, y, por otra, de poder asignar dinámicamente el ancho de banda para soportar aplicaciones multimedias, ha dado lugar a que el protocolo IP haya sido objeto de una revisión a cuyo resultado se le ha dado el nombre de IPnG (*Internet Protocol next Generation*, protocolo Internet de la próxima generación) o IP versión 6 (IPv6)[38].

III.2.2.1 El protocolo IPv6

En 1994[39] el IAB (*Internet Activities Board*)[40] estudió las necesidades de seguridad del protocolo IP. La versión 6 del protocole IP (IPv6) cuenta con facilidades de autenticación y confidencialidad.

Las principales novedades del IPv6 respecto al IPv4 se encuentran en los aspectos siguientes [RFC 2460]:

- soporte de una dirección ampliada y jerarquizada; las direcciones se codifican con 128 bits (16 octetos) y no con 32 bits (4 octetos), como ocurría anteriormente; las direcciones se representan por números hexadecimales[41] separados por dos puntos cada 2 octetos y no mediante la notación decimal separada por puntos utilizada anteriormente; (por ejemplo: 0123:4567:89ab:cdef:0123:4567:89ab:cdef);
- la posibilidad de poder asignar dinámicamente la anchura de banda para permitir aplicaciones multimedios;
- la capacidad de crear redes IP virtuales;
- el soporte de procedimientos de autenticación y de encriptación mediante encabezamientos de opciones;
- la simplificación del encabezamiento de los paquetes con objeto de facilitar y acelerar su encaminamiento.

La adopción del IPv6 impone, entre otras, la modificación del esquema de direccionamiento, de la gestión de las direcciones[42], la instalación en todo el entorno de Internet de sistemas que soporten IPv6 y de sistemas que funcionen con las dos versiones, la sincronización a gran escala de la migración de las versiones, etc.

Por todos estos motivos, la versión 6, especificada en 1995, sigue teniendo escasa implantación y no parece haber ninguna acción por parte de los gobiernos ni ninguna recomendación internacional que pueda imponer la adopción de la versión 6 del protocolo en toda la red. Sólo algunas infraestructuras privadas integran IPv6.

Tampoco es habitual la implementación del nuevo protocolo Internet (IPv6), que integra de modo nativo funciones de seguridad, para hacer frente a las necesidades de seguridad de la red. Se ha creado una solución intermedia denominada IPSec[43], compatible con IPv6 e IPv4, que ha sido adoptada por la comunidad de Internet. El IETF (*Internet Engineering Task Force*, Grupo Especial sobre Ingeniería de Internet)[44] publicó en 1995 varios documentos (RFC 1825 a 1829) especificando los modos de asegurar una infraestructura de Internet.

---

38 IPv6: RFC 1883 de 1995, se sustituyó en diciembre de 1998 por RFC 2460 – www.ietf.org/rfc/rfc2460.txt

39 RFC 1636: Report of IAB Workshop on Security in the Internet Architecture. 8-10 de febrero de 1994.

40 www.iab.org/

41 Alfabeto del sistema de numeración hexadecimal (base 16): 0 1 2 3 4 5 6 7 8 9 A B C D E F.

42 RFC 1886 definió en 1995 las modificaciones a efectuar en las DNS para soportar IPv6.

43 RFC 2401 – www.ietf.org/rfc/rfc2401.txt

44 IETF: www.ietf.org

III.2.2.2 El protocolo IPSec

IPSec permite dotar de confidencialidad el contenido de los paquetes transportados por este protocolo. IPSec ofrece servicios de confidencialidad y de autenticación de los datos a nivel de su transferencia mediante el protocolo IP, gracias a la implementación del encabezamiento de extensión de la autenticación (*Authentication Header* [AH], encabezamiento de autenticación) o del encabezamiento de confidencialidad – autenticación (*Encapsulating Security Payload Header* [ESP], encabezamiento de encapsulamiento de la parte útil de seguridad).

Cualquier aplicación, con independencia de la naturaleza del tráfico que genera, puede utilizar estos servicios de seguridad sin necesidad de modificación. IPSec funciona en modo punto a punto (se aseguran los datos entre el emisor y el receptor mediante una asociación de seguridad).

El encabezamiento de autenticación (AH) ofrece servicios de autenticación y de integridad de los paquetes IP, lo que permite garantizar la imposibilidad de modificación de los datos transmitidos y la autenticidad de la dirección de origen que figura en el paquete.

El encabezamiento de *encapsulación de la parte útil de seguridad* (ESP, *Encapsulating Security Payload*) permite la implementación de mecanismos de encriptación (encriptación simétrica tal como DES, Triple DES, RC5 e IDEA) y ofrece servicios de autenticación semejantes a los propuestos por el encabezamiento de autenticación (AH, *Authentication Header*).

Los algoritmos de encriptación utilizan claves que deben generarse y difundirse. La gestión de las claves de encriptación constituye pues una tarea importante que debe realizarse durante la implementación de las soluciones basadas en IPSec. Entre los protocolos de intercambio de claves cabe citar: *Oakley Key Determination Protocol*[45] que se basa en el algoritmo de intercambio de claves Diffie-Hellman [RFC 2412]; ISAKMP (*Internet Security Association and Key Management Protocol*, Asociación de seguridad de Internet y protocolo de gestión de claves) [RFC 2408] e IKE (*Internet Key Exchange*, intercambio de claves de Internet) [RFC 2409].

III.2.2.3 Redes privadas virtuales

La implantación del protocolo IPSec a nivel de puntos de acceso de Internet permite crear entre dichos puntos un canal de comunicación cuyos extremos se someten a autenticación (Figura III.8).

Estos extremos se encuentran en sistemas de la organización y por tanto están protegidos físicamente. En función de la opción adoptada, los datos transportados sobre esta conexión pueden encriptarse. De este modo se puede establecer un camino seguro entre dos puntos de una infraestructura de red no fiable (concepto de red privada virtual). Obsérvese que la palabra «red» en la expresión «red privada virtual» es una hipérbole puesto que sólo se crea una conexión lógica (virtual).

III.2.3 La seguridad en las aplicaciones

La mayor parte de las aplicaciones tienen una versión segura que suele permitir realizar la autenticación de los corresponsales y la encriptación de los datos transmitidos.

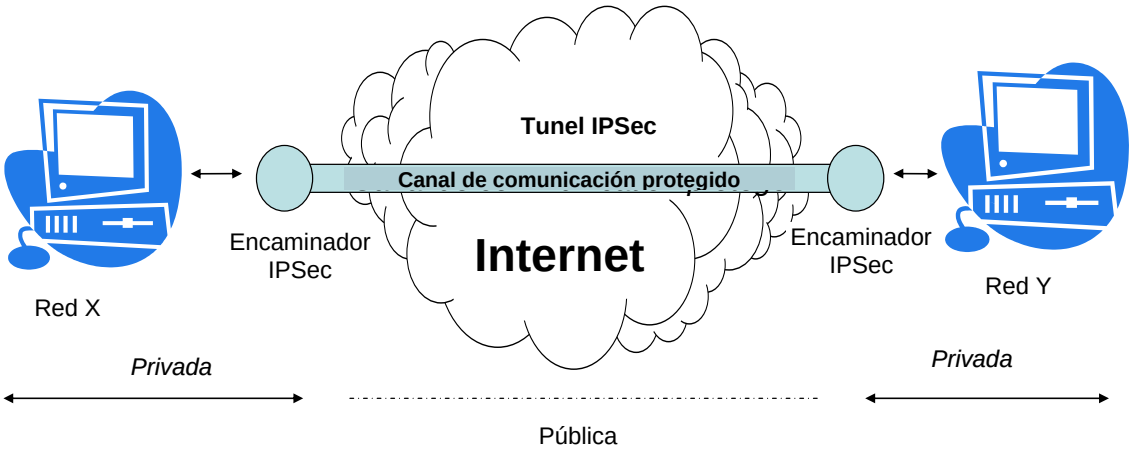
Una alternativa a la implantación de las nuevas versiones seguras de los protocolos de aplicación consiste en implantar un mecanismo común de seguridad que ofrezca servicios genéricos de seguridad a todas las aplicaciones. El software SSL (*Secure Sockets Layer*, capa de zócalos segura) es el que se suele utilizar en la actualidad, principalmente para realizar transacciones comerciales por Internet.

El uso generalizado de documentos de hipertexto y la descarga de contenidos, activos o no, plantean numerosos problemas de seguridad principalmente en relación con: su origen, su autor, su autenticidad, su carácter dañino o inocuo, etc. Comienzan a surgir elementos de respuesta a esta nueva dimensión de la seguridad de los sistemas de información: las técnicas de firma de documentos XML, de filigrana y de gestión de derechos electrónicos, con el fin de dotar a la seguridad de una cierta persistencia. Un determinado nivel de seguridad debe poder conservarse, incluso si el objeto afectado por dicha seguridad traspasa las fronteras físicas del entorno en el que se gestiona habitualmente su seguridad.

---

[45] Oakley Key determination protocol: RFC 2412 – www.ietf.org/rfc/rfc2412.txt

Figura III.8 – Constitución de una red privada virtual mediante un canal de comunicación IPsec



III.2.4 El protocolo de seguridad SSL (Secure Sockets Layer) y el S-HTT (HTTP seguro)

El SSL (*Secure Sockets Layer*, capa de zócalos segura) es un software que garantiza la seguridad de los intercambios informáticos, y que además está soportado por la mayor parte de los navegadores web existentes en el mercado.

Las dos entidades comunicantes de una conexión SSL se autentican y recurren a un procedimiento de certificación y a un tercero de confianza. A continuación negocian el nivel de seguridad que debe aplicarse a la transferencia. Acto seguido los datos a transmitir se encriptan para la comunicación SSL (Figura III.8).

La implantación del protocolo SSL repercute considerablemente en el servidor por ser imprescindible la certificación. Esto implica un diálogo con una autoridad de certificación reconocida y exige asimismo que los programas informáticos que efectúan la retransmisión en los cortafuegos soporten el modo de funcionamiento SSL. La certificación se considera a veces como un freno al desarrollo de esta solución.

La extensión al protocolo HTTP *seguro* (S-HTTP) es una solución alternativa desarrollada por la asociación CommerceNet. S-HTTP ofrece las mismas facilidades de seguridad que SSL, con las mismas restricciones de certificación, aunque no soporta el flujo de datos del protocolo HTTP. Esta solución tiene escasa implantación.

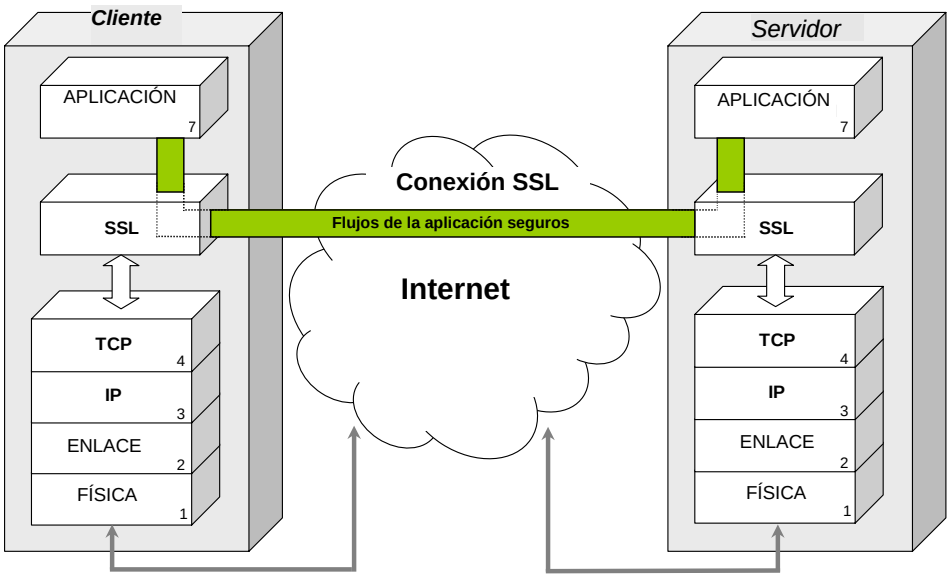
III.2.5 La seguridad de la mensajería electrónica y de los servidores de nombres

Los riesgos de seguridad afrontados, en relación con el uso de un sistema de mensajería, se relacionan con:

- la pérdida, interceptación, alteración o destrucción de los mensajes;
- la infección de sistemas mediante mensajes con virus, gusanos o troyanos;
- el acoso: inundación de mensajes, correo indeseado, mensajes no solicitados dirigidos a personas cuya dirección de correo electrónico se utiliza sin su consentimiento y con las que el remitente (del correo indeseado) nunca ha tenido relación alguna. El correo indeseado por envío masivo de mensajes infectados puede contribuir a la propagación rápida de los virus (correo indeseado + virus), ya que se introducen motores de mensajería en el código de los virus para que puedan difundirse autónomamente;

– la usurpación de identidad de los usuarios (un intruso se hace pasar por otro, un elemento del sistema emite, escucha o intercepta mensajes no destinados al mismo, etc.;
– los mensajes pueden introducirse, reproducirse, mezclarse, suprimirse y retrasarse;
– una denegación de servicio por la caída de un elemento de la cadena del sistema de mensajería;
– la divulgación de informaciones confidenciales;
– el rechazo (un elemento del sistema niega haber enviado o recibido un mensaje).

Figura III.8 – Arquitectura SSL (*secure socket layer*, capa de zócalo segura)



A éstos se asocian igualmente todas las amenazas propias de las redes y de sus modos de funcionamiento (ataques a nivel de encaminamiento, de servidor de nombres, etc.).

Para reducir en lo posible estas limitaciones de seguridad inherentes al modo de funcionamiento de la mensajería, las nuevas versiones de estos programas informáticos cuenta con facilidades de encriptación que garantizan la confidencialidad, integridad y autenticidad de las informaciones intercambiadas y de los corresponsales.

Los imperativos de seguridad de los sistemas de mensajería se expresan en términos de:

– confidencialidad e integridad (de un mensaje o secuencia de mensajes);
– no rechazo (prueba de la emisión, prueba de la recepción, firma, certificación de los mensajes);
– autenticación de la identidad de todos los elementos del sistema de mensajería (usuarios, elementos intermediarios, memoria de mensajes, agentes de transferencia de mensajes, etc.).

El riesgo más importante es sin duda el vinculado a la introducción de virus, gusanos o troyanos mediante mensajes. Un método de prevención consiste en instalar un antivirus en cada sistema para detectar la presencia de virus y desinfectarlos en la medida de lo posible. Un antivirus no detecta más que los virus para los que se ha diseñado y no protege contra nuevas formas de infección; además, su actualización es necesaria y exige un esfuerzo de gestión nada despreciable.

Una medida complementaria consiste en instalar un servidor de mensajería en cuarentena que examina sistemáticamente todos los mensajes y sus adjuntos. Se pueden ejecutar varios antivirus simultáneamente y de este modo incrementar la probabilidad de detección de los mensajes infectados.

El protocolo inicial de mensajería SMTP (*Simple Mail Transfer Protocol*, protocolo sencillo de transferencia de correo) del entorno Internet se ha mejorado a lo largo del tiempo para soportar, por una parte, contenidos de mensajes multimedios y, por otra, para integrar mecanismos de seguridad. En la actualidad hay varios disponibles. Entre ellos cabe citar: el *Secure Multipurpose Internet Mail Extensions* (extensiones de correo Internet polivalente seguro) o *Secure MIME* (S/MIME), el *Privacy Enhanced Mail* (PEM, correo de privacidad mejorada) y el *Pretty Good Privacy* (PGP, privacidad bastante buena).

Todas las aplicaciones del mundo Internet recurren directa o indirectamente a los servicios ofrecidos por los servidores DNS (*Domain Name Server*, servidor de nombres de dominio) (que gestionan la relación entre los nombres lógicos y las direcciones IP correspondientes). Los DNS contribuyen activamente al encaminamiento correcto de la información. De este modo, constituyen puntos sensibles de la arquitectura de comunicación y son por lo tanto servidores que han de protegerse. La creación de mecanismos de seguridad (control de acceso, de autenticación, de rastreo, de duplicidad, de coherencia, la encriptación de las solicitudes y de sus respuestas, etc.) permiten evitar que personas malintencionadas modifiquen el valor de las informaciones guardadas para encaminarlas hacia destinatarios distintos de los previstos inicialmente (desvío), los inunden con peticiones inútiles que pueden provocar desde denegación de servicio hasta indisponibilidad de recursos y caída de la red, y creen falsos servidores de nombres con objeto de obtener respuestas erróneas que provoquen errores de transmisión o intrusiones.

III.2.6 La detección de intrusiones

Las intrusiones, incidentes y anomalías deben detectarse e identificarse lo antes posible y gestionarse con rigor a fin de garantizar el funcionamiento normal de los sistemas y su protección.

Un incidente es un acontecimiento que surge inopinadamente. Aunque no suele reviste gravedad, puede tener consecuencias graves. Una anomalía es una excepción que puede inducir el funcionamiento anormal del sistema de información lo que puede desembocar en una violación de la política de seguridad vigente. Puede tener un origen accidental (por ejemplo, un error de configuración) o provocado (un ataque dirigido al sistema de información). La intrusión es característica de un ataque y puede considerarse como incidente o anomalía.

La detección de las intrusiones se puede definir como el conjunto de prácticas y mecanismos utilizados con objeto de detectar errores que puedan dar lugar a violaciones de la política de seguridad, y de diagnosticar las intrusiones y ataques (incluidos la detección de las anomalías y el uso abusivo de los recursos)[46].

Los sistemas de detección de intrusiones (IDS – *Intrusions Detection System*) constan de tres bloques funcionales esenciales: el de la recogida de información, el del análisis de la información recuperada y el de la detección de las intrusiones y respuesta a las intrusiones detectadas.

III.2.7 Segmentación de los entornos

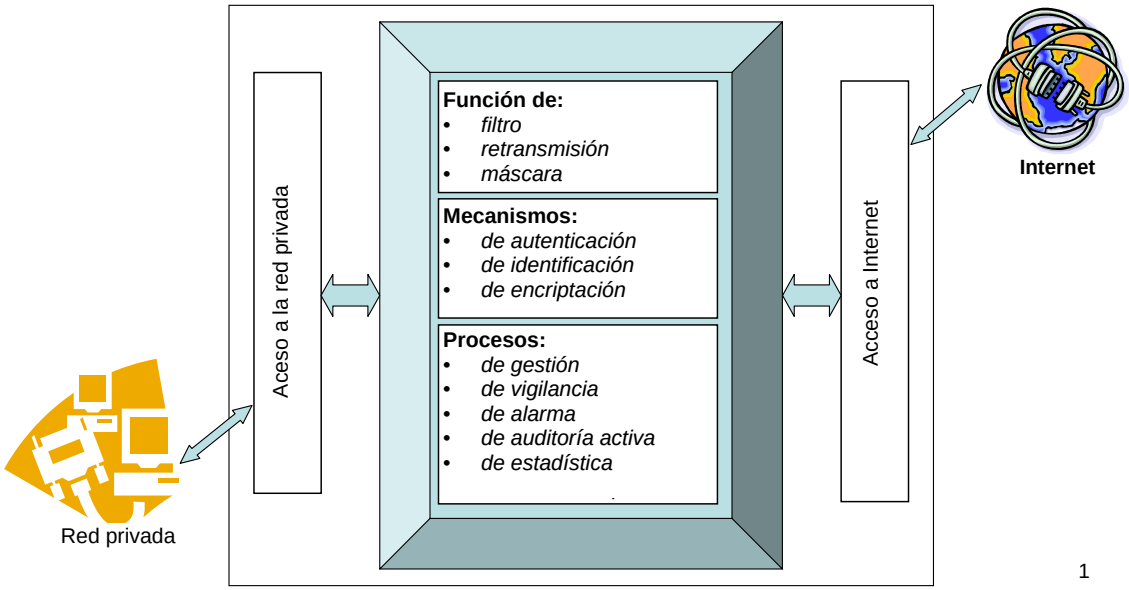
La separación y el enmascaramiento de un entorno privado frente a la Internet pública se basa en la instalación de uno o varios sistemas *cortafuegos* (*firewalls*).

---

[46] Alessandri, D. et Al. «Towards a taxonomy of intrusion detection systems and attacks» www.domino.watson.ibm.com/library/cyberdig.nsf/papers/5FA980EB952E09D085256AC600535997/$File/rz3366.pdf

Un *cortafuegos* es un sistema que permite bloquear y filtrar los flujos que recibe, analizarlos y autorizarlos si reúnen determinadas condiciones, y rechazarlos en el caso contrario. La segmentación de una red permite constituir entornos IP disjuntos, independizando físicamente los accesos de las redes que se desea separar. Esto permite interconectar dos redes de niveles de seguridad diferentes (Figura III.9)[47].

Figura III.9 – Estructura funcional de un *cortafuegos*



Dependiendo de la naturaleza del análisis y de los tratamientos efectuados por el cortafuegos, se pueden considerar distintos tipos de *cortafuegos*. Se suelen diferenciar por el nivel de filtrado de datos en el que funcionan: nivel 3 (IP), nivel 4 (TCP, UDP) y nivel 7 (FTP, HTTP, etc.) del modelo OSI.

Hay un software de cortafuegos que recibe el nombre de intermediario (*proxy*) (servidor intermediario, *proxy* del cortafuegos) que desempeña el papel de software de retransmisión. Establece en representación del usuario el servicio invocado por éste. El objetivo de un sistema intermediario (*proxy*) es que el programa informático de retransmisión efectúe un enmascaramiento de las direcciones de modo que el entorno interno de la organización sea invisible. Se supone asimismo que constituye el paso obligado para todas las aplicaciones que necesitan acceder a Internet. Esto supone la instalación de una aplicación de «retransmisión» en la estación de trabajo del usuario y en el cortafuegos.

La implantación y configuración de un cortafuegos responde a una opción de arquitectura de red para hacer frente de modo más eficaz a las necesidades de seguridad y de control exigidas por la conexión con los sistemas.

El cortafuegos constituye una de las herramientas de implementación de la política de seguridad y no es más que uno de los componentes físicos y lógicos de su instalación. Efectivamente, no basta con tener un cortafuegos para proteger eficazmente la red y los sistemas de una organización. Debe acompañarse asimismo de herramientas, medidas y procedimientos que respondan a los objetivos de seguridad previamente determinados por la política de seguridad. La eficacia del cortafuegos depende esencialmente de su situación con relación a los sistemas que debe proteger, de su configuración y de su gestión.

Aunque los sistemas cortafuegos o de detección de intrusiones contribuyan a realizar ciertos servicios de seguridad, no bastan por sí solos para proteger totalmente los recursos de información.

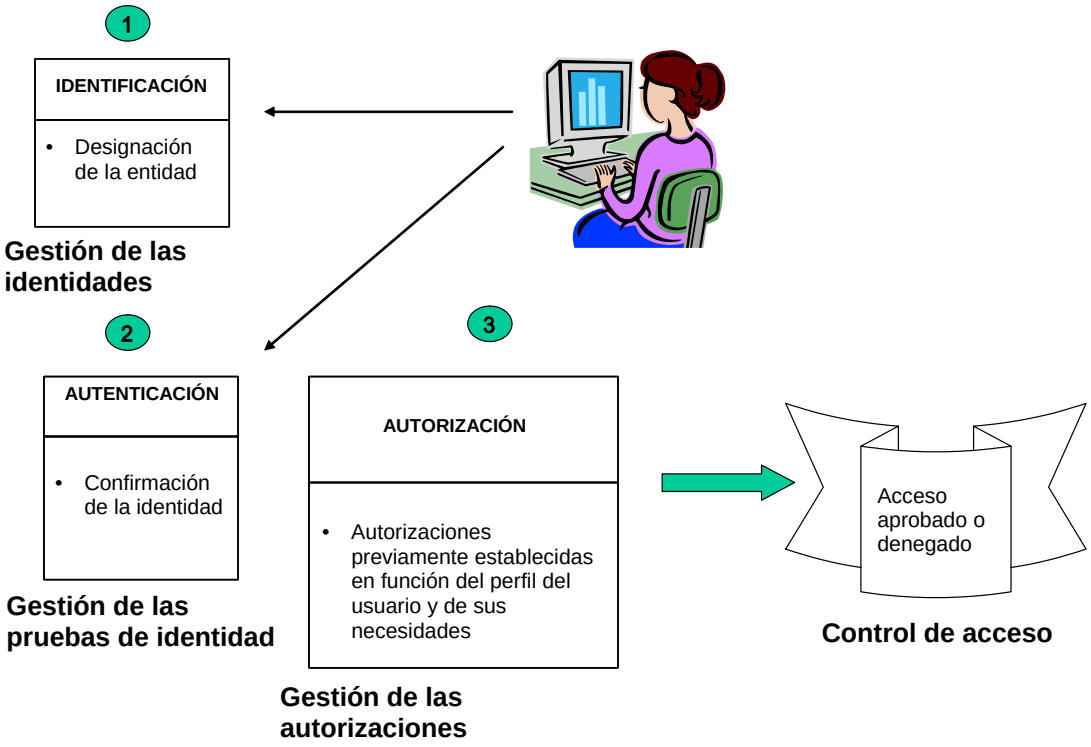
47 Reproducción del libro «Sécurité informatique et télécoms: cours et exercices corrigés»; S. Ghernaouti-Hélie; Dunod 2006.

III.2.8 El control de acceso

III.2.8.1 Principios generales

Los mecanismos de control de acceso lógico a los recursos informáticos se basan en la identificación de las personas, su autenticación y en los permisos y derechos de acceso que les son otorgados (Figura III.10).

Figura III.10 – Bases de los elementos de control de acceso lógico



Tras la autenticación de la identificación, el mecanismo de control de acceso aprueba, en función del perfil del usuario, el acceso a los recursos solicitados. Esto exige que la identificación del usuario (gestión de identidades – *Identity management*), las pruebas de su identidad (gestión de pruebas de identidad – *Identity proof management*) y sus derechos de acceso, se gestionen adecuadamente (gestión de las autorizaciones – *Authorization management*).

El perfil del usuario (*user profile*) contiene toda la información necesaria para decidir la autorización de acceso. Debe definirse cuidadosamente y se determina a partir de la definición de la política de gestión de acceso.

La autenticación permite vincular el concepto de identidad a la persona. Las autorizaciones de acceso permiten filtrar selectivamente las peticiones de acceso a los recursos y a los servicios ofrecidos a través de la red con objeto de no conceder el acceso a los mismos más que a las entidades habilitadas.

El servicio de autenticación tiene por objeto verificar la veracidad de la identidad (concepto de prueba de identidad). Esto suele depender de uno o más de los factores siguientes:

– de un secreto mantenido por una entidad (conocido por ella), contraseña o número de identificación personal (PIN – *Personal Identification Number*);
– de lo que posee (tarjeta, ficha, etc.);
– de lo que es (huella digital, vocal, retiniana, etc.).

La verificación de la identidad depende de un escenario en el que el solicitante del acceso facilita su identidad y una prueba que se supone él sólo conoce o posee (contraseña, clave secreta, huella). El servicio de autenticación procede a comparar esta información con los datos previamente registrados en un servidor de autenticación.

El servidor de autenticación debe estar perfectamente protegido y asegurado por mecanismos adecuados de control de acceso, de gestión segura de sistemas y por la encriptación de los datos que guarda. Los servidores de autenticación no deben ser falibles ni vulnerables puesto que de su robustez depende el nivel de seguridad global de la infraestructura informática y de las telecomunicaciones.

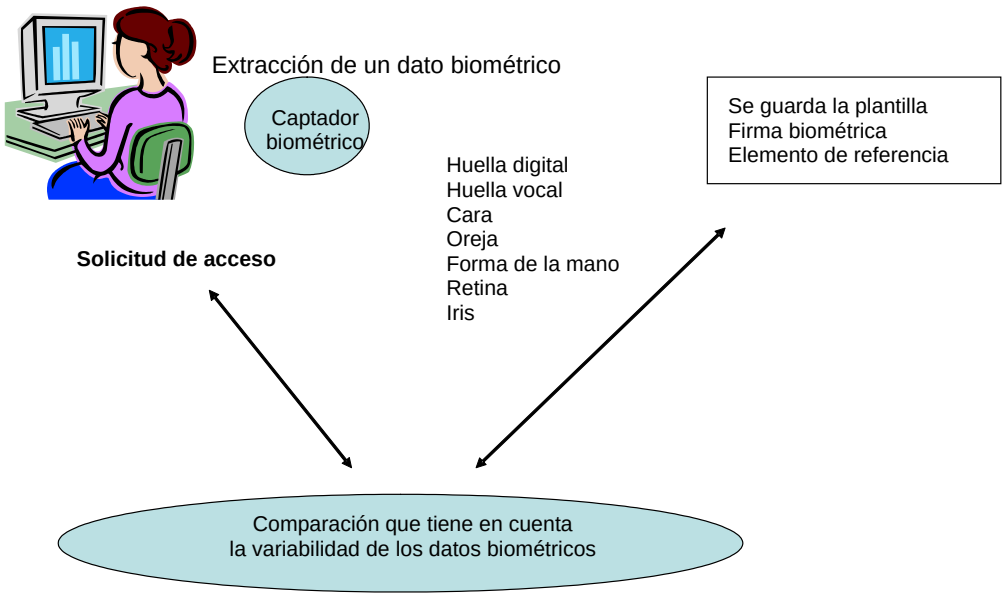
III.2.8.2 Aportaciones y limitaciones de la biometría

La individualización biométrica es un método de individualización a partir de datos biométricos que pueden servir para controlar la identidad de los individuos con el fin de implementar el control de acceso a locales o en el marco de controles judiciales (policía, etc.).

La aplicación de la biometría al control de acceso a los recursos informáticos permite prescindir de la contraseña sustituyéndola por una característica física de la que se puede extraer fácilmente un dato binario.

Para utilizar las características físicas de las personas a fin de identificarlas y validar su identificación, es necesario extraer y registrar previamente las características biométricas de los individuos (concepto de plantilla). Estas grabaciones deben realizarse de modo fiable y guardarse de un modo seguro (Figura III.11).

Figura III.11 – El control de acceso biométrico



El proceso de autenticación puede durar un tiempo considerable debido a que la fase de comparación debe tener en cuenta las variaciones propias del carácter vivo del dato verificado. Por ejemplo, una muestra vocal nunca coincide exactamente con otra. La comparación se basa en un tratamiento estadístico y probabilístico del dato biométrico. La introducción en el sistema de autenticación de este componente de indefinición no permite obtener resultados de autenticación con un grado de exactitud cierto. El sistema no puede certificar al 100% que se trate de la persona «x». La tasa de errores de estos sistemas sigue siendo alta y esto no permite garantizar un nivel de seguridad elevado. La biometría asociada a mecanismos de autenticación «tradicionales» basados en contraseñas (concepto de control doble), refuerza el nivel de seguridad de estos últimos.

Por otra parte, la difusión de la biometría plantea numerosos problemas éticos y ergonómicos así como de orden económico, jurídico y tecnológico, entre los que cabe citar los siguientes:

- la confidencialidad de los datos biométricos que pueden considerarse privados;
- la posibilidad de no disponer de datos biométricos únicos (como ocurre con los gemelos);
- el hecho de que los captadores de datos biométricos se suelan considerar intrusos y sean rechazados por la mayor parte de los usuarios cuando se les plantea esta alternativa. Suponen igualmente una amenaza para la libertad individual en la medida en que podría existir una proliferación de captadores tales como cámaras de vídeo, por ejemplo, distribuidas por los lugares públicos, que actuarían con desconocimiento de los ciudadanos;
- los casos de usurpación o de usos abusivos y fraudulentos de los datos biométricos.

Junto con su falta de precisión y los costes de adquisición, instalación y control que siguen siendo elevados, las soluciones de control de acceso basadas en el uso de datos biométricos están poco difundidas.

Resumen de las limitaciones que afectan a la utilización de datos biométricos para el control de acceso:

1 los datos biométricos que contribuyen a identificar a un individuo varían a lo largo del tiempo;

2 los datos biométricos deben recogerse para crear una muestra de referencia que se guardará en una base de datos. Al traducirse a parámetros digitales, estos datos se hacen frágiles (por lo tanto modificables), debiendo ser protegidos de la mejor manera posible. Para cada demanda de acceso, han de recuperarse los datos biométricos del usuario. Esto plantea un problema de aceptación del método de captura y un sentimiento de intrusión que se suele tolerar bastante mal;

3 la técnica de control de acceso fundamentada en el uso de la biometría no es segura al 100% debido a la variabilidad de las muestras humanas, que se debe tener en cuenta en el proceso de autenticación. Dependiendo de los sistemas, la probabilidad de obtención de falsos positivos y falsos negativos puede ser importante. Esta probabilidad depende de la técnica y calidad de registro de los datos biométricos.

III.2.9 Protección y gestión de las infraestructuras de comunicación

III.2.9.1 Protección

La capa 1 o física puede contribuir a la seguridad de las transmisiones introduciendo perturbaciones en la línea, es decir enviando información no significativa para enmascarar el flujo de datos pertinentes en un flujo ininterrumpido de datos sin importancia. No obstante, para proteger las transmisiones contra escuchas pasivas realizadas por captura de las radiaciones electromagnéticas inducidas por la señal transportada en los soportes de transmisión, habría que aislar completamente estos últimos en jaulas de Faraday. Es evidente que tal medida de protección sólo se adoptaría en caso de necesidad.

La seguridad física de los soportes de transmisión, de los empalmes y de los equipos de conexión debe realizarse correctamente.

La infraestructura de transmisión se debe proteger contra la radiación eventual, que podría poner en peligro la transmisión de datos, y contra los ataques pasivos (escucha de datos) y activos (modificación, destrucción y creación de datos).

Es imprescindible proteger las conexiones de los usuarios. Para esto, hay que identificarlos «¿Quiénes son los usuarios?», localizarlos «¿Dónde están?» y conocer sus necesidades «¿Cuáles son los flujos de aplicación transportados?». Respondiendo a la cuestión general de saber «¿Quién hace qué?» se distinguen las diversas necesidades de la red de transporte.

Para que la transferencia de datos sea segura hay que integrar el proceso de seguridad en el nivel de la infraestructura de comunicación que, por lo tanto, debe ser capaz de asimilar dicho proceso en su totalidad. Esto suele exigir la actualización del conjunto de encaminadores, lo que puede provocar la aparición de problemas relacionados con la interoperabilidad de éstos y con la gestión del cambio.

Por otra parte, la encriptación de los datos a nivel de «red» genera paquetes de datos de tamaño mayor que los paquetes no encriptados; por consiguiente su transferencia utiliza aún más ancho de banda y recursos de comunicación. Además del aumento del tiempo de procesamiento de los paquetes que conlleva el proceso de encriptación, el rendimiento de la red puede verse afectado considerablemente por la implementación de la seguridad a este nivel.

La ventaja principal de la encriptación a nivel de infraestructura de red reside en la independencia de la aplicación y de los mecanismos de encriptación vinculados al transporte que son ahora completamente transparentes para el usuario.

Por contra, la seguridad de las transacciones a nivel de la aplicación (encriptación de los datos lo más cerca posible de la aplicación que los manipula) modifica la propia aplicación y los datos se encriptan antes de entregarse al protocolo de red que se encargará de su encaminamiento. A continuación se desencriptan en el servidor de aplicación de destino. En la fase de establecimiento del diálogo entre dos entidades de aplicación (un cliente y un servidor por ejemplo) se realiza la autenticación y negociación de una clave de sesión. La complejidad de esta fase puede ser variable y exige un retardo de establecimiento también variable. Una vez realizada, la encriptación suele ser bastante rápida. Es independiente de la plataforma de ejecución y de la infraestructura de comunicación.

La protección a nivel de la esfera de trabajo del usuario que implementa una aplicación distribuida ya no depende del transporte de datos ni de la red, sino del entorno directo del usuario. El problema de protección de las aplicaciones reside en el hecho de que es necesario proteger todo el entorno de la aplicación, la estación de trabajo del usuario (y no solamente la aplicación misma) y por extensión su entorno físico (acceso a los locales, etc.).

La protección de las aplicaciones equivale a garantizar los derechos de los individuos en relación con las estaciones de trabajo, con las aplicaciones y con la zona geográfica en las que se integran.

Las funciones de base del sistema operativo de la estación de trabajo del usuario desempeñan un papel primordial en esta protección (imposibilidad que un tercero tome el control durante una sesión, desconexión automática tras un cierto tiempo, etc.). Esto implica asimismo la protección de las tarjetas de red, el soporte de protocolos de aplicación en modo seguro (transmisión de ficheros protegidos, mensajería segura, etc.) y las operaciones de replicación (*mirroring*) y duplicación (*duplexing*) (protección de la información duplicándola en los discos, redundancia de las operaciones de escritura y de los equipos).

La aseguración de la infraestructura de transporte o de la aplicación equivale a tratar, a niveles diferentes, un mismo problema:

- que los procesos y usuarios se autentiquen;
- que el emisor y el receptor utilicen un algoritmo de encriptación/desencriptación idéntico;
- que cada una de las entidades que se comunican entre sí tenga conocimiento del algoritmo y claves de encriptación/desencriptación;
- que las claves de encriptación/desencriptación se gestionen;
- que los datos se formateen antes de ser transferidos.

III.2.9.2 La gestión

Cuando las actividades de gestión de los sistemas y de las redes se realizan correctamente, permiten ofrecer los niveles de disponibilidad y de rendimiento necesarios para la implementación de la seguridad. Entre ellas se incluyen además, las tareas de vigilancia de la red, de detección de las anomalías y de los incidentes (tales como las intrusiones), que contribuyen sobremanera a la seguridad global de la red y del sistema de información al que sirve.

Una buena gestión de la red contribuye a que las infraestructuras, servicios y datos estén disponibles de una manera eficaz. Gracias a la gestión de la red, y especialmente de las funciones de gestión de las configuraciones, del rendimiento y de los incidentes, pueden alcanzarse los objetivos de la seguridad a saber, la disponibilidad y la integridad.

Por otra parte, la dimensión de la gestión de la red que se refiere a la gestión contable permite disponer de todos los datos necesarios no sólo para la facturación a los usuarios sino también para la implementación de las funciones de vigilancia y auditoría que tienen una importancia primordial en materia de seguridad. Esto permite verificar las acciones con fines de prueba o de no rechazo.

La gestión de la red contribuye igualmente a alcanzar el objetivo de confidencialidad en la medida en que asegura que no haya escuchas clandestinas ni accesos no autorizados a los datos. La implementación de la función de control de acceso a los recursos, que forma parte de la gestión de red, es fundamental para la implementación operacional de la seguridad.

De la calidad de la gestión de los encaminadores, de las facilidades de adaptación de su decisión de encaminamiento en función del estado de la red y de las demandas de encaminamiento de tráfico, dependen en gran medida el rendimiento, la calidad de servicio, la disponibilidad y la fiabilidad de la red. La actualización de las tablas de encaminamiento de las grandes redes constituye un verdadero rompecabezas operacional para los administradores de las redes, en la medida en que las diversas modificaciones de los valores de estas tablas deben sincronizarse para evitar el mal funcionamiento y las pérdidas de los datos durante su transmisión. Los protocolos de gestión de red permiten, entre otras cosas, actualizar las tablas de encaminamiento. La administración de la red puede contribuir a la aseguración de los encaminadores al crear accesos seguros durante su configuración, generando alarmas cuando existan intentos de intrusión y asegurando los centros de gestión y supervisión de los encaminadores.

Resulta por tanto imprescindible saber protegerla impidiendo su modificación por parte de terceros y bloqueando o detectando, entre otras, las acciones siguientes:

- modificaciones de las direcciones contenidas en las tablas de encaminamiento, paquetes IP, etc.;
- modificaciones de los caminos y de las copias ilegales de los datos transportados;
- vigilancia de los flujos;
- desvío, modificación y destrucción de los paquetes de datos;
- denegación de servicio, caída de los encaminadores, inundación de la red, etc.

Es importante poder asegurar el proceso de encaminamiento de los datos a través de las redes de telecomunicación. Los proveedores del servicio «red» deben proteger todas las entidades que intervienen en este proceso y muy especialmente los encaminadores y los servidores de nombres para que la calidad del servicio de encaminamiento satisfaga los criterios de seguridad, de disponibilidad (que el servicio sea operacional), de confidencialidad (que los datos se entreguen a los destinatarios correctos) y de integridad (que los datos no se modifiquen durante su transferencia).

La entrega de los datos a los derechohabientes no está garantizada por el servicio de red. Efectivamente, el servicio de entrega correcta no verifica que los datos entregados a la dirección correcta lo sean a las entidades habilitadas para recibirlos. Esto exigiría un control suplementario del tipo «control de acceso». Además, si los datos se transmiten sin codificar y son objeto de escucha, pueden ser comprensibles para terceros no autorizados. Cuando se trata de datos sensibles es necesario encriptarlos para que resulten ininteligibles.

La vigilancia de una red informática consiste en observar el funcionamiento de esta última de modo continuo. La vigilancia de la red tiene por objeto no solamente garantizar que la calidad de servicio de la red sea aceptable sino también detectar problemas, incidentes, errores y anomalías que degraden la eficacia de la red y que puedan llegar a afectar a la seguridad de los recursos para responder lo más rápidamente posible y de manera adaptada a los problemas de funcionamiento. La función de vigilancia de la red permite el rastreo de las acciones y eventos a fin de registrarlas para analizarlas (concepto de auditoría). La vigilancia de la red contribuye asimismo a garantizar la disponibilidad de los recursos verificando el correcto funcionamiento de la red. Por consiguiente, se trata de una función crucial de la gestión de red puesto que contribuye a implementar la gestión de la eficacia, de los incidentes, de las configuraciones, de los usuarios y de la seguridad.

SECCIÓN IV

PLANTEAMIENTO GLOBAL

Capítulo IV.1 – Diversos aspectos jurídicos de las nuevas tecnologías

IV.1.1 Protección de los datos de carácter personal y comercio electrónico[48]

Este apartado aborda la protección de los datos personales en relación, principalmente, con el comercio electrónico e identifica, a partir de la situación existente en Francia y Suiza, las principales legislaciones que deben conocer los administradores de sistemas y los responsables de seguridad, cuando sus organizaciones ofrecen servicios en línea de comercio electrónico. De este modo, pueden extrapolarse y adaptarse a los países en desarrollo los principios generales para la realización de negocios en el ciberespacio.

IV.1.1.1 El comercio electrónico: lo que es ilegal «fuera de línea» lo es también «en línea»

La cuestión del comercio electrónico (cibercomercio) se puede contemplar desde la perspectiva del comercio electrónico con los consumidores (*business-to-consumer* (B2C)) o del comercio electrónico entre empresas (*business-to-business* (B2B)). Asimismo se clasificarán en la misma categoría las variantes asociadas por ejemplo a la ciberadministración. Se tratará entonces de comercio electrónico con el ciudadano y otras instituciones públicas o privadas. Esta distinción es importante a nivel jurídico puesto que el derecho mercantil distingue en general las transacciones entre empresas de las realizadas con el consumidor.

En todos los casos, la seguridad, combinada con las iniciativas oportunas de marketing y de venta por Internet, dentro de un marco legal apropiado, constituye la piedra angular del comercio electrónico. La creación de un contexto favorable al intercambio de datos gracias a la instauración de la confianza basada en las herramientas de seguridad y el respecto a la legislación favorece la adopción por parte del público en general de servicios basados en la informática y las telecomunicaciones y permite asimismo desarrollar una verdadera economía de los servicios.

Hay toda una nueva legislación nacida de la necesidad de definir un marco jurídico apropiado a la utilización de las nuevas tecnologías que viene a completar la mayor parte de la legislación existente igualmente aplicable en el ciberespacio. En todo caso, lo que es ilegal «fuera de línea» lo es también «en línea». El ciberespacio es un espacio internacional y transfronterizo. Por este motivo, el concepto de jurisdicción es muy difícil de delimitar para poder resolver los problemas jurídicos del comercio electrónico. De este modo, cuando se efectúan transacciones a través de la red es necesario mencionar el límite de la oferta y dar una información exacta en cuanto a la jurisdicción aplicable en caso de litigio.

IV.1.1.2 El deber de protección

La protección de los datos personales es un aspecto importante del comercio electrónico. Se debe informar al consumidor del carácter de las informaciones recogidas, utilizadas y comunicadas por el anunciante o por el comerciante en línea. Se debe informar anticipadamente al consumidor de la utilización, comunicación y acceso por parte de terceros a información que le afecta. Se le debe informar asimismo de las precauciones adoptadas para proteger la información que le afecta. Una política real de protección de los datos privados (*privacy policy*) debe expresarse claramente, estar disponible, ser visible y ser fácilmente accesible e inteligible en el momento en que se emprende la transacción comercial. La política debe estar disponible principalmente en el sitio web del comerciante.

Por otra parte, es necesario que la empresa proveedora del servicio adopte las medidas de seguridad suficientes para proteger los datos de los clientes que recoge y procesa. La empresa debe velar por que los servicios de terceros implicados en los intercambios comerciales dispongan de niveles de seguridad adecuados para satisfacer los imperativos de la seguridad.

---

48 A este punto ha colaborado Igli Taschi, ayudante diplomado de la Universidad de Lausana.

IV.1.1.3 El respeto de los derechos fundamentales

La confidencialidad de los datos de carácter personal y el respeto de la intimidad digital derivan del respeto de los derechos fundamentales del hombre.

Ejemplo de Directiva Europea

Además de la Directiva Europea de 1995, existen diversas legislaciones nacionales desde principios de los años 70 que afectan a la protección de los datos personales y el control de la utilización de los ficheros públicos que contienen informaciones nominales con objeto de evitar el riesgo del almacenamiento abusivo de datos personales.

El ejemplo de Francia

La Ley «Informatique et liberté» (Informática y libertad) publicada en enero de 1978, modificada por la nueva Ley Informática y libertad publicada en agosto de 2004 y aplicable con carácter inmediato, constituye un ejemplo de este tipo de iniciativa jurídica en Francia. Esta última introduce conceptos jurídicos adaptados a las nuevas formas de procesamiento aparecidas en la sociedad de la información y en la economía digital, adapta la Directiva Comunitaria 95/46/CE de octubre de 1995 y tiene por objeto reforzar los derechos y protecciones reconocidas a las personas físicas y aumentar el nivel de obligaciones que incumbe a los responsables de los procesamientos.

En estas leyes se suelen abordar cuestiones relativas a la definición de las informaciones nominales o de carácter personal; al derecho de acceso, de oposición y de rectificación de los datos; la finalidad del procesamiento, la recogida de información; la conservación y actualización; la seguridad de los ficheros nominales; la comercialización de los ficheros y el control de los flujos transfronterizos.

En muchos casos, otras leyes vienen a completar esta legislación, como por ejemplo la Ley francesa de Seguridad cotidiana de 15.11.2001 que obliga a borrar y convertir en anónimos los datos relativos a las comunicaciones electrónicas salvo los concernientes a su facturación. Los datos denominados «indirectos» (URL visitadas, direcciones IP de los servidores consultados, titulares de los mensajes, etc.) deben borrarse igualmente.

El ejemplo de Suiza

En Suiza, la Ley Federal de protección de datos data de 1992 (en Alemania: Ley de 21 de enero de 1977, en Bélgica: Ley de 8 de diciembre de 1992, en Canadá: Ley de protección de informaciones personales – 1982S, en Estados Unidos: Ley de protección de las libertades individuales – 1974; Ley de bases de datos y vida privada – 1988).

La protección de los datos en Suiza está garantizada en primer lugar por el Artículo 13/2 de la nueva Constitución Federal, en vigor desde el 1 de enero de 2000, en virtud del cual «*toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent*» (toda persona tiene el derecho de ser protegida contra el empleo abusivo de los datos que le afectan).

Los textos más importantes a nivel federal son la *loi fédérale sur la protection des données* (LPD, Ley Federal de Protección de Datos) de 19 de junio de 1992 y el Reglamento de Aplicación de 14 de junio de 1993. Su aplicación no depende de un soporte particular ni de una técnica específica de recogida y tratamiento de los datos. Se aplica tanto a las personas privadas como a la administración pública, a las personas físicas y a las personas jurídicas de derecho privado, con independencia del tipo de procesamiento considerado. El Artículo 3, letra a) de la LPD precisa que hay que entender por datos personales «*todas las informaciones que se relacionan con una persona identificada o identificable*». Se aplican reglas particulares a los datos sensibles y a los perfiles de la personalidad, conceptos igualmente definidos en la Ley.

El concepto de procesamiento es amplio puesto que incluye «*toda operación relativa a datos personales – con independencia de los medios o procedimientos utilizados – especialmente la recogida, conservación, explotación, modificación, comunicación, archivo o destrucción de los datos*». El Artículo 2/2 de la LPD señala sin embargo un cierto número de situaciones particulares en las que la ley no es aplicable. Se trata por ejemplo del caso de los procesos judiciales pendientes o en la hipótesis de «*datos personales que una persona física procesa para un uso exclusivamente personal y que no comunica a terceros*» (subapartado a). En una sentencia de 5 de abril de 2000, el Tribunal Federal

considera que la mensajería electrónica está amparada por el secreto de las telecomunicaciones. El Artículo 43 de la Ley Federal de Telecomunicaciones (LTC) señala igualmente la obligación de preservación del secreto: «queda prohibido a toda persona que haya estado o esté encargada de garantizar un servicio de telecomunicaciones la entrega a terceros de informaciones sobre las comunicaciones de los usuarios; asimismo, queda prohibido que ofrezca a cualquiera la posibilidad de comunicar dichas informaciones a terceros». El Artículo 44 de la LTC, complementado por los Artículos 6 a 11 de la Ordenanza del Consejo Federal sobre el servicio de vigilancia de la correspondencia postal y de las telecomunicaciones de 1 de diciembre de 1997 (RS 780.11), establece el procedimiento y detalla las condiciones en las que procede efectuar la vigilancia.

La reglamentación suiza en materia de protección de datos personales por Internet es semejante en muchos aspectos a la directiva comunitaria en dicha materia.

IV.1.1.4 Rentabilidad de la legislación

La legislación en materia de tratamiento de datos de carácter personal y de protección de la vida privada en el sector de las comunicaciones electrónicas, es un factor que anima a las instituciones a gestionar adecuadamente su seguridad informática y la de sus redes (datos de los usuarios, vigilancia de las comunicaciones y de los empleados, gestión de las copias de seguridad, tratamiento automatizado de los datos de carácter personal, etc.).

Las organizaciones deben proveerse de los medios suficientes de seguridad y de control.

El valor económico de las inversiones necesarias para garantizar el umbral mínimo de seguridad (protección física y jurídica) es función de las pérdidas materiales y asimismo de los riesgos para su reputación y su imagen que potencialmente afronta la organización. La legislación se convierte por este motivo en un factor endógeno de consideración de la seguridad.

IV.1.2 El comercio electrónico y la formalización de contratos en el ciberespacio[49]

En este apartado se abordan diversos aspectos del concepto de contrato asociado a las transacciones comerciales realizadas en el ciberespacio y se presentan los textos de las principales leyes existentes en Suiza y en la Unión Europea que le son aplicables. A partir del ejemplo jurídico de Suiza y de las principales directivas europeas, pueden identificarse diversos principios de base que pueden adaptarse en función de los países y legislaciones nacionales.

IV.1.2.1 La cuestión del derecho aplicable

El primer problema jurídico que afecta al comercio electrónico lo plantea la definición del concepto geográfico de realización del comercio electrónico. Las características de Internet (cobertura internacional, tecnología digital y modo de funcionamiento) anulan el concepto de frontera geográfica de los Estados ya que los flujos de información no se detienen en las fronteras de los países.

Los datos y los servicios son accesibles y realizables a distancia, con independencia de la ubicación de los internautas y de los servidores. Con frecuencia, el comerciante y el cliente interaccionan desde países distintos. De este modo, el concepto de derecho aplicable adquiere una gran importancia en caso de litigio y constituye un elemento capital para la planificación de la oferta. En este sentido cuando se efectúan transacciones por la red hay que mencionar el límite de la oferta y ofrecer una información exacta en cuanto a la jurisdicción[50] aplicable en caso de litigio.

La legislación aplicable y la jurisdicción pueden convenirse entre las partes del contrato. De no existir dicha cláusula, hay que determinar si el contrato entra en el ámbito de aplicación de un Convenio Internacional tal como el de los Principios Unidroit que afectan a los contratos de comercio internacional (1994) también conocidos como *Netiqueta* o el Convenio de la Haya de 15 de junio de 1955,

---

49 En este apartado ha colaborado Igli Taschi, ayudante diplomado de la Universidad de Lausana.

50 Jurisdicción aplicable: En derecho internacional, designa la ley del país en el que debe desarrollarse el procedimiento jurídico. Se habla asimismo de lex fori. *Regla de procedimiento internacional*.

por ejemplo. Sin embargo, los convenios internacionales no son vinculantes salvo en el caso de que se indique expresamente en el contrato.

De no poderse aplicar ninguna de estas dos soluciones, el contrato se regirá por las reglas de derecho vigentes.

En la legislación suiza, por ejemplo, se aplica la Ley Federal de Derecho Internacional Privado de 1987 (LDIP), cuyo Artículo 1 estipula:

«Art. 1»

[1] La presente Ley rige en materia internacional:
a. la competencia de las autoridades judiciales y administrativas suizas;
b. el derecho aplicable;
c. las condiciones de reconocimiento y de ejecución de las decisiones extranjeras;
d. la quiebra y el convenio de acreedores;
e. el arbitraje.

[2] Se reservan los tratados internacionales.»

El principio de base es el siguiente: se aplica el derecho del Estado con el que el contrato presenta los *vínculos más estrechos* (117/1 de la LDIP). Generalmente, se trata del proveedor de bienes y servicios en la medida en que esto se indique explícitamente en las condiciones generales, con una excepción: el Artículo 120/2 de la LDIP que afecta a los *Contratos celebrados con consumidores* y que estipula lo siguiente:

«Los contratos sobre suministro de consumos normales destinados a uso personal o familiar del consumidor, no relacionados con la actividad profesional ni comercial del mismo, se rigen por el derecho del Estado de residencia habitual del consumidor:

a. si el proveedor ha recibido el pedido en dicho Estado;
b. si la celebración del contrato ha estado precedida en dicho Estado por una oferta o una publicidad y el consumidor ha llevado a cabo los actos necesarios para la celebración del contrato, o
c. si el consumidor ha sido incitado por su proveedor a desplazarse a un Estado extranjero con el objeto de formular desde allí el pedido.

[2] La elección de derecho queda excluida.»

El contenido del sitio, por ejemplo el idioma utilizado o la moneda propuesta, pueden dar una idea del mercado objetivo del comerciante y, eventualmente, de la legislación aplicable.

En lo que se refiere a la jurisdicción, en el caso de que no se haya determinado por un acuerdo entre las partes, la presentación de una queja en el lugar de la residencia o sede del demandado siempre es posible.

IV.1.2.2 La celebración electrónica de contratos

Las reglas aplicables en esta materia suelen ser las mismas que las aplicables a los contratos convencionales. Se celebra un contrato cuando las dos partes han intercambiado una oferta y la aceptación de la misma.

Directiva Europea

La Directiva 97/7/CE del Parlamento Europeo y del Consejo de Europa de 20 de mayo de 1997 trata de la problemática de la venta a distancia y del comercio electrónico e indica que la información previa a la celebración de un contrato debe constar de los elementos siguientes:

– identidad del proveedor y, en el caso de que el contrato necesite un pago anticipado de su dirección;
– características esenciales del bien o servicio;
– precio del bien o servicio, impuestos incluidos;
– gastos de envío, en su caso;

– modalidades de pago, de entrega o de ejecución;

– existencia de derecho de retracto sin perjuicio de los casos contemplados en el Artículo 6, apartado 3 de esta directiva;
– coste de utilización de la técnica de comunicación a distancia, cuando se calcula sobre una base distinta de la tarifa de base;
– vigencia de la oferta o del precio;
– duración mínima del contrato en el caso de contratos sobre suministro indefinido o periódico de bienes o servicios.

El punto más importante de la celebración del contrato se refiere a la definición de lo que representan la oferta y la aceptación de la misma. La mercancía «expuesta» en un sitio Internet con indicación de su precio y la información de carácter publicitario asociada, no constituye una oferta sino más bien una convocatoria de licitación en el sentido del Código de Obligaciones suizo, que estipula en su Artículo 7: «*Art. 7 … [2] El envío de tarifas, precios de venta, etc., no constituye una oferta de contrato …*».

El envío de un mensaje electrónico o de un formulario de pedido se considera igualmente una solicitud de oferta.

Es la aceptación, o la pulsación sobre «comprar» por parte del comprador, lo que permite considerar la oferta en firme y concluir el contrato. La mera consulta de un sitio no puede expresar la voluntad de consumir como tampoco lo es la entrada en un comercio. Por contra, la presentación de mercancías en un sitio web puede constituir una oferta solamente en el caso en que el ofertante indique sus existencias de dicha mercancía y, como consecuencia de un pedido, disminuyan, o bien en el caso de que la naturaleza de las mercancías sea tal que el comerciante tenga siempre la capacidad de satisfacer el pedido.

El contrato se cierra cuando el destinatario del servicio, es decir el consumidor que desea comprar la mercancía expuesta, recibe por vía electrónica procedente del proveedor, el acuse de recepción de la aceptación únicamente si estos documentos se envían en el menor plazo posible. En lo que se refiere al concepto de demora cabe efectuar la distinción entre contrato entre ausentes o entre presentes.

Contrato concluido entre ausentes, sí pero …

El contrato concluido a través de Internet se considera como concluido entre ausentes, lo que implica que la oferta debe aceptarse en un plazo razonable, como lo precisa el Artículo 5 del Código de Obligaciones suizo:

« Art. 5»:

b. Entre ausentes

[1] Cuando la oferta se haya formulado a una persona ausente sin estipular el plazo, el autor de la oferta queda vinculado hasta el momento en que pueda esperar la llegada de una respuesta expedida a tiempo y regularmente.

[2] Tiene el derecho de admitir que la oferta se haya recibido a tiempo.

[3] Si la aceptación expedida a tiempo llega tarde al autor de la oferta, y éste entiende no estar vinculado, debe informar de lo mismo al aceptante con carácter inmediato.»

Sin embargo, si el intercambio de datos sobre el contrato se efectúa a través de un foro de discusión, *chat*, mensajería instantánea o por telefonía sobre Internet, el contrato se considerará concluido entre los presentes y la aceptación deberá ser inmediata. Así, el Artículo 4/1 del Código de Obligaciones suizo dispone que: *«Cuando se haya hecho la oferta a una persona presente, sin fijar un plazo de aceptación, el autor de la oferta queda vinculado si la aceptación no tiene lugar inmediatamente.»*

IV.1.2.3 La firma electrónica

La utilización de un sistema de encriptación asimétrica permite verificar la integridad de los mensajes para garantizar que éstos no han sido modificados durante su transmisión y para cerciorarse de sus emisores, de modo que éstos no puedan negar haber enviado los mensajes (concepto de no rechazo). Para estos servicios de seguridad informática se utiliza un certificado digital que permite «firmar» el documento digital. De este modo, análogamente a la firma manuscrita, se firman digitalmente los

datos (concepto de firma electrónica). A los conceptos de firma y de certificado digital se asocian los de las claves de encriptación (claves privadas y públicas) y el de organismo de certificación (igualmente denominado tercero de confianza o autoridad de certificación).

Para que la firma electrónica pueda considerarse una transposición al mundo digital de la firma manuscrita de un documento en papel, debe estar vinculada únicamente al signatario, permitir la identificación de éste y haber sido creada por medios al alcance exclusivo del signatario.

En la legislación suiza, la Ley reconoce el valor de la firma electrónica en pie de igualdad con la manuscrita. El Artículo 14/2*bis* del Código de Obligaciones define la firma del siguiente modo: «*Art. 14: …c. Firma*

[1] La firma debe escribirla a mano el que se obliga.

…

[2bis] La firma electrónica calificada basada en un certificado calificado emitido por un proveedor de servicios de certificación reconocido en el sentido de la Ley de 19 de diciembre de 2003 de firma electrónica, se asimila a la firma manuscrita, sin perjuicio de las disposiciones legales y convencionales.

…»

Mientras que la firma electrónica se rige por la Ley Federal de Servicios de Certificación en el Dominio de la Firma Electrónica (SCSE) de 19 de diciembre de 2003. En esta Ley se define la firma electrónica así como los diversos participantes en la implementación del mecanismo de firma y del certificado digital.

«Art. 2 Definiciones

En el sentido de la presente Ley, se entiende por:

a. firma electrónica: los datos electrónicos anexos o vinculados lógicamente a otros datos electrónicos que sirven para verificar su autenticidad;

b. firma electrónica avanzada: la firma electrónica que cumple los requisitos siguientes:

1. *estar vinculada únicamente al titular,*
2. *permitir identificar al titular,*
3. *haber sido creada por medios que el titular puede controlar de modo exclusivo,*
4. *estar vinculada a los datos con los que se relaciona de modo tal que toda modificación posterior de los datos sea detectable;*

c. firma electrónica calificada: firma electrónica avanzada basada en un dispositivo seguro de creación de firmas en el sentido del Art. 6/1 y 6/2, y en un certificado calificado de válido en el momento de su creación;

d. clave de firma: datos únicos tales como los códigos y claves criptográficas privadas utilizados por el titular para componer la firma electrónica;

e. clave de verificación de la firma: datos tales como los códigos y claves criptográficas públicas utilizados para verificar la firma electrónica;

f. certificado calificado: certificado digital que reúne las condiciones del Art. 7;

g. proveedor de servicios de certificación (proveedor): organismo que certifica los datos en un entorno electrónico y que, a tal fin, emite certificados digitales;

h. organismo de reconocimiento: organismo que, con arreglo a las reglas de acreditación, está habilitado para reconocer y supervisar a los proveedores …»

La firma electrónica y la Directiva Europea

La Directiva CE 1999/93 de 13 de diciembre de 1999 relativa a un marco comunitario para la firma electrónica distingue tres tipos de firma electrónica según el grado de integración de los mecanismos de encriptación y los niveles de seguridad ofrecidos.

Existen varias modalidades de implementación de la firma electrónica. En primer lugar se puede «firmar» un mensaje sin que la firma dependa del contenido del mismo (concepto de firma electrónica propiamente dicha). De este modo no importa que exista la posibilidad de «despegar» la firma de un mensaje y volverla a utilizar suplantando al propietario de la misma. Para obviar este inconveniente, se puede vincular la firma al contenido a firmar, por medio de una función criptográfica, para poder validar la autenticidad del emisor y la integridad del mensaje cuando se recibe (concepto de firma electrónica avanzada).

Por último, la directiva contempla la firma electrónica cierta que debe basarse en los dispositivos de seguridad del Anexo II relativo a los proveedores de servicio de certificación que emiten certificados calificados[51].

IV.1.2.4 El derecho de revocación

La facilidad con la que se pueden efectuar compras en Internet puede favorecer comportamientos de consumo propios de decisiones poco maduras. En este contexto, el derecho de revocación adquiere una gran importancia.

En Suiza, el derecho de revocación se rige por el Artículo 9 del Código de Obligaciones. Su principio es el siguiente: «la retirada de la oferta será válida, siempre que llegue al destinatario de la oferta antes de ésta». Para la retirada de la aceptación se utiliza idéntico mecanismo.

El derecho de revocación y la Directiva Europea

A nivel europeo el derecho de revocación se rige por la Directiva 1997/7 de 20 de mayo de 1997. En ésta se estipula que para todo contrato a distancia, el consumidor dispone de un plazo de siete días laborables como mínimo para retractarse sin penalización ni necesidad de indicar el motivo. En caso de que el proveedor no cumpla las obligaciones contempladas en el Artículo 5, especialmente las modalidades del derecho de retracción, el plazo es de tres meses.

IV.1.2.5 Gestión de los litigios

A partir del momento de la conclusión válida de un contrato, se plantea la cuestión de la prueba en los litigios. Con independencia de que se trate de Internet o no, resulta necesario aportar pruebas. Por consiguiente, siempre es conveniente conservar justificantes de la transacción, por ejemplo, la copia de un mensaje electrónico e incluso un vuelco de pantalla.

El ejemplo de Francia

En Francia, el Artículo 109 del Código de Consumo considera la prueba discrecional cuando se trata de B2B. En tal caso se admite el mensaje electrónico como medio de prueba en pie de igualdad con el documento en papel. Por contra, en todo lo que se relaciona con el comercio y con el consumidor, se exige la prueba escrita a partir de un cierto importe. Esto se hace con el fin de proteger al consumidor medio que no tiene ni la capacidad ni los medios jurídicos de defenderse cuando hay un litigio contra una empresa comercial.

No obstante, se pueden utilizar los mensajes electrónicos como medio de prueba al amparo de lo dispuesto en la Ley sobre firma electrónica. Esto significa que un mensaje electrónico firmado electrónicamente se considerará prueba válida si se respetan las disposiciones sobre firma electrónica mencionadas anteriormente.

---

51 www.foruminternet.org/documents/textes_europeens/lire.phtml?id=34

Condiciones generales

Con frecuencia, los contratos concluidos a distancia comportan condiciones generales que también forma parte del contrato. Estas condiciones generales deben ser fácilmente accesibles, deben poder consultarse en línea y debe informarse claramente al cliente de que forman parte del contrato, a fin de valorarlas en caso de litigio.

Resolución de litigios en línea

En caso de litigio y habida cuenta del carácter internacional del comercio electrónico, se encuentran a disposición de los interesados otros medios distintos de los tribunales convencionales para resolver sus diferencias. El concepto de ODR (*On-line Dispute Resolution*, *Resolución de litigios en línea*) surge de la voluntad de encontrar soluciones inmediatas a conflictos vinculados al incumplimiento de contratos celebrados por Internet. Este tipo de resolución de litigios se basa en la conciliación que recurre a la negociación, a la mediación y al arbitraje[52]. Y resulta más rápido, asequible y fácil de utilizar para los usuarios. Por contra, al basarse en códigos de conducta o en recomendaciones calificadas de «*soft law*» (derecho naciente) (como por ejemplo, la *Uniform Domain-Name Dispute Resolution Policy (política de resolución de litigios de nombres de dominio uniforme)* del ICANN), su carácter vinculante es limitado.

IV.1.3 El ciberespacio y la propiedad intelectual[53]

IV.1.3.1 La protección de la propiedad intelectual en el ordenamiento jurídico

La propiedad intelectual está protegida por diversas leyes entre las que cabe citar:

- la ley de marcas;
- la ley de derecho de autor;
- la ley de patentes;
- la ley de diseños y modelos;
- la ley de protección de obtenciones vegetales;
- la ley de topografías de los semiconductores;
- la ley de escudos de armas públicos y otros emblemas públicos.

Además, la propiedad intelectual esta contemplada asimismo en la ley contra la competencia desleal.

IV.1.3.2 El derecho de autor y derechos afines

Se trata de una ley que protege:

- a los autores de obras literarias y artísticas;
- a los artistas intérpretes, productores de fonogramas o de vídeogramas así como organismos de difusión.

Una obra es una creación intelectual, literaria o artística, con carácter individual, independientemente de su valor o destino.

Entre las creaciones intelectuales cabe citar:

- las obras que utilizan el idioma ya sean literarias, científicas u otras;
- las obras musicales y otras obras acústicas;
- las obras de bellas artes, en particular las esculturas y obras gráficas;
- las obras de contenido científico o técnico, tales como los dibujos, planos, mapas y obras esculpidas o modeladas;
- las obras de arquitectura;
- las obras de artes aplicadas;

---

52 Este mecanismo de resolución de conflictos es el objeto de un reglamento tipo de la Comisión de Naciones para el Derecho Comercial Internacional (CNUDCI).

53 En este apartado ha colaborado el Profesor Sarra Ben Laggha de la Escuela Politécnica de Túnez, responsable de cátedra en la Universidad de Lausana.

- las obras fotográficas, cinematográficas y demás obras visuales o audiovisuales;
- las obras coreográficas y las pantomimas;
- los programas de ordenador (aplicaciones informáticas);
- los proyectos, títulos y partes de obras dotadas de un carácter individual.

El derecho de autor otorga al autor de la obra (la persona física que ha creado la obra) o a su supuesto autor (la persona que presenta la obra mientras no se haya designado autor de la misma) derechos morales y patrimoniales.

No es necesario depositar la obra en una oficina ni registrar los derechos. Sin embargo, el depósito legal es habitual en ciertas legislaciones. Por otra parte, sólo se pueden proteger las ideas si están plasmadas en obras, puesto que sólo se puede proteger la obra tangible.

Los derechos morales conciernen fundamentalmente al reconocimiento de la calidad del autor y a la decisión de la divulgación o no de su obra y de cuándo, en qué modo y bajo qué nombre hacerlo.

Los derechos patrimoniales conciernen a la utilización de la obra (confección y venta de ejemplares, presentación, circulación, difusión, etc.).

La transferencia de la propiedad de la obra, ya se trate del original o de una copia, no supone la de las de los derechos de los autores que, por otra parte, son cedibles y transmisibles por sucesión.

Los derechos afines se refieren a los derechos de los artistas intérpretes (personas físicas que ejecutan una obra o que participan, en el plano artístico, en la ejecución de la misma), los derechos de los productores de fonogramas y de vídeogramas así como a los derechos de los organismos de difusión.

IV.1.3.3 El derecho de las marcas

La marca tiene por objeto distinguir los productos y servicios del titular de los de otras empresas. La marca tiene asimismo por objeto identificar un objeto (y no sólo un sujeto de derecho identificado más bien por un nombre o una razón social).

Para ser susceptible de protección, la marca no debe corresponder a:

- signos que pertenezcan al dominio público;
- formas que constituyan la naturaleza misma del producto y las necesarias para la función del objeto en cuestión;
- signos que puedan inducir a error;
- signos contrarios al derecho vigente o a las buenas costumbres.

Para poder ser protegida, la marca debe depositarse. Una marca registrada puede ser objeto de oposición si:

- es idéntica a una marca ya registrada para productos idénticos;
- es idéntica o similar a una marca ya registrada para productos o servicios idénticos o similares cuando pueda existir riesgo de confusión.

IV.1.3.4 El derecho de las patentes

Las patentes de invención se otorgan para las nuevas invenciones susceptibles de utilización industrial.

Las patentes de invención no pueden otorgarse ni para lo que deriva de un modo evidente del estado de la técnica, ni para las variedades vegetales ni razas animales, ni para los procedimientos de obtención de animales o vegetales esencialmente biológicos; sin embargo los procedimientos micro-biológicos y los productos obtenidos por estos procedimientos pueden ser objeto de patente.

La patente se otorga (en determinadas condiciones) al que deposita la patente (inventor, su causa-habiente o un tercero al que pertenezca la invención a otro título).

Si la misma invención hubiera sido presentada por varias personas de manera independiente, la patente correspondería a aquella que pudiera invocar un depósito anterior o depósito que gozase de una prioridad anterior.

IV.1.3.5 Protección intelectual de los sitios web

En Internet y especialmente en los sitios web, hay que recurrir a diversos derechos para proteger la propiedad intelectual de los sitios web[54]:

- En lo que se refiere al nombre de dominio:
  - El registro del nombre de dominio no confiere por sí solo ningún derecho exclusivo específico a su titular.
  - Para proteger un nombre de dominio hay que recurrir a las bases legales que son:
    - el derecho de las marcas;
    - el derecho de las razones sociales;
    - el derecho al nombre;
    - el derecho de la competencia;
- En lo que se refiere al contenido del sitio:
  - La difusión de las obras por Internet:
    - el contenido creado especialmente para el sitio, está protegido por el derecho de autor;
    - la digitalización de una obra existente y su difusión en línea es una forma de reproducción que no puede realizarse sin el consentimiento del autor de la obra original;
    - los vínculos hacia otros sitios: la simple utilización de un enlace de hipertexto no lesiona ningún derecho exclusivo puesto que no comporta ninguna reproducción. La cuestión es más delicada para los enlaces profundos (aquellos que permiten llegar a una página sin pasar por la página principal del sitio). Esto plantea la cuestión de si la página en cuestión es una obra o no. En general, este tipo de litigio se rige por el derecho de competencia teniendo como criterio determinante el modo en que los enlaces de hipertexto se utilizan, la lealtad de este uso se presenta entonces como un concepto fundamental.

IV.1.3.6 Carácter complementario de las soluciones

Para garantizar el respeto de los derechos de autor, se adoptan determinadas medidas técnicas. Las legislaciones las sostienen y prohíben su burla.

De este modo existe la protección legal, la protección técnica y la protección legal de la protección técnica.

IV.1.4 Diversos aspectos jurídicos del correo indeseado[55]

IV.1.4.1 Contexto y perjuicios

En un sentido amplio, el correo indeseado (*spam*)[56] se define como el envío de mensajes electrónicos no solicitados, caracterizado por lo siguiente:

- el envío de mensajes no solicitados masiva y reiteradamente;
- los mensajes persiguen un objetivo comercial o se envían con fines maliciosos (*phishing o suplantación de identidad*, control del ordenador, introducción de programas maliciosos (virus, programas informáticos de intromisión publicitaria o *adware*, programas informáticos espías o *spyware*…));
- las direcciones se pueden obtener sin el conocimiento del propietario (violando las normas relativas a la protección de datos de carácter privado);
- el correo indeseado suele incluir contenidos ilegales, equívocos o perjudiciales.

---

54 Extraído del documento de Philippe Gilliéron; «Propriété intellectuelle et Internet» libro CEDIDAC 53, Universidad de Lausana 2003.

55 En este apartado ha colaborado Igli Tashi, ayudante diplomado de la Universidad de de Lausana.

56 La palabra «SPAM» es originalmente una marca registrada de la compañía Hormel, acrónimo de «*Spiced Pork and Meat*», una especie de carne en conserva que llevaban los soldados americanos durante la Segunda Guerra Mundial. Parece ser que los Monty Python han inspirado la asociación de este alimento con la práctica del envío de correos no solicitados. En una de sus célebres actuaciones, cantan «Spam Spam Spam Spam...» para alabar las cualidades de este producto, repetidamente y tan fuerte que no deja oír la conversación de los demás protagonistas.

La utilización de correo indeseado en ciertas circunstancias, teniendo en cuenta su carácter no solicitado, puede considerarse como política de venta o publicidad agresiva.

Hoy en día, el fenómeno del correo indeseado no se limita solamente a la mensajería electrónica por Internet sino también a los teléfonos móviles a través de los SMS o mediante los nuevos equipos multimedios tales como los PC de bolsillo (*pockets* PC).

El correo indeseado genera costes para todos los usuarios de Internet. Estos costes suelen estar relacionados con el tiempo de procesamiento de los mensajes y la adquisición de diferentes herramientas para protegerse contra este fenómeno sin contar con el coste social, es decir la pérdida de confianza por parte de los usuarios, la disminución de la productividad de las organizaciones, etc.

De acuerdo con un estudio de la sociedad Clerswift publicado en el *Journal du Net* el 13 de septiembre de 2005, el reparto del correo indeseado por categorías es el siguiente:

Tipos de correo indeseado	**Junio de 2005**
Sanidad	43,86%
Productos	37,65%
Finanzas	9,06%
Pornografía	5,32%
Suplantación de identidad (*phishing*)	1,41%
Apuestas	0,1%
Otros	2,32%

El correo indeseado puede adoptar diversas formas de estafa, de las que una de las más comunes es la denominada estafa nigeriana o *carta de Nigeria*[57]. La suplantación de identidad o *phishing* consiste en enviar un mensaje que pretende estar emitido por una entidad conocida tal como un banco que invita al internauta, bajo diversos pretextos, a conectarse a un falso sitio de la entidad en cuestión y a entregar sus códigos de acceso e informaciones sensibles, que serán utilizadas posteriormente sin su conocimiento.

Además de las estafas y de la suplantación de identidad o *phishing*, el correo indeseado puede enviarse también con objeto de destruir y bloquear la mensajería del destinatario provocando de este modo su indisponibilidad y la denegación de servicio de sus recursos. El «bombardeo de mensajes» puede adoptar diversas formas: envío de mensajes de gran tamaño que genera problemas a nivel del procesamiento o del almacenamiento temporal, envío de gran número de mensajes o envío a un gran número de destinatarios con objeto de inundar el servidor o incluso, de usurpar la dirección del remitente.

IV.1.4.2 Respuestas jurídicas al fenómeno del correo indeseado

El correo indeseado incumbe a varios dominios jurídicos, especialmente el de la protección de datos, la competencia desleal y asimismo el dominio penal.

---

57 El remitente del correo indeseado se presenta como heredero de un rico importante, normalmente en un país lejano, fallecido recientemente. El sedicente heredero pretende tener problemas para hacer valer sus derechos y propone a la víctima utilizar la cuenta bancaria de esta última ofreciéndole a cambio una remuneración importante por las molestias ocasionadas. Esta última debe adelantar los gastos relativos a la transacción. Se trata invariablemente de intentos de estafa.

El ejemplo de Suiza

En Suiza, no hay ninguna norma jurídica que regule explícitamente la cuestión del correo indeseado.

Desde el punto de vista de la protección de datos, el Director General de la Agencia de Protección de Datos, especifica en su documento «*Aide-mémoire concernant les messages publicitaires indésirables diffusés par courrier électronique (spams) (notas sobre los mensajes publicitarios indeseables difundidos por correo electrónico (spams)*»[58], que «*las direcciones electrónicas constituyen datos personales que permiten identificar a las personas*». En virtud del Artículo 12/3 de la Ley Federal suiza de Protección de Datos (LPD, RS 235.1), «…*Como norma general, no hay ataque a la personalidad cuando la persona afectada haya permitido el acceso libre a sus datos y no se haya opuesto formalmente a su procesamiento*.». El tratamiento de direcciones electrónicas por un emisor de correo indeseado constituye una desviación del fin primordial si se considera el Artículo 4/3, LPD, realizado sin conocimiento, Artículo 4/2, LPD, y sin el consentimiento, Artículo 13/1, LPD, de la persona afectada. Se trata por consiguiente de un ataque contra la protección de datos.

Art. 4 Principios

[1] Toda recogida de datos personales sólo podrá realizarse de un modo lícito.

[2] Su tratamiento debe efectuarse con arreglo a los principios de la buena fe y de la proporcionalidad.

[3] Los datos personales no deben tratarse más que con el fin indicado en el momento de su recogida, ya sea el previsto por las leyes o el determinado por las circunstancias.

La Ley de Protección de Datos concede a las personas afectadas la posibilidad de recurso legal, con arreglo al Artículo 15 LPD que remite al Artículo 28 y ss. del CC.

La Directiva Europea

A nivel europeo, la Directiva 95/46/CE de 24 de octubre de 1995 *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales* define los estándares mínimos en materia de constitución de ficheros y de tratamiento de datos. El Artículo 10 de esta Directiva obliga a que el titular conozca la identidad del responsable del tratamiento y, en su caso de su representante, y los fines del tratamiento de que se van a ser objeto los datos.

El ejemplo de Francia

En Francia, la Ley «informatiques et libertés (informática y libertad)» ha introducido en el Código Penal francés la infracción de ataques al derecho de la persona, resultante de ficheros o tratamientos informáticos. Esta Ley que data de 1978, fue revisada en 2004 introduciendo 14 nuevos Artículos que endurecían las penas en materia de datos de carácter personal.

El ejemplo de Estados Unidos

Estados Unidos, al ser el primer país generador de correo indeseado, ha creado un texto legal específico relativo al correo indeseado que permite procesar a los emisores de correo indeseado: la Ley CAN SPAM de 1 de enero de 2004.

La captura de direcciones en sitios web está prohibida y se prohíben asimismo los programas que generan direcciones de correo electrónico combinando aleatoriamente letras y números.

El correo indeseado plantea asimismo un problema desde el punto de vista de la competencia desleal al utilizarse con fines publicitarios.

El correo indeseado, la publicidad y la competencia desleal

La publicidad por Internet no dispone de ningún marco legal específico. Se refiere al derecho de la publicidad en general. En noviembre de 2001, la Comisión Suiza para la lealtad publicó un aviso relativo al envío de correo indeseado, considerándolo como un método de venta especialmente agresivo. La utilización de dicho método contemplado desde el punto de vista de la publicidad debe respetar ciertos aspectos importantes con independencia de que se efectúe en el marco del comercio «convencional» o en el del comercio electrónico.

---

58 Sitio: www.edsb.ch/f/doku/merkblaetter/spam.htm

Esto afecta:

- a la protección de los jóvenes internautas;
- al respecto de la persona humana;
- al respecto de una publicidad leal, verídica y honesta;
- al respecto de la intimidad jurídica de los internautas;
- a la facilidad de navegación.

El legislador suizo estipula en la Ley Federal contra la competencia desleal, Artículo 3, letras b, c y d: *«Actúa de manera desleal aquel que, esencialmente:*

…….

b. Proporciona indicaciones inexactas o falaces sobre sí mismo, su empresa, razón social, mercaderías, obras, prestaciones, precios, existencias, métodos de venta, o negocios, o aquel que, con tales alegaciones otorga ventaja a un tercero sobre sus competidores.

c. Exhibe o utiliza títulos o denominaciones profesionales inexactas, que puedan dar a entender diferencias o capacidades particulares.

d. Adopta medidas conducentes a provocar la confusión con las mercaderías, obras, prestaciones o asuntos de un tercero».

Cabe destacar que es el apartado h el que pone el dedo en la llaga de la problemática del correo indeseado al estipular lo siguiente:

«Actúa de manera desleal aquel que, esencialmente:

…….

h. Obstaculiza la libertad de decisión de la clientela utilizando métodos de venta particularmente agresivos»

Cuando se utiliza con fines comerciales con la intensidad de envíos mencionada, el uso del correo indeseado puede caer en el ámbito de este Artículo.

El correo indeseado y la intención delictiva

Cuando los emisores de correo indeseado actúan con intención delictiva, ésta puede referirse al derecho penal. Aunque los mensajes puedan tener carácter comercial, su contenido puede ser ilegal.

El correo indeseado y la pornografía

La mayor parte de los mensajes de correo indeseado invitan a visitar sitios de contenido pornográfico. Esta conducta está prohibida por el Artículo 197 del CPS (Código Penal suizo), y especialmente el hecho de dar acceso a este tipo de contenidos a personas que no lo desean (Artículo 197/2) y a los menores de 16 años (Artículo 197/1).

El correo indeseado, las estafas, los virus y la venta de productos prohibidos

La estafa está prohibida en el Artículo 146 del Código Penal suizo. Se define como la obtención de la víctima, con ánimo de lucro, de una ventaja pecuniaria. Esta definición es perfectamente aplicable al caso de la carta de Nigeria.

A veces el correo indeseado es el mejor medio de introducir virus en las máquinas destinatarias. En el derecho suizo, la introducción de virus se considera un deterioro de datos prohibido por el Artículo 144*bis* del Código Penal, en la medida en que dicho virus provoque daños (modificación de datos, borrado o inutilización de los mismos) para el internauta afectado.

La utilización del correo indeseado para venta de medicamentos constituye asimismo una práctica prohibida por la Ley suiza. La Ley sobre medicamentos y dispositivos médicos (LPTh) prohíbe en su Artículo 32 la publicidad que pueda incitar a un uso excesivo, abusivo o inapropiado de los medicamentos, y la publicidad de medicamentos que no puedan comercializarse en Suiza o que no puedan entregarse sin receta.

IV.1.4.3 La regulación del correo indeseado

Hay dos planteamientos opuestos para la regulación del correo indeseado: el de consentimiento previo (*opt-in*) y el de autoexclusión (*opt-out*).

El de consentimiento previo, también conocido como «*marketing con permiso*», es el más respetuoso con el internauta en la medida en que se trata de no enviar más que publicidad dirigida si éste ha otorgado su consentimiento explícito. La opción de recibir mensajes publicitarios puede materializarse como casilla de autoverificación previamente marcada o no, e incluso darse por supuesta. En este último caso, se debe prevenir al visitante con claridad del carácter comercial y de las consecuencias exactas de su inscripción.

El concepto de autoexclusión (*opt-out*) se refiere a la cancelación de la inscripción y consagra la existencia de un derecho de oposición *a posteriori* a recibir correos electrónicos. A tal efecto, cada mensaje publicitario enviado debe ofrecer la posibilidad de borrarse del fichero. Los ficheros *opt-out* pueden o bien constituirse de manera legal (por ejemplo, por compra de un fichero *opt-in*) o bien crearse a partir de una captura masiva de direcciones.

Los legisladores suizos y americanos han optado por la solución *opt-out* mientras que el planteamiento de la Comunidad Europea se inclina más bien por la solución *opt-in* basándose en la Directiva 2002/58/CE *relativa al tratamiento de datos personales y la protección de la vida privada en el sector de las comunicaciones electrónicas (directiva sobre vida privada y comunicaciones electrónicas*).

Dado que los emisores de correo indeseado suelen actuar anónimamente o desde el extranjero, el recurso a la justicia suele resultar caro y complicado y supone la mayor parte de las veces el recurso a un abogado.

IV.1.4.4 Respuestas técnicas al fenómeno del correo indeseado

Técnicas basadas en la limitación de recursos

Limitando recursos tales como el número de destinatarios por mensaje, el número de mensajes por remitente y por unidad de tiempo, podría limitarse la repercusión del correo indeseado.

La lista negra

Se fundamenta en calificar el correo en función de la reputación del servidor que utiliza el emisor.

La reputación de un servidor de correo que ha emitido recientemente correo indeseado queda afectada en la medida en que se supone que podría seguir emitiéndolo. El servidor del emisor se identifica por su dirección IP.

Filtro de palabras clave

Se trata de filtrar mensajes en base a ciertas palabras clave. Esta técnica resulta insuficiente debido a lo fácil que es para un emisor de correo indeseado enviar mensajes cuyo contenido burle los filtros de palabras clave.

Filtro de huella

En la medida en que el correo indeseado consiste en el envío masivo de mensajes idénticos, un filtro de huella calcula una firma en base al contenido del correo electrónico y lo compara con una base de datos de huellas de mensajes considerados correo indeseado.

Política de lucha contra los programas informáticos maliciosos

Cada vez son más frecuentes los programas informáticos maliciosos (virus, troyanos, robots,...) que instalan un servidor de mensajería en la máquina infectada. Esta funcionalidad de herramientas maliciosas tiene por objeto facilitar la propagación del correo indeseado. La lucha contra éste pasa pues por la persecución de los programas informáticos maliciosos.

La utilización de programas informáticos contra el correo indeseado a nivel de servidores de mensajería contribuye a limitar la propagación de aquél bloqueándolo, aunque no siempre con la eficacia deseada. Efectivamente, a veces no llegan a los destinatarios mensajes que no son correo indeseado (concepto de *falsos negativos*) e incluso, mensajes que sí son correo indeseado se consideran normales (concepto de *falsos positivos*).

Por otra parte, el comportamiento del internauta puede desempeñar un papel importante en la lucha contra el correo indeseado. Por ejemplo, la adopción de un comportamiento consciente de la mensajería (sensibilización al riesgo de usurpación de identidad, control preventivo del uso que se hará de su dirección electrónica antes de confiarla a un formulario en línea, utilización de varias direcciones electrónicas, evitación de ciertos sitios, no apertura de mensajes de origen desconocido, supresión de mensajes de correo indeseado sin leerlos, no responder nunca, no pulsar nunca sobre las líneas de hipertexto contenidas en estos mensajes …) contribuye a limitar la magnitud del correo indeseado.

IV.1.4.5 Complementación técnico jurídica

En la medida en la que las soluciones jurídicas tengan una repercusión limitada sobre la práctica del correo indeseado, habrá que recurrir a soluciones de carácter tecnológico. Sólo la complementación de las soluciones técnicas y jurídicas permite luchar contra el fenómeno del correo indeseado. Un emisor de correo indeseado menos, desalentado por una norma jurídica, o frustrado eficazmente por una solución técnica, supone siempre varios millones de correos indeseados no enviados.

IV.1.5 Resumen de los principales problemas jurídicos relacionados con el ciberespacio[59]

IV.1.5.1 Estatuto jurídico de la Internet comercial

El estatuto jurídico de la Internet comercial se refiere a la definición de los estatutos de las herramientas empleadas en el marco de utilización de las tecnologías de la información.

En lo que se refiere a la mensajería electrónica, se plantean cuestiones sobre el contenido de los mensajes, la dirección de la mensajería, la problemática de identificación a través de dicha dirección: usurpación de la identidad, de un signo distintivo o de la razón social de una empresa. Esto incumbe al derecho civil de los países.

En lo referente a los sitios web, el concepto de obra, su calificación de audiovisual o no, plantea problemas relacionados con el derecho de autor. Los enlaces hipertexto remiten al problema de sus contenidos, de la responsabilidad, de la calificación protegida o no y plantean igualmente problemas relacionados con los motores de búsqueda.

IV.1.5.2 El cibercontrato

Los problemas planteados por la celebración de contratos en el ciberespacio no son exclusivamente de orden jurídico. En efecto, para ello se necesita, entre otras cosas, la implementación de mecanismos técnicos que permitan su celebración (herramientas y procedimientos utilizados (carácter mundial, inmaterial y desvinculación geográfica)).

Desde el punto de vista jurídico, cabe observar:
- la oferta; calificación (a distancia o no), aceptación;
- la publicidad y la venta, el correo indeseado, etc.
- la ejecución del contrato;
- la aceptación de la oferta *en línea* y la expresión informática de la aceptación;
- el derecho de retracto;
- la determinación de la ley aplicable así como las jurisdicciones competentes.

Existen diversas directivas europeas a propósito, a saber:
- el Reglamento de la CE 44/2001 de 22 de diciembre de 2000 relativo a la competencia jurisdiccional y al reconocimiento de las decisiones en materia civil y mercantil;
- la Directiva CE 2000/31 sobre comercio electrónico;

---

59 En este apartado ha colaborado Igli Taschi, ayudante diplomado de la Escuela de HEC de la Universidad de de Lausana.

– la Directiva 98/34/CE que prevé un procedimiento de información en el sector de las normas y reglamentos técnicos;
– la Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo 1997, relativa a la protección de los consumidores en materia de contratos a distancia.

Además, hay que tener en cuenta la Ley CNUDCI sobre comercio electrónico de 1996, las *declarations on the global Electronic Commerce* (*declaraciones sobre comercio electrónico mundial*) de 1998 y la *Joint EU-US statement on Electronic commerce* (*declaración conjunta UE-EE.UU. sobre comercio electrónico*.

IV.1.5.3 El documento y la firma electrónica

El documento electrónico firmado electrónicamente plantea el problema de su valor. El objetivo consiste en poder garantizar el valor jurídico de la firma estampada en un documento a fin de identificar al autor de la misma y de constatar su voluntad de estampar la firma y por tanto de asumir la responsabilidad del contenido de dicho documento.

Cabe recordar la Directiva CE 93/1999 de 13 de diciembre de 1999 relativa a un marco comunitario para las firmas electrónicas y en *Italia,* la Ley de 15 de marzo de 1997 Nº 59, en EE.UU., *Electronic Signatures in Global et National Commerce Act* (*Ley de firmas electrónicas en el comercio mundial y nacional*) de 30 de junio de 2000 así como en Reino Unido, por ejemplo, la *Electronic Communication Act* (*Ley de comunicaciones electrónicas*) de 25 de mayo de 2000.

IV.1.5.4 Medios electrónicos de pago

Los medios electrónicos de pago, tarjetas de crédito, cheques y dinero electrónico, pueden inducir al abuso por parte de terceros que pueden interceptar la información asociada, por ejemplo, durante la comunicación entre los proveedores del servicio y sus destinatarios.

La Directiva CE 2000/46 sobre dinero electrónico

IV.1.5.5 Protección de los nombres de dominio

El nombre de un dominio constituye un nuevo bien inmaterial que puede poseer un valor comercial considerable. La problemática asociada a los nombres de dominio se centra en los puntos siguientes:
– Las marcas y los nombres de domino.
– Los signos distintivos y los nombres de dominio.
– Los nombres comerciales y los nombres de dominio.

Además de las leyes nacionales sobre marcas, nombres y patentes, cabe citar en Estados Unidos la Anticybersquatting Consumer Protection Act (ACPA), *Ley para la protección del consumidor y contra el registro abusivo de nombres de dominio*.

IV.1.5.6 La propiedad intelectual

La propiedad intelectual en Internet plantea cuestiones vinculadas a los derechos de autor, marcas y patentes. Citemos, por ejemplo: el tratado de la OMPI sobre los derechos de autor, el tratado de la OMPI sobre las interpretaciones o ejecuciones y fonogramas, a nivel europeo el Libro Verde sobre el derecho de autor y derechos afines en la sociedad de la información de 1995 así como la Directiva del Parlamento Europeo y del Consejo sobre armonización de determinados aspectos del derecho de autor y derechos afines en la sociedad de la información.

IV.1.5.7 Protección de la intimidad digital

En el contexto de la protección de la intimidad digital, se prohíbe el envío de correo indeseado (ver Directiva EU 97/7 sobre protección de los consumidores en los contratos celebrados a distancia y la Directiva CE 97/66 sobre la protección de personas en relación con los datos personales en el dominio de las telecomunicaciones que prohíbe el marketing directo del correo indeseado).

IV.1.5.8 Otras cuestiones de orden jurídico

Sin ánimo de ser exhaustivos, hay muchas otras cuestiones jurídicas que deben tenerse en cuenta cuando se trata de definir un marco legal apropiado para la utilización de Internet. Entre ellas cabe citar todas las relativas a:

- el concepto de defensa de la competencia (véanse las directivas americanas «Antitrust guidelines for collaboration among competitors» (Directrices de defensa de la competencia para la colaboración entre competidores) de abril de 2000);
- la responsabilidad de los proveedores e intermediarios técnicos (las responsabilidades que afectan al proveedor relativas a las actividades del internauta, las actividades delictivas, la pedofilia, pornografía, etc.;
- y el secreto de la correspondencia.

Capítulo IV.2 – Perspectivas

IV.2.1 La educación, formación y sensibilización de los que intervienen en la ciberseguridad

Es importante concienciar a todos los que intervienen en el mundo de Internet en cuanto a los beneficios del control de la seguridad y de las medidas elementales que, enunciadas con claridad, definidas y aplicadas inteligentemente, refuerzan la confianza de los usuarios en las tecnologías de tratamiento de la información y de la comunicación de las que forma parte Internet. Hay que hacer de este último un patrimonio abierto a todos y no el beneficio exclusivo de la delincuencia.

La difusión de una cierta cultura y un enfoque multidisciplinar de la seguridad y del control del riesgo informático de origen delictivo es obligatoria. La posesión de una visión estratégica de estas problemáticas se ha convertido en una necesidad, tanto para las organizaciones como para los Estados.

Por otra parte, resulta igualmente necesario educar, informar y formar en las tecnologías de tratamiento de la información y de las comunicaciones y no solamente en la seguridad y en las medidas disuasorias. La sensibilización a los problemas de seguridad no debe limitarse al fomento de una cierta cultura de seguridad. Además de la cultura de seguridad debe existir una cultura informática. Asimismo hay que dotar de los medios necesarios a los distintos implicados para que aprendan a gestionar el riesgo tecnológico, el operacional y el que afecta a la información, que les amenazan en función del uso que hacen de las nuevas tecnologías.

La dimensión virtual de Internet y su aspecto lúdico, pueden ocultar – especialmente para los jóvenes y los no iniciados en la informática – el daño potencial de estos ataques que es considerable y puede alcanzar tintes dramáticos tanto para las organizaciones (empresa, administración o colectividad) como para los individuos víctimas de los mismos. Sin embargo, el control de los riesgos tecnológicos no se limita a la persecución de los piratas informáticos ni a la implementación de las reglas tecnológicas. Los daños más graves suelen provenir de una simple negligencia motivada por la incompetencia, los fallos de diseño o la implementación de tecnologías, por el excesivo poder otorgado a los administradores de sistemas, por una gestión defectuosa, etc.

IV.2.2 Un nuevo planteamiento de la seguridad

La conciencia de la fragilidad del mundo digital y de la falta de control total no sólo de las tecnologías e infraestructuras informáticas y de las telecomunicaciones sino también de las soluciones de seguridad comercializadas debe plantear serias cuestiones en cuanto a la dependencia de una tecnología difícilmente controlable. El secuestro de los datos por soluciones informáticas es una realidad que no es necesario ocultar.

Resulta ingenuo pensar que habrá soluciones de orden tecnológico o jurídico que palien los errores de diseño y de gestión de la informática y de las telecomunicaciones, ya sea esto a nivel estratégico, táctico u operacional. Además, las medidas tradicionales de seguridad no podrán proteger correctamente los recursos sensibles o críticos de las personas, de las organizaciones y de los Estados, si no se realizan de modo transparente, verificable y controlable.

La implementación de una estrategia completa de seguridad que integre las fases de prevención, protección, defensa y reacción pasa por la adopción de medios humanos, jurídicos, tecnológicos y económicos que permitan su realización.

IV.2.3 Propiedades de la política de seguridad

A grandes rasgos, una buena política de seguridad es el resultado de un análisis de riesgos y se define de manera completa y coherente a fin de responder con precisión a las necesidades de seguridad en un contexto dado.

La definición de la política debe ser:

- simple y comprensible;
- adoptable por un personal previamente sensibilizado, e incluso formado;
- fácilmente realizable;
- de mantenimiento fácil;
- verificable y controlable.

La política de seguridad no debe ser estática. Debe evaluarse, optimizarse y adaptarse periódicamente a la dinámica del contexto en el que se inscribe. Debe ser configurable y personalizable de acuerdo con los perfiles de los usuarios, según los flujos y en función del contexto y de la localización de sus protagonistas. La política de seguridad varía en función del espacio y del tiempo.

La política de seguridad puede estructurarse en distintas políticas de control de acceso, de protección, de gestión de crisis, de seguimiento y de optimización y, finalmente, de seguridad.

IV.2.4 Identificación de los recursos sensibles para protegerlos

La realización de un inventario completo y preciso de todos los recursos e implicados de la cadena de seguridad, contribuirá al conocimiento de los entornos así como a su protección. La identificación de los valores y la clasificación de los recursos para determinar su grado de sensibilidad (o grado de criticidad) permiten diferenciar lo que debe ser obligatoriamente asegurado. Esto último indica su importancia en caso de pérdida, alteración o divulgación de los datos. Cuanto más grave son las consecuencias para la organización, más sensible es el recurso y más valor posee.

Cada recurso puede percibirse como un objetivo de seguridad para el que hay que identificar los riesgos y sus escenarios posibles (error de utilización, de parametrización, accidentes, dolo, sabotaje, ataque lógico, etc.), los mecanismos de seguridad inherentes y aplicables (configuración, parámetros, etc.), así como las restricciones técnicas y organizativas a fin de determinar la viabilidad técnica y organizacional de la política de seguridad para cada objetivo.

IV.2.5 Objetivos, misión y principios fundamentales de la ciberseguridad

Los objetivos de la ciberseguridad son:

- la confidencialidad (ningún acceso ilícito): preservación del secreto de la información y acceso exclusivamente a las entidades autorizadas;

la integridad y la exactitud (ninguna falsificación y ningún error): mantenimiento integral y sin alteración de los datos y programas;

la disponibilidad (ningún retraso): mantenimiento de la accesibilidad de modo continuo y sin interrupción ni degradación;

- la perdurabilidad (ninguna destrucción): los datos y programas informáticos existen y se conservan el tiempo necesario;
- el no rechazo y la imputabilidad (ninguna impugnación): garantía del origen, de la fuente, del destino y de la veracidad de una acción;
- el respeto a la intimidad digital;
- la autenticación (ninguna duda sobre la identificación de un recurso).

Las actividades de una misión pueden clasificarse en los siguientes grupos:

- concebir un plan de seguridad en función de un análisis previo de riesgos;
- definir el perímetro de vulnerabilidad relacionado con la utilización de las nuevas tecnologías;
- ofrecer de modo continuo un nivel de protección adaptado a los riesgos afrontados;
- implementar y validar la organización, las medidas, las herramientas y los procedimientos de seguridad;
- efectuar el seguimiento, auditar, controlar y hacer evolucionar el sistema de información y su seguridad;
- optimizar el rendimiento del sistema de información en función del nivel de seguridad requerido;
- armonizar las necesidades con los riesgos y los costes.

Los principios fundamentales a los que debe referirse toda acción emprendida en nombre de la realización de la ciberseguridad son los siguientes:

- principio de vocabulario. Necesidad de acordar un idioma común de definición de la seguridad;
- principio de coherencia. La ciberseguridad resulta de la integración armoniosa de las herramientas, mecanismos y procedimientos vinculados a la prevención, detección, protección y corrección de los siniestros relativos a fallos, dolo o causas naturales;
- principio de voluntad de la dirección. Es responsabilidad de los dirigentes facilitar los medios necesarios para la implementación y gestión del plan de ciberseguridad;
- principio financiero. El coste de la seguridad y de las medidas de control debe estar en relación con el riesgo;
- principio de simplicidad, de universalidad y de discreción. Las medidas de seguridad deben ser simples, flexibles y comprensibles para los internautas. Las soluciones y medidas de seguridad no deben ser provocadoras para no tentar a un atacante potencial;
- principio de dinamicidad y de continuum. La seguridad deber ser dinámica para integrar la dimensión temporal de la vida de los sistemas y de la evolución de las necesidades y los riegos. Los sistemas deben ser operacionales de modo permanente;
- principio de evaluación, de control y de adaptación a fin de garantizar la adecuación del nivel de seguridad a las necesidades reales.

IV.2.6 Factores de éxito

IV.2.6.1 Líneas directrices en materia de estrategia

Las condiciones de éxito para la realización de una estrategia de seguridad son las siguientes:

- una voluntad estratégica;
- una política de seguridad simple, precisa, comprensible y aplicable;
- la publicación de la política de seguridad;
- una gestión centralizada de la seguridad y una cierta automatización de los procesos de seguridad;
- un nivel de confianza y de integridad de las personas, de los sistemas y de las herramientas implicadas;
- procedimientos de registro, vigilancia y auditoría;
- la voluntad de evitar poner los recursos en situación de peligro;
- un marco legal aplicable a nivel nacional e internacional;
- el respeto de las restricciones de orden jurídico.

IV.2.6.2 Pautas de actuación para los internautas

A continuación se presentan ciertas pautas para los internautas que constituyen medidas sencillas, económicas y relativamente eficaces, para que al adoptarlas los usuarios contribuyan a reforzar la seguridad de sus recursos y ciberactividades[60]:

- cuando el ordenador no se utiliza debe estar apagado;
- el internauta no debe abrir los correos de origen desconocido;
- el internauta debe disponer de un antivirus actualizado periódicamente para garantizar un mínimo de seguridad;
- el internauta no debe divulgar sus contraseñas y debe cambiarlas periódicamente;
- el internauta no debe divulgar por Internet datos personales relativos a sí mismo o a terceros;
- el internauta no debe permitir a un tercero utilizar su cuenta para navegar por Internet;
- el internauta debe utilizar sistemas de encriptación cuando pretenda proteger sus datos;
- el internauta no debe visitar sitios de carácter inapropiado, bajarse programas o ficheros ilegales y ni siquiera reenviarlos;
- el internauta no debe hacer en la web lo que no hace en la vida real, por estar perseguido por la ley (difamación, estafa, etc.);
- el internauta no debe sentirse más protegido de lo que lo está realmente;
- el internauta debe tener bien presente que tras cada actividad de Internet hay un individuo que, como en la vida ordinaria, no tiene por qué ser honrado.

IV.2.6.3 Pautas para asegurar un sistema de mensajería

A continuación se presentan pautas elementales que contribuirán a proteger un sistema de mensajería.

En el servidor:

- implantar un programa antivirus;
- filtrar los mensajes con arreglo a ciertos criterios parametrizables (tamaño, ficheros adjuntos, etc.);
- configurar correctamente el servidor;
- gestionarlo eficazmente para garantizar su disponibilidad;
- evitar las cuentas de mantenimiento por defecto;
- proteger físicamente el servidor.

Para el usuario:

- instalar, gestionar e imponer el empleo de programas antivirus;
- definir reglas de utilización de la mensajería (no abrir ficheros ejecutables, etc.);
- concienciar suficientemente a los usuarios sobre los riesgos afrontados;
- comprometer a los usuarios para que utilicen adecuadamente los recursos informáticos;
- configurar correctamente la estación de trabajo del usuario y su aplicación de mensajería;
- instalar versiones seguras de mensajería;
- utilizar procedimientos de encriptación para los mensajes confidenciales y autenticar sus remitentes.

---

60 Reproducción de la memoria de DEA en Derecho, Delincuencia y Seguridad de las nuevas tecnologías. «Sentiment de sécurité sur Internet» de Anne-Sophie Perron, dirigida por S. Ghernaouti-Hélie – Lausana 2005.

IV.2.6.4 Pautas para la protección de un entorno Internet-Intranet

A continuación se indican algunas pautas elementales que contribuirán a proteger un entorno Internet-Intranet mediante un sistema cortafuegos (*firewall*):

- el cortafuegos debe estar protegido y asegurado contra accesos no autorizados (concepto de sistema de confianza con un sistema operativo asegurado);
- todo el tráfico (tanto el entrante como el saliente) debe pasar por el cortafuegos;
- únicamente el tráfico definido por la política de seguridad como válido y autorizado puede atravesar el cortafuegos;
- debe configurarse el cortafuegos de modo tal que lo que no esté autorizado explícitamente quede prohibido;

el cortafuegos no puede ser también el servidor web de la entidad.

- si los datos de la red interna son muy sensibles, hay que acceder a internet a través de máquinas no conectadas a la red interna.
- el cortafuegos no puede proteger el entorno que se pretende asegurar contra ataques o accesos ilícitos que no pasen a través del mismo. Por otra parte, su eficacia es nula en lo que se refiere a los delitos perpetrados en el interior de la empresa.

El cortafuegos no es un antivirus, por tanto hay que protegerlo además contra las infecciones de los virus. Es imprescindible que los antivirus estén instalados en todos los sistemas que ofrezcan un servicio de conectividad (servidores de mensajería, servidores de comunicaciones, etc.) y en todas las máquinas que contengan datos (servidores de archivos, de bases de datos, etc.) así como en las estaciones de trabajo de los usuarios.

SECCIÓN V

ANEXOS

Anexo A – Glosario de los términos de seguridad más importantes[61]

Accidente (*accident*)

Elemento fortuito, imprevisible que afecta a una entidad.

Administrador de la seguridad (*security administrator*)

Persona responsable de la definición o implementación de toda la política de seguridad o de parte de ella.

Algoritmo criptográfico (*cryptographic algorithm*)

Algoritmo utilizado para la encriptación de datos confidenciales. Se basa en una función matemática y en una clave de encriptación.

Algoritmo de encriptación asimétrica (*asymmetric cryptographic algorithm*)

Algoritmo basado en la utilización de dos claves, de las que una sirve para encriptar los datos, sirviendo la otra para desencriptarlos.

Análisis de riesgos (*risk analysis*), ***evaluación de los riegos*** (*risk assessment*)

Proceso de identificación y evaluación de los riesgos (estimación de su probabilidad de ocurrencia y de su repercusión).

Análisis de tráfico (*traffic analysis*)

Observación y estudio de los flujos de información entre las entidades origen y destino (presencia, ausencia, volumen, dirección, frecuencia, etc.).

Anonimato (*anonymity*)

Característica de una entidad de nombre desconocido o que no facilita su nombre. Propiedad que permite a una entidad utilizar recursos sin identificarse (de incógnito). Debería poder respetarse la voluntad de ciertos usuarios que pueden tener un motivo justificado para no revelar su identidad cuando hacen declaraciones sobre Internet a fin de no restringir de manera excesiva su libertad de expresión, favorecer la expresión libre de las informaciones e ideas y garantizar la protección contra la vigilancia no autorizada en línea por parte de entidades públicas o privadas. Por contra, las instancias judiciales y policiales deberían tener la posibilidad de obtener información sobre las personas responsables de actividades ilícitas, dentro de los límites fijados por la legislación nacional, el Convenio Europeo de los Derechos del Hombre y demás tratados internacionales como el Convenio sobre Ciberdelincuencia.

Antivirus

Programa de detección de virus.

Ataque (a*ttack*)

Ofensiva, agresión o acción contra personas o bienes en perjuicio de los mismos. Existen diversos tipos de ataques informáticos.

---

[61] Reproducción del libro «Sécurité informatique et réseaux, cours et exercices corrigés»; de S. Ghernaouti-Hélie, Dunod 2006.

Ataque activo (*active attack*)

Ataque que modifica los recursos objeto del ataque (con perjuicio de los criterios de integridad, disponibilidad y confidencialidad).

Ataque pasivo (*passive attack*)

Ataque que no altera su objetivo (escucha pasiva o vulneración de la confidencialidad).

Vulneración (*breach*)

Efecto de degradación causado por una agresión o ataque que puede tener *repercusiones tangibles* (alteración física y material, perturbación del funcionamiento lógico, desorganización de los procedimientos ...); *repercusiones lógicas* (indisponibilidad, pérdida de integridad o pérdida de confidencialidad de la información); *repercusiones estratégicas* (principalmente en el aspecto financiero, gastos extraordinarios de alojamiento, de transporte, de telecomunicaciones, de intervención de expertos, de compra o alquiler de material y programas informáticos, de personal y de subcontratación, pérdidas de explotación (pérdidas de imagen, de tesorería o de clientela), de fondos o de bienes, etc.

Auditoría de seguridad (*security audit*)

Examen metódico de todos los componentes y protagonistas de la seguridad, política, medidas, soluciones, procedimientos y medios aplicados por una organización para asegurar su entorno, que se lleva a cabo con fines de control de conformidad, evaluación de la adecuación de los medios (organizativa, técnica, humana y financiera) invertidos en relación con los riesgos afrontados, de optimización, racionalidad y rendimiento.

Auditabilidad (*auditability*)

Propiedad de un entorno que permite el registro de las acciones y acontecimientos que ocurren a fin de dejar un rastro explotable con fines de análisis y de auditoría.

Auditor

Persona que realiza una auditoría.

Autenticidad (*authenticity*)

Carácter de lo que es auténtico. Capacidad que permite atestar y certificar la conformidad. A menudo se asocia al hecho de que una información, o un evento, no hayan sido alterados, modificados, falsificados y hayan sido producidos por la entidad que reivindica su autoría.

Autenticación (*authentication*)

Acción de autentificar. La autenticación sirve para confirmar (o no) que una acción, declaración, o información es auténtica (original y verdadera). Proceso aplicado principalmente para verificar la identidad de una entidad y garantizar que la identidad ofrecida corresponde a la identidad de dicha entidad previamente registrada.

Autorización (*authorization*)

Acción de autorizar, permitir y habilitar. Hecho de recibir el permiso de realizar ciertas acciones, de otorgar derechos, de obtener el derecho de acceso a un servicio, a informaciones, a un sistema, etc.

Autoridad (*authority*)

Órgano de poder. Suele hacer referencia a la entidad responsable de la emisión de certificados digitales.

Autoridad de certificación (CA, *Certification Authority*)

Tercero de confianza para la generación, firma y publicación de certificados de claves públicas.

Necesidad de seguridad (*security need*)

Para el entorno a proteger, identificación y expresión de los niveles de disponibilidad, integridad y confidencialidad asociados a los recursos y valores objeto de protección.

Activo, valor (*asset*)

Entidad que tiene un precio y representa, para el que la posee, un capital, patrimonio (concepto *activo sensible*). En materia de seguridad es importante determinar los valores y clasificarlos en función de su importancia a fin de adoptar las medidas de protección necesarias y suficientes con objeto de evitar su pérdida o por lo menos minimizar las repercusiones negativas consecuencia de su eventual pérdida.

Error (*bug*)

Se refiere a un error de programación. Por extensión defecto de concepción o de realización que se manifiesta en anomalías de funcionamiento (J. O. 19 de febrero de 1984).

Bomba lógica (*logical bomb*)

Programa malicioso que se activa con ocasión de determinados acontecimientos (fecha de cumpleaños, por ejemplo) para atacar al sistema en el que se encuentra.

Certificado (*certificate*), **certificado de clave pública** (*public-key certificate*)

Conjunto de datos emitidos por una autoridad de certificación (tercero de confianza) que permite realizar servicios de seguridad (confidencialidad, autenticación e integridad). El denominado certificado digital se refiere a la implementación de la encriptación con clave pública. Efectivamente, un certificado contiene, entre otros cosas, el valor de la clave pública de su propietario que se atestigua por el hecho de venir firmado por la autoridad de certificación emisora.

Cédula del usuario (*user charter*)

Documento establecido por una organización precisando los derechos, deberes y responsabilidades de sus empleados con respecto a la utilización de los recursos informáticos y de telecomunicaciones que pone a su disposición, y que firman las partes implicadas.

Troyano (*Troyan horse*)

Programa malicioso introducido subrepticiamente en los sistemas para tomar el control de los mismos (robar tiempo de procesador, alterar, modificar y destruir datos y programas, alterar el funcionamiento, efectuar escuchas ilícitas, etc.).

Encriptación y desencriptación (*encryption, decryption*)

La encriptación (*encipherment, encryption*) es una transformación criptográfica de los datos (*criptograma*) con objeto de garantizar su confidencialidad. Consiste en transformar los datos en algo incomprensible para todos los que no posean la clave de desencriptación. Un texto descodificado se encripta por medio de un algoritmo y una clave de encriptación, con objeto de obtener un texto encriptado que podrá desencriptarse por medio de la clave de desencriptación correspondiente (excepto en el caso de que la encriptación sea irreversible). La *desencriptación* (*decipherment, decryption*) es la operación inversa de la encriptación.

Clave (*key*)

Clave de encriptación o desencriptación, se trata generalmente de un valor matemático suministrado a un algoritmo de encriptación. Salvo que se trate de claves públicas, las claves de encriptación deben mantenerse secretas. De este modo, hay que proteger un secreto (la clave) que permite proteger otro secreto (la información encriptada para su confidencialidad).

Clave privada (*private key*)

Clave utilizada en los mecanismos de encriptación asimétrica (o encriptación con clave pública) que pertenece a una entidad y que debe ser secreta.

Clave pública (*public key*)

Generalmente, en criptografía asimétrica, una entidad debe facilitar su clave pública a los interlocutores que desean enviarle datos encriptados a fin de que pueda desencriptarlos con la correspondiente clave privada.

Clave de sesión (*session key*)

Clave secreta generada a través de un sistema de encriptación asimétrica por los corresponsales cuando establecen una sesión de trabajo, cuya vigencia está limitada a dicha sesión, y que sirve para encriptar grandes volúmenes de información con un algoritmo de encriptación asimétrica.

Código (*cipher*)

Algoritmo de encriptación que permite transformar un texto descodificado en un texto encriptado.

Condensado, resumen o compendio (*digest*)

Cadena de caracteres que resulta de la aplicación de una función de troceado a una serie de información.

Confianza (*trust*)

Seguridad del que se fía de alguien o de algo (criterio cualitativo, sugestivo y muy relativo).

Confidencialidad (*confidentiality*)

Mantenimiento del secreto de las informaciones y transacciones. Carácter de lo secreto. Objetivo de seguridad a alcanzar a fin de evitar la divulgación no autorizada de informaciones a terceros que debe permitir su protección frente a lecturas, escuchas y copias ilícitas de origen intencional o accidental durante su almacenamiento, tratamiento y transferencia (concepto de **confidencialidad de los datos** (*data confidentiality*)).

Conformidad (*compliance*)

Carácter de lo que es conforme está en concordancia o guarda parecido. Conformidad con ciertas normas.

Contramedida (*counter measure*)

Función, medida, procedimiento o mecanismo dedicado a la seguridad de un sistema a fin de reducir el nivel de vulnerabilidad del mismo y contrarrestar una amenaza antes de que ésta se convierta en acción maliciosa.

Control de acceso (*access control*)

Mecanismo que permite evitar la utilización inapropiada o no autorizada de un recurso (servicios, sistemas, datos y programas).

Chivatos (*cookies*)

Ficheros enviados a la estación de trabajo de los internautas sin su conocimiento cuando acceden a determinados sitios web, que recogen informaciones que les afectan, en principio para la personalización de los servicios web ofrecidos.

Parche de seguridad (*patch*)

Actualización de seguridad de un soporte lógico para eliminar una vulnerabilidad identificada tras su instalación.

Criptoanálisis (*cryptanalysis*)

El criptoanálisis comprende el conjunto de medios que permite analizar una información previamente encriptada, a fin de desencriptarla. Cuanto más robusto es un sistema de encriptación más difícil resulta el criptoanálisis del mismo.

Criptograma (*cryptogram, cyphertext*)

Datos sometidos a una transformación criptográfica, datos encriptados y texto o mensajes encriptados. Datos obtenidos por encriptación.

Criptografía (*cryptography*)

Aplicación de las matemáticas que permite escribir la información de manera que resulte ininteligible para los que no poseen la capacidad de desencriptarla. Ver *Encriptación*.

Criptografía con clave pública (*public key cryptography*)

Sistema de encriptación asimétrica que utiliza un par de claves denominado *clave doble*, compuesto de una clave privada secreta y de una clave pública y publicable. Estas dos claves son complementarias e indisociables. La relación matemática que las vincula no permite recuperar la clave secreta a partir de la pública.

Periodo criptográfico (*cryptographic period*)

Periodo de tiempo durante el que las claves de un sistema permanecen inalteradas.

DDoS (*Distributed Denial of Service*)

Ataque por saturación (o denegación de servicio) efectuado simultáneamente desde varios sistemas.

Denegación de servicio (DoS, *Denial of Service*)

Ataque por saturación de una entidad a fin de inutilizarla y de impedirle prestar los servicios que se esperan de ella.

Disponibilidad (*availability*)

Criterio de seguridad que permite que los recursos sean accesibles y utilizables con arreglo a las necesidades (sin rechazos de acceso autorizado a los sistemas, servicios, datos e infraestructuras, etc.).

Disuasión (*dissuasion*)

Medida destinada a persuadir por intimidación a un malhechor a que renuncie a efectuar un ataque o a persuadirle de que el valor del objetivo codiciado es inferior al del perjuicio que el sistema amenazado puede infringirle.

Eficacia (*efficiency*)

Carácter de lo que produce el efecto esperado y resultados útiles. Propiedad de las medidas de seguridad que garantiza su pertinencia y su capacidad de proteger perfectamente un recurso.

Huella digital (*digest*) – Ver *Función de troceo*

Ética (*ethics*)

Lo que concierne a los principios de la moral. Conjunto de reglas morales adoptadas por una comunidad.

Fiabilidad (*reliabiliy*)

Capacidad de un sistema para funcionar sin incidentes durante un tiempo determinado.

Envío de improperios (*flaming***)**

Técnica que consiste en enviar un gran número de mensajes improcedentes (*flames*) con objeto de menoscabar la credibilidad de un grupo de debate.

Inundación (*flooding*)

Tipo de medio de intrusión en los sistemas basado en la vulneración de las contraseñas de los usuarios.

Inundador (*flooder*)

Programa malicioso para ralentizar las comunicaciones entre un proveedor de acceso y un internauta o para desconectar a este último.

Función de troceo (*hash function*)

En el contexto de la encriptación, esta función se denomina también función *compendio*. Permite generar, a partir de los datos de entrada que se le suministran, su resumen (especie de huella digital (*compendio*)), más corta que el mensaje original e incomprensible. Este resumen puede encriptarse seguidamente con la clave privada del emisor y asociarse al mensaje a transmitir. A la recepción del mensaje y de su huella, el destinatario desencripta esta última con la clave pública del emisor y a continuación recalcula la huella a partir del mensaje recibido con la misma función *troceo*, y la compara con la recibida. De ser idéntico el resultado, el destinatario da por verificada la identidad del emisor y por garantizada la integridad del mensaje. Efectivamente, si el mensaje ha sido alterado, aunque sea levemente, su huella habrá quedado considerablemente modificada.

Función de troceo unidireccional (*one-way hash function*)

Función que permite calcular la huella de los datos, pero no generar datos con una huella particular. Esta función no debe producir colisiones, es decir, una misma huella no debe poder ser generada a partir de mensajes diferentes.

Gravedad de la repercusión (*impact gravity*)

Apreciación del nivel de gravedad de un incidente, ponderado por su frecuencia de aparición. Es importante poder cuantificar este criterio de repercusión a fin de identificar en la medida de lo posible los imperativos de seguridad y el grado de urgencia de la respuesta a estos imperativos (ejemplo de cuantificación: repercusión de gravedad insignificante: (0) sin gravedad, (1) poco grave, (3) muy grave, (4) extremadamente grave).

Pirateo/pirata informático (*hack, hacker*)

Acción consistente en introducirse ilícitamente en un sistema. Persona que, con independencia de sus motivos, penetra sin autorización e ilegalmente en un sistema que pertenece a un tercero.

Intrusión indebida (*hacking*)

Conjunto de operaciones que permite la intrusión en un sistema informático.

Identificación (*identification*)

Proceso que permite reconocer una entidad previamente identificada.

Identidad (*identity*)

Información que permite designar y distinguir de manera única y sin ambigüedad, cuando es posible, una entidad en el interior de un dominio de nombres.

Repercusión (*impact*)

Expresa el nivel de las consecuencias producidas por un ataque: **repercusión financiera** (*financial impact*), coste del ataque; **repercusión lógica** (*logical impact*) al ataque a los criterios de disponibilidad, integridad y confidencialidad, **repercusión estratégica** (*strategical impact*) perjudicial para la supervivencia de una organización; **repercusión tangible** (*tangible impact*) ataque directamente constatable y real.

Imputabilidad (*imputability*)

Propiedad que permite imputar con certeza una operación a un usuario en un momento determinado. Hecho de poder identificar a un responsable en caso de violación del reglamento.

Infraestructura de gestión de claves (IGC o PKI, *Public Key Infrastructure*)

Infraestructura de soporte para la realización e implementación de la encriptación asimétrica (con clave pública) que ofrece, entre otros, servicios de gestión y distribución de claves de encriptación y de certificados digitales.

Infraestructura de gestión de privilegios (PMI, *privilege management infrastructure*)

Infraestructura capaz de soportar la gestión de los privilegios, permisos o habilitaciones.

Ingeniería social (*social engeneering*)

Técnicas, procedimientos y medios utilizados por los malhechores aprovechándose frecuentemente de la credulidad de los usuarios para conseguir, entre otros, sus contraseñas y parámetros de conexión y usurpar su identidad digital a fin de burlar los sistemas y penetrar en los mismos haciéndose pasar por las personas habilitadas.

Inocuidad (*safety*)

Cualidad de lo que no es nocivo.

Integridad (*integrity*)

Estado de algo que permanece intacto. Criterio de seguridad que, llevado a la práctica, permite garantizar que un recurso no ha sido alterado (modificado ni destruido) sin autorización.

Intranet (*Intranet*)

Red interna, red privada de una entidad, que utiliza las tecnologías de Internet y suele estar aislada de ésta por sistemas *cortafuegos*.

IPSec (*Internet Protocol Security*)

Versión del protocolo IP que ofrece servicios de seguridad. IPSec permite crear un canal lógico de comunicación (tunnel IP), a través de la Internet pública, entre dos corresponsales. Las extremidades del túnel se autentican y los datos que circulan por el mismo pueden encriptarse (concepto de canal encriptado o de red virtual).

IPv6 (*Internet Protocole version 6*)

Evolución de la versión 4 del protocolo IP que, entre otros, integra en modo nativo mecanismos que permiten prestar servicios de seguridad (autenticación de las entidades origen y destino y confidencialidad de los datos transmitidos).

Programa espía *(spyware)*

Programa que envía a un malhechor informaciones sensibles desde el ordenador comprometido.

Programa malicioso *(malware)*

Término genérico que designa a un programa del tipo virus, gusano, troyano, etc. o cualquier otra forma de programa informático atacante que actúe con mayor o menor grado de autonomía.

Dolo (*malevolence*)

Comportamiento de carácter hostil que se traduce en ataques a los recursos de una organización que pueden ser cometidos directa o indirectamente por personas del interior o del exterior (hurto de materiales, de datos, divulgación de informaciones confidenciales, intrusiones ilícitas, etc.).

Gestión de claves (*key management*)

Gestión de las claves de encriptación, generación, distribución, archivo y destrucción de las claves en función de la política de seguridad.

Gestión del riesgo (*risk management*)

Proceso continuo de evaluación de los riesgos afrontados por una organización a fin de controlarlos, y reducirlos a un nivel aceptable. Permite determinar la política de seguridad más apropiada para la protección de los valores de la organización.

Enmascaramiento (*masquerade*)

Tipo de ataque que se basa en la burla de los sistemas.

Amenaza (*threat*)

Signo o indicio que anuncia un peligro. Acción o evento susceptible de producirse, transformarse en agresión contra un entorno o unos recursos y actuar en detrimento de su seguridad.

Medidas de seguridad (*security measures*)

Conjunto de medios tecnológicos, organizativos, jurídicos, financieros, humanos y procedimentales, y de las acciones que permiten alcanzar los objetivos de seguridad fijados por la política de seguridad. Las medidas suelen clasificarse con arreglo a su función (por ejemplo: medidas preventivas, de protección, de disuasión, etc.).

Contraseña (*password*)

Información confidencial que debe exhibir un derechohabiente con el fin de demostrar su identidad en un procedimiento de autenticación en el marco de una demanda de acceso a un recurso.

No rechazo (*non-repudiation*)

Capacidad de prevenir el hecho de que un remitente desmienta posteriormente haber enviado un mensaje o efectuado una acción. Garantiza la disponibilidad de pruebas que pueden presentarse a un tercero y utilizarse para demostrar que tal tipo de evento o de acción ha tenido lugar. Prueba que un mensaje ha sido enviado por una persona determinada en un momento preciso, sin haberse modificado después de su envío. Esta prueba debería poder verificarse en todo momento por un tercero. Sin el no rechazo, los emisores y receptores de informaciones podrían negar su recepción o envío.

Sin opción (*no-opt*)

Servicio en el que los clientes no tienen la posibilidad de elegir el modo de utilización de la información que le afecta (posibilidad de ataque a la protección de datos privados).

Notarización (*notarization*)

Registro de los datos con fines de prueba.

Avería (*failure*)

Disfunción o interrupción del funcionamiento que comporta la indisponibilidad de un recurso.

Cortafuegos (*firewall*)

Dispositivo físico o lógico que permite aislar y enmascarar recursos, filtrar datos y controlar flujos, contribuyendo a la protección del entorno informático privado de una entidad conectada a Internet.

Pérdida de servicio esencial (*lost of essential services*)

Indisponibilidad o perturbación total o parcial del funcionamiento de los recursos necesarios para la buena marcha de un sistema o de una entidad.

Pérdidas directas (*direct losses*)

Pérdidas identificables directamente consecuencia de un fallo de seguridad.

Pérdidas indirectas (*indirect losses*)

Pérdidas generadas indirectamente por un fallo de seguridad.

Piratería de telecomunicaciones (*phreak*)

Utilización ilegal o maliciosa de los servicios de telecomunicaciones por parte de un pirata de las telecomunicaciones (*phreaker*) (concepto de piratería de telecomunicaciones (*phreaking*)) en perjuicio de un individuo u operador.

Pirata, malhechor o atacante

Persona que se introduce ilegalmente en los sistemas con la intención de realizar ataques pasivos o activos

Plan de gestión de crisis (*emergency plan*)

Conjunto de medios técnicos y organizativos previstos para ofrecer una respuesta óptima a un incidente grave que afecte a la buena marcha de las operaciones y sea perjudicial para la entidad.

Plan de socorro (*backup plan*)

Conjunto de medios técnicos y organizativos previstos para garantizar la perdurabilidad de la información y la continuidad de las actividades con independencia de la naturaleza de los problemas encontrados.

Política de seguridad (*security policy*)

Referencial de seguridad establecido por una entidad, que recoge su estrategia de seguridad y especifica los medios para llevarla a la práctica.

Puerta falsa (*backdoor, trap door*)

Se suele referir normalmente a una sección de código integrada en los programas informáticos, que permite a entidades no autorizadas controlar los sistemas, copiar información, etc. sin el conocimiento de su propietario.

Prevención (*prevention*)

Conjunto de medidas adoptadas para prevenir un peligro o riesgo, con ánimo de impedir la materialización de amenazas y reducir la frecuencia de los incidentes desde el punto de vista de la protección.

Perfil de usuario (*user profile*)

Relación de atributos sobre un usuario que contribuyen a gestionar la red y los sistemas al que se conecta (parámetros de identificación, de autenticación, derechos de acceso, permisos y demás informaciones útiles, a fin de controlar el acceso, la facturación, etc.).

Protección (*protection*)

Acción y efecto de proteger. Se dice de la medida de seguridad que contribuye a detectar, neutralizar o disminuir los efectos de una agresión.

Protección de datos privados y de la intimidad digital (*privacy protection*)

Medidas de protección que permiten garantizar que las informaciones y las actividades de los internautas no sean conocidas por terceros distintos de los previstos y no se utilicen con fines contrarios a los consentidos por su propietario. Esto se refiere al derecho de los individuos a controlar las informaciones que les afectan y que pueden capturarse directamente o indirectamente por observación del comportamiento de su navegación y de los sitios visitados.

Rechazo (*repudiation*)

Hecho de negar la participación en intercambios, totalmente o en parte.

Red privada virtual (RPV o VPN, *Virtual Private Network*)

El concepto de red privada virtual se refiere a la utilización del protocolo IPSec a fin de crear un canal de comunicación seguro de uso privado a través de una red pública no segura. Suelen implementarlo las entidades para conectar sus diversos sitios a través de Internet manteniendo la confidencialidad de los datos intercambiados.

Revocación (*revocation*)

Notificación de la pérdida de integridad de una clave privada. El certificado de la clave pública correspondiente ya no debe utilizarse.

Riesgo (*risk*)

Peligro más o menos probable que proviene de una amenaza y puede traducirse en términos de probabilidad de aparición y de nivel de repercusión.

RSSI (Responsable de la Seguridad del Sistema de Información)

Persona encargada de la seguridad de los sistemas de información.

Sabotaje

Acción maliciosa, vandalismo o deterioro deliberado con objeto de impedir el funcionamiento normal de una entidad, infraestructura, servicio o recurso, que puede provocar un siniestro.

Seguridad (*security*)

Situación en la que alguien o algo queda libre de todo peligro. Mecanismo destinado a prevenir un evento pernicioso o a limitar sus efectos. Por ejemplo, la **seguridad física** (*physical security*) se refiere a las medidas que permiten ofrecer una protección física y material del entorno, mientras que la **seguridad lógica** (*logical security*) se refiere a los procedimientos y medios lógicos de protección.

Sensibilidad (*sensitivity*)

Característica de una entidad que indica su valor o importancia.

S-http

Versión segura del protocolo http que permite efectuar intercambios seguros entre un cliente y un servidor web.

Firma digital (*digital signature*)

Por analogía a la firma manual, la digital, obtenida por un algoritmo de encriptación asimétrica, permite autenticar al emisor de un mensaje y verificar su integridad.

Husmeador (*sniffer*)

Programa informático que sirve para efectuar escuchas pasivas de los datos que circulan por una red.

Escucha pasiva (*sniffing*)

Acción consistente en efectuar escuchas pasivas para recuperar los parámetros de conexión con intención de utilizarlos después sin el conocimiento de sus propietarios legítimos y efectuar intrusiones no autorizadas.

Spammer

Persona que realiza el envío de correo indeseado (*spam*).

Envío de correo indeseado (*spamming*)

Técnica que consiste en el envío de mensajes indeseados por correo electrónico.

Falsificador de direcciones (*spoofer*)

Persona que practica la falsificación de direcciones.

Falsificación de direcciones (*spoofing*)

Usurpación de direcciones IP con fines de intrusión.

SSL (*Secure Sockets Layer*)

Software que garantiza la seguridad de los intercambios por Internet, desarrollado por Netscape y soportado por la mayor parte de los navegadores web del mercado.

Estenografía (*steganography*)

Técnica que permite camuflar una información en otra con objeto de transmitirla o almacenarla clandestinamente. El marcado de un documento y la filigrana *(watermarking)* son aplicaciones de la estenografía que consisten en marcar una imagen de modo indeleble.

Sistema de detección de intrusión (IDS, *intrusion detection system*)

Sistema que permite detectar incidentes que pueden resultar en violaciones de la política de seguridad y que permite diagnosticar intrusiones potenciales.

Prueba de penetración (*penetration test*)

Pruebas practicadas para analizar y comprobar el grado de protección de los sistemas y la robustez de los mecanismos de seguridad.

Virus

Programa malicioso introducido en un sistema sin el conocimiento de sus usuarios. Posee la capacidad de duplicarse (ya sea de modo idéntico, ya modificándose (virus polimorfo)), de atacar al entorno en el que se ejecuta y de contaminar a los demás usuarios con los que se relaciona. Se distinguen diversos tipos de virus en función de su signatura, de su comportamiento, de su tipo de reproducción, de la infección, de las disfunciones inducidas, etc. Los **gusanos, troyanos y bombas lógicas** son códigos maliciosos de la familia genérica de los virus.

Vulnerabilidad (*vulnerability*)

Fallo de seguridad que puede traducirse, intencional o accidentalmente, en una violación de la política de seguridad.

Anexo B – Capítulos de la norma ISO/CEI 17799:2005 que constituye un documento de referencia en materia de gestión de la seguridad

Introducción
- 0.1 ¿Qué es la seguridad de la información?
- 0.2 ¿Por qué es necesaria la seguridad de la información?
- 0.3 ¿Cómo establecer las necesidades de seguridad?
- 0.4 Evaluación de los riesgos de seguridad
- 0.5 Selección de los controles
- 0.6 Punto de partida en seguridad de la información
- 0.7 Factores críticos de éxito X
- 0.8 Desarrollo de sus propias directrices

1 Alcance

2 Terminología y definiciones

3 Estructura de la presente norma
- 3.1 Cláusulas
- 3.2 Principales categorías de seguridad

4 Evaluación de los riesgos y tratamientos
- 4.1 Evaluación de los riesgos de seguridad
- 4.2 Tratamiento de los riesgos de seguridad

5 Política de seguridad
- 5.1 Política de seguridad de la información
  - 5.1.1 Documento de política de seguridad de la información
  - 5.1.2 Examen de la política de seguridad de la información

6 Organización de la seguridad de la información
- 6.1 Organización interna
  - 6.1.1 Implicación de la dirección en la seguridad de la información
  - 6.1.2 Coordinación de la seguridad de la información
  - 6.1.3 Asignación de responsabilidades para la seguridad de la información
  - 6.1.4 Proceso de autorización para los equipos de tratamiento de la información
  - 6.1.5 Acuerdos de confidencialidad
  - 6.1.6 Contacto con las autoridades
  - 6.1.7 Contacto con grupos de interés específico
  - 6.1.8 Examen independiente de la seguridad de la información
- 6.2 Partes externas
  - 6.2.1 Identificación de los riesgos vinculados a las partes externas
  - 6.2.2 La seguridad en las transacciones con los clientes
  - 6.2.3 La seguridad en los acuerdos con terceros

7 Gestión de activos y valores
- 7.1 Responsabilidad de los valores
  - 7.1.1 Inventario de valores
  - 7.1.2 Propiedad de los valores
  - 7.1.3 Utilización aceptable de los valores
- 7.2 Clasificación de la información
  - 7.2.1 Directivas de clasificación
  - 7.2.2 Marcado (etiquetado) y manipulación de la información

8 Seguridad de los recursos humanos
- 8.1 Antes de empezar
  - 8.1.1 Funciones y responsabilidades
  - 8.1.2 Análisis
  - 8.1.3 Modalidades y condiciones de contratación
- 8.2 Durante la misma
  - 8.2.1 Responsabilidades de la dirección
  - 8.2.2 Concienciación, sensibilización, educación y formación en la seguridad de la información
  - 8.2.3 Medidas disciplinarias
- 8.3 Suspensión o modificación de la misma
  - 8.3.1 Responsabilidades de la suspensión
  - 8.3.2 Restitución de valores
  - 8.3.3 Supresión de los derechos de acceso

9 Seguridad física y del entorno
- 9.1 Zonas de seguridad
  - 9.1.1 Perímetro de seguridad
  - 9.1.2 Controles de acceso físico
  - 9.1.3 Asegurar las oficinas, salas y equipos
  - 9.1.4 Protección contra las amenazas externas y del entorno
  - 9.1.5 Trabajar en zonas seguras
  - 9.1.6 Sectores de acceso público de entrega y carga
- 9.2 Seguridad de los equipos
  - 9.2.1 Situación y protección de los equipos
  - 9.2.2 Soporte de las utilidades
  - 9.2.3 Seguridad del cableado
  - 9.2.4 Mantenimiento de los equipos
  - 9.2.5 Seguridad de los equipos fuera de los límites de la organización
  - 9.2.6 Seguridad de los equipos abandonados o reutilizados
  - 9.2.7 Eliminación de los equipos

10 Gestión de las comunicaciones y de las operaciones
- 10.1 Procedimientos operacionales y responsabilidades
  - 10.1.1 Modos operatorios documentados
  - 10.1.2 Gestión del cambio
  - 10.1.3 Segregación de las funciones
  - 10.1.4 Separación de las facilidades vinculadas al desarrollo, a las pruebas y a las operaciones
- 10.2 Gestión de la entrega de servicios ofrecidos por terceros
  - 10.2.1 Entrega de servicios
  - 10.2.2 Vigilancia y control de los servicios prestados por terceros
  - 10.2.3 Gestión de los cambios en los servicios ofrecidos por terceros
- 10.3 Planificación y aceptación de los sistemas
  - 10.3.1 Gestión de la capacidad
  - 10.3.2 Tolerancia de los sistemas
- 10.4 Protección contra los códigos maliciosos y móviles
  - 10.4.1 Controles contra los códigos maliciosos
  - 10.4.2 Controles contra los códigos móviles

- 10.5 Copia de seguridad/respaldo
  - 10.5.1 Copia de seguridad de la información
- 10.6 Gestión de la seguridad de las redes
  - 10.6.1 Control de la red
  - 10.6.2 Seguridad de los servicios de red
- 10.7 Manipulación de los soportes
  - 10.7.1 Gestión de los soportes amovibles
  - 10.7.2 Destrucción de los soportes
  - 10.7.3 Procedimientos de manipulación de los datos
  - 10.7.4 Seguridad de la documentación de los sistemas
- 10.8 Intercambio de las informaciones
  - 10.8.1 Políticas y procedimientos de intercambio de información
  - 10.8.2 Acuerdos de intercambio
  - 10.8.3 Soportes físicos en tránsito
  - 10.8.4 Mensajería electrónica
  - 10.8.5 Sistemas de información
- 10.9 Servicios de comercio electrónico
  - 10.9.1 Comercio electrónico
  - 10.9.2 Transacciones en línea
  - 10.9.3 Información accesible al público
- 10.10 Vigilancia
  - 10.10.1 Auditoría de los diarios y registros históricos (*logs*)
  - 10.10.2 Vigilancia de la utilización del sistema
  - 10.10.3 Protección de las informaciones registradas por diario
  - 10.10.4 Diarios de los administradores y operadores
  - 10.10.5 Registro por diario de los errores e incidentes
  - 10.10.6 Sincronización de los relojes

- 11 Control de acceso
  - 11.1 Imperativos de la organización (necesidades del negocio) en materia de control de acceso
    - 11.1.1 Política de control de acceso
  - 11.2 Gestión de los accesos de los usuarios
    - 11.2.1 Registro de los usuarios
    - 11.2.2 Gestión de privilegios
    - 11.2.3 Gestión de las contraseñas de los usuarios
    - 11.2.4 Examen de los derechos de acceso de los usuarios
  - 11.3 Responsabilidades de los usuarios
    - 11.3.1 Utilización de contraseñas
    - 11.3.2 Equipos de los usuarios sin vigilancia
    - 11.3.3 Política de recogida y limpieza de despachos y pantallas
  - 11.4 Control de acceso a la red
    - 11.4.1 Política de utilización de los servicios de red
    - 11.4.2 Autenticación de los usuarios para las conexiones externas
    - 11.4.3 Identificación de los equipos en las redes
    - 11.4.4 Protección de los puertos de telediagnóstico y de teleconfiguración
    - 11.4.5 Segmentación de las redes
    - 11.4.6 Control de la conexión de red
    - 11.4.7 Control del encaminamiento de la red

- 11.5 Control de acceso al sistema operativo
  - 11.5.1 Procedimientos de conexión seguros
  - 11.5.2 Identificación y autenticación de los usuarios
  - 11.5.3 Sistema de gestión de contraseñas
  - 11.5.4 Empleo de las utilidades del sistema
  - 11.5.5 Tiempo de desconexión de la sesión (*time-out*)
  - 11.5.6 Limitación del tiempo de conexión
- 11.6 Control de acceso a las aplicaciones y a las informaciones
  - 11.6.1 Restricción del acceso a las informaciones
  - 11.6.2 Aislamiento de los sistemas sensibles
- 11.7 Movilidad en informática y teletrabajo
  - 11.7.1 Movilidad y comunicaciones
  - 11.7.2 Teletrabajo

12 Adquisición, desarrollo y mantenimiento de los sistemas de información
- 12.1 Necesidades de seguridad de los sistemas de información
  - 12.1.1 Análisis y especificación de las necesidades de seguridad
- 12.2 Exactitud de la ejecución de las aplicaciones
  - 12.2.1 Validación de los datos capturados
  - 12.2.2 Control del tratamiento interno
  - 12.2.3 Integridad de los mensajes
  - 12.2.4 Validación de los resultados
- 12.3 Control de la encriptación
  - 12.3.1 Política de control del empleo de la encriptación
  - 12.3.2 Gestión de claves
- 12.4 Seguridad de los ficheros del sistema
  - 12.4.1 Control de los programas informáticos operacionales
  - 12.4.2 Protección de los datos de prueba del sistema
  - 12.4.3 Control de acceso al código fuente de los programas
- 12.5 Seguridad en el desarrollo y soporte de los procesos
  - 12.5.1 Procedimientos de control de cambio
  - 12.5.2 Examen técnico de las aplicaciones tras la modificación del sistema operativo
  - 12.5.3 Restricciones de los cambios en los paquetes de programas informáticos
  - 12.5.4 Fugas de información
  - 12.5.5 Desarrollo externo de los programas informáticos
- 12.6 Gestión de las vulnerabilidades técnicas
  - 12.6.1 Control de las vulnerabilidades técnicas

13 Gestión de los incidentes de seguridad de la información
- 13.1 Notificación de los eventos y de las debilidades de seguridad de la información
  - 13.1.1 Notificación de los eventos de seguridad de la información
  - 13.1.2 Notificación de las debilidades de seguridad
- 13.2 Gestión de los incidentes y mejoras de la seguridad de la información
  - 13.2.1 Responsabilidades y procedimientos
  - 13.2.2 Experiencias a obtener de los incidentes de seguridad
  - 13.2.3 Recogida de pruebas

14 Gestión de la continuidad del negocio
- 14.1 Aspectos de seguridad de la gestión de la continuidad del negocio
  - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
  - 14.1.2 Continuidad del negocio y evolución de los riegos
  - 14.1.3 Desarrollo e implementación de planes de continuidad que integran la seguridad de la información
  - 14.1.4 Cuadro de planificación de la continuidad de las actividades
  - 14.1.5 Prueba, mantenimiento y revaluación de los planes de continuidad

15 Conformidad
- 15.1 Conformidad con las exigencias legales
  - 15.1.1 Identificación de la legislación aplicable
  - 15.1.2 Derechos de la propiedad intelectual
  - 15.1.3 Protección de los registros de la organización
  - 15.1.4 Protección de los datos e intimidad digital
  - 15.1.5 Prevención de uso indebido de las facilidades de tratamiento de la información
  - 15.1.6 Reglamentación de los controles de encriptación
- 15.2 Conformidad con las normas y políticas de seguridad y conformidad técnica
  - 15.2.1 Conformidad con las políticas y las normas de seguridad
  - 15.2.2 Control de la conformidad técnica
- 15.3 Consideraciones sobre la auditoría de los sistemas de información
  - 15.3.1 Control de auditoría de los sistemas de información
  - 15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Bibliografía e Índice

Anexo C – Mandato y actividades del UIT-D en materia de ciberseguridad

Para más información:
www.itu.int/ITU-D/cybersecurity

Las fuertes sinergias entre las prioridades y acciones que hay en este Programa de ciberseguridad y lucha contra el correo indeseado y el Plan de Acción de la CMSI de Ginebra y el Programa de Acciones de Túnez se destacan en el cuadro de correspondencia, prácticamente biunívoca, que se muestra a continuación. En el Programa de Acciones de Túnez de 2005 se identificó la UIT como organización rectora para facilitar y moderar las acciones destinadas a aplicar el Plan de Acción de Ginebra en el dominio de creación de confianza y seguridad en la utilización de las TIC. En el Plan de Acción de Doha, adoptado en la Conferencia Mundial de Desarrollo de Telecomunicaciones de la UIT en marzo de 2006, los miembros de la UIT decidieron que la ciberseguridad y la lucha contra el correo indeseado eran de la máxima prioridad para el Programa 3.

Línea de Acción C.5 de la CMSI (Creación de confianza y seguridad en la utilización de las TIC) y Mandato de la UIT en materia de ciberseguridad y lucha contra el correo indeseado

Línea de Acción C.5 de la CMSI	Mandato de la UIT en relación con C.5
12 La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información.	Examinar las cuestiones de ciberseguridad a fin de aprovechar el potencial de las redes para la prestación de aplicaciones de ciberservicios seguras y accesibles.
a) Propiciar la cooperación entre los gobiernos dentro de las Naciones Unidas, y con todas las partes interesadas en otros foros apropiados, para aumentar la confianza del usuario y proteger los datos y la integridad de la red; considerar los riesgos actuales y potenciales para las TIC, y abordar otras cuestiones de seguridad de la información y de las redes.	Minimizar, impedir y detectar las ciberamenazas, es asimismo necesario aumentar la sensibilización y la cooperación para recopilar y difundir información relacionada con la ciberseguridad e intercambiar buenas prácticas para mejorar la asistencia, la respuesta y la recuperación mutuas y eficaces entre los miembros y entre gobiernos, empresas y sociedad civil.
b) Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel internacional para la prevención, detección y recuperación de estos incidentes; y alentando la educación y la sensibilización.	Elaborar directrices, instrumentos de planificación y manuales sobre los aspectos tecnológicos y políticos de la ciberseguridad. Elaborar herramientas informáticas de ciberseguridad, para los encargados de formular políticas y demás sectores pertinentes. Ofrecer ayuda a los Estados Miembros para el diseño de leyes y de una legislación modelo para la prevención de la ciberdelincuencia. Desarrollar material de formación sobre estrategias tecnológicas y evolución tecnológica para la implementación de la ciberseguridad.

Línea de Acción C.5 de la CMSI		Mandato de la UIT en relación con C.5
c)	Los gobiernos y otras partes interesadas deben fomentar activamente la educación y la sensibilización de los usuarios sobre la privacidad en línea y los medios de protección de la privacidad.	Contribuir a hacer más patente e identificar cuestiones clave en apoyo de una cultura de ciberseguridad, así como recomendar modelos de buenas prácticas en apoyo de las aplicaciones TIC y para la minimización de las ciberamenazas.
d)	Tomar medidas apropiadas contra el envío masivo de mensajes electrónicos no solicitados («*spam*») a nivel nacional e internacional.	Desarrollar una comprensión común de las cuestiones del correo indeseado y de las ciberamenazas, con especial énfasis en las contramedidas. Tener en cuenta, en su caso, el trabajo de otras partes interesadas: la OCDE y los signatarios de acuerdos clave sobre ciberseguridad y correo indeseado.
e)	Alentar una evaluación interna de la legislación nacional con miras a superar cualquier obstáculo al uso efectivo de documentos y transacciones electrónicas, incluido los medios electrónicos de autenticación.	Organizar cursillos, reuniones y seminarios para abordar los aspectos técnicos y jurídicos, de orden estratégico y político, sobre ciberseguridad. Ofrecer ayuda a los Estados Miembros para que desarrollen leyes y legislación modelo para la prevención de la ciberdelincuencia.
f)	Seguir fortaleciendo el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y de los consumidores.	Identificar las necesidades de la ciberseguridad y proponer soluciones para el desarrollo de aplicaciones TIC seguras. Contribuir a la toma de conciencia e identificación de cuestiones clave en apoyo de una cultura de ciberseguridad, así como recomendar modelos de buenas prácticas en apoyo de las aplicaciones TIC y minimización de las ciberamenazas.
g)	Compartir prácticas óptimas en el ámbito de la seguridad de la información y la seguridad de las redes, y propiciar su utilización por todas las partes interesadas.	Desarrollar herramientas que faciliten la compartición de información sobre cuestiones tecnológicas y políticas, así como sobre las mejores prácticas sobre ciberseguridad. Actuar como facilitador para la cooperación regional e interregional, dando apoyo a las actividades adecuadas de creación de capacidades a nivel regional.

Línea de Acción C.5 de la CMSI	Mandato de la UIT en relación con C.5
h) Invitar a los países interesados a establecer puntos de contacto para intervenir y resolver incidentes en tiempo real, y desarrollar una red cooperativa entre estos puntos de contacto de forma que se comparta información y tecnologías para intervenir en caso de estos incidentes.	Entre las acciones se podría considerar, el desarrollo de MoU entre los Estados Miembros interesados para mejorar la ciberseguridad. Poner en marcha un proyecto mundial de múltiples partes interesadas [...] que ofrezca soluciones en varios dominios, entre ellos: 1) La creación de puntos focales nacionales. 2) Respuestas a los incidentes, vigilancia y alerta sobre los mismos. Examinar las prácticas óptimas para el establecimiento y explotación de capacidades de respuesta a los incidentes, vigilancia y alerta, así como de recuperación, que puedan usadas por los Estados Miembros para establecer sus propias capacidades nacionales.
i) Alentar el desarrollo de nuevas aplicaciones seguras y fiables que faciliten las transacciones en línea.	Identificar las necesidades de ciberseguridad y plantear soluciones para el desarrollo de aplicaciones TIC seguras.
j) Alentar a los países interesados a que contribuyan activamente en las actividades en curso de las Naciones Unidas tendentes a crear confianza y seguridad en la utilización de las TIC.	Invita a los Estados Miembros de la UIT, a los Miembros de los Sectores y Asociados a: – A contribuir a esta tarea en la Comisión de Estudio 1 del UIT-D y a participar a las actividades en curso de los proyectos de la BDT. – A contribuir a crear confianza y seguridad en la utilización de las TIC en los ámbitos nacional, regional e internacional llevando a cabo las actividades descritas en el párrafo 12[1] del Plan de Acción de Ginebra.

[1] El párrafo 12 contiene el texto completo de la Línea de Acción C.5 de la CMSI, que aparece en la columna 1 del presente documento.

Mandato del UIT-D en materia de ciberseguridad y de lucha contra el correo indeseado

En el marco de las decisiones adoptadas por los miembros de la UIT en las Conferencias de Plenipotenciarios de la UIT de 2002 y 2006 (PP02 y PP06) y en las Conferencias Mundiales de Desarrollo de las Telecomunicaciones de 2002 y 2006 (CMDT-02 y CMDT-06), se incluye el mandato del UIT-D para la ciberseguridad, las ciberamenazas y la lucha contra el correo indeseado, en la siguientes decisiones:

1) Programa 3 de la CMDT-2002 y 2006 – Ciberestrategias y aplicaciones TIC.
2) Resolución 45 de la CMDT-2006 – Mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo indeseado.
3) Anexo 2 de la Resolución 2 de la CMDT-2006 – Comisión de Estudio 1 del UIT-D, Cuestión 22 – Garantía de seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad.
4) Resolución 130 (Revisada en Antalya 2006) – Refuerzo del papel de la UIT en la creación de confianza y seguridad en el empleo de las tecnologías de la información y las comunicaciones.

1 Programa 3 del Plan de Acción de Doha, CMDT-06 (Ciberestrategias y aplicaciones de las TIC)

Prioridades

a) Es necesario que en este programa se aborde la problemática de ciberseguridad para aprovechar el potencial de las redes para ofrecer aplicaciones de ciberservicios seguras y accesibles.
b) Este programa debe desarrollar asimismo una comprensión común de las cuestiones del correo indeseado y las ciberamenazas, así como sus contramedidas.
c) Para minimizar, prevenir y detectar las ciberamenazas resulta asimismo necesario facilitar más contactos y cooperación con objeto de respaldar la recogida y difusión de información sobre ciberseguridad, y para intercambiar prácticas recomendadas que den soporte a una eficaz ayuda recíproca, respuesta y recuperación entre los miembros y entre los gobiernos, empresas y la sociedad civil.
d) La BDT debe actuar asimismo como facilitadora de la cooperación regional e interregional, y dar soporte a las oportunas actividades de creación de capacidades a nivel regional.
e) Esto podría consistir, entre otras cosas, en el desarrollo de MoU entre los Estados Miembros interesados para mejorar la ciberseguridad.

Tareas

a) Desarrollar directrices, herramientas de planificación y manuales sobre el aspecto tecnológico y el político de la ciberseguridad.
b) Desarrollar herramientas de ciberseguridad para los decisores de las políticas y otros sectores pertinentes.
c) Desarrollar material de formación sobre estrategias tecnológicas y evolución tecnológica para la implementación de la ciberseguridad.
d) Organizar talleres, reuniones y seminarios para abordar cuestiones técnicas, políticas, legales y estratégicas de la ciberseguridad.
e) Ofrecer ayuda a los Estados Miembros para que desarrollen leyes y una legislación modelo para la prevención de la ciberdelincuencia.

f) Identificar los requisitos de la ciberseguridad y proponer soluciones para el desarrollo de aplicaciones TIC seguras. Ayudar a la concienciación e identificar cuestiones clave para soportar la cultura de la ciberseguridad así como recomendar modelos de buenas prácticas para soportar las aplicaciones TIC y minimizar las ciberamenazas.
g) Desarrollar herramientas que faciliten la compartición de información sobre las cuestiones tecnológicas y políticas y sobre las prácticas óptimas de ciberseguridad.
h) Tener en cuenta, en su caso, el trabajo pertinente de otros participantes: la OCDE y los signatarios de acuerdos fundamentales sobre ciberseguridad y correo indeseado tal como el *Plan de Acción de Londres* y el *Memorándum de Entendimiento Seúl-Melbourne contra el correo indeseado.*

2 Resolución 45 de la CMDT-06 – Mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo indeseado (extractos)

recordando

su apoyo fundamental al Programa 3 (ciberestrategias y aplicaciones de las TIC), lo que confirma que éste asumirá la responsabilidad primordial de la Línea de Acción del Programa de Acciones de Túnez sobre creación de confianza y seguridad en la utilización de las TIC (Líneas de Acción C5),

tomando nota

de que la Resolución 50 (Florianópolis, 2004) de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) sobre ciberseguridad se limita exclusivamente al estudio de aspectos técnicos para reducir las repercusiones de este fenómeno,

insta a los Estados Miembros

a que proporcionen el apoyo necesario para aplicar la presente Resolución,

resuelve

encargar al Director de la Oficina de Desarrollo de las Telecomunicaciones

a) que, junto con el Programa 3 y sobre la base de las contribuciones de los Miembros, organice reuniones de Estados Miembros y Miembros de Sector para considerar la manera de mejorar la ciberseguridad, con inclusión entre otras cosas, de un Memorándum de Entendimiento sobre mejora de la ciberseguridad y lucha contra el correo indeseado en los Estados Miembros interesados;
b) que notifique los resultados de dichas reuniones a la Conferencia de Plenipotenciarios (Antalya, 2006).

Consecuencias de la Resolución 45: Proyecto de mejora de la cooperación sobre ciberseguridad y lucha contra el correo indeseado

Dentro de la coordinación del Programa 3, la BDT va a desarrollar un proyecto mundial con la participación de múltiples partes interesadas para vincular las iniciativas existentes con el objetivo de abordar las necesidades de los países en desarrollo.

Este proyecto está programado para empezar en 2007 y se centrará en la oferta de soluciones en los siguientes dominios:

1) Definición de una completa legislación.
2) Desarrollo de medidas técnicas.
3) Creación de asociaciones en la industria, especialmente con los proveedores de servicios de Internet, operadores móviles y asociaciones de marketing directo.
4) Formación de los consumidores y protagonistas de la industria sobre medidas contra el correo indeseado y prácticas de seguridad de Internet.

5) Cooperación internacional a nivel de los gobiernos, industria, consumidores, empresas y grupos opuestos al correo indeseado, para obtener un planteamiento mundial y coordinado ante este problema.

Además de lo enumerado anteriormente, durante los debates y presentaciones se identificaron los aspectos siguientes, que se indican sin ningún orden de prioridad específico, y que se consideraron importantes para la cooperación y ayuda a los Estados Miembros, en los que podría implicarse el UIT-D con entidades de reconocida experiencia en el dominio de la ciberseguridad y la lucha contra el correo indeseado:

a) Concienciación básica.
b) Adecuación de la legislación nacional.
c) Creación de capacidad personal e institucional.
d) Puesta en vigor (dominio de creación de capacidad).
e) Estrategias y políticas nacionales sobre seguridad.
f) Intercambio de información entre países y entre las partes interesadas pertinentes.
g) Establecimiento de coordinadores nacionales.
h) Supervisión y evaluación del progreso de las iniciativas existentes.
i) Respuesta, vigilancia y alerta ante incidentes.
j) Evaluación de las vulnerabilidades y amenazas a la ciberseguridad.
k) Herramientas y aplicaciones efectivas para la red y la ciberseguridad.
l) Asociaciones.
m) Cooperación internacional.

En relación con el proyecto:

– El proyecto, cuyo título es «Proyecto de mejora de la cooperación sobre ciberseguridad y lucha contra el correo indeseado», tendrá una duración de cuatro años, comenzando en 2007, y se integrará en el Plan Operacional de la BDT para 2007.
– Se entregarán Informes anuales a las sesiones del Consejo de la UIT sobre el progreso de su puesta en práctica.
– El proyecto deberá tener en cuenta en su aplicación, las decisiones de la CMDT-06 sobre el mandato del Sector de Desarrollo de materia de ciberseguridad y lucha contra el correo indeseado.
– El proyecto debe apuntar principalmente a ofrecer ayuda a los países en desarrollo en los ámbitos identificados anteriormente por la reunión como vitales para la cooperación en el dominio de la ciberseguridad y lucha contra el correo indeseado.
– En lo que se refiere a la legislación pertinente, considerar en su caso, el trabajo pertinente del Consejo de Europa en su ayuda a los países para desarrollar su legislación nacional armonizada con el Convenio sobre Ciberdelincuencia.
– La ejecución de actividades en el marco de este proyecto debe basarse en la solicitud expresa de los países, haciendo hincapié en los países en desarrollo.
– Una vez desarrollado el proyecto, deberá presentarse a las posibles entidades de financiación, entre ellas los Estados Miembros, y organizaciones internacionales o del sector privado, tales como el Banco Mundial y la Comisión Europea.

3 Resolución 2 de la CMDT-06 – Comisión de Estudio 1 del UIT-D, Cuestión 22 – Garantía de seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad

a) Estudiar, catalogar, describir y concienciar sobre:
   - las cuestiones principales afrontadas por los decisores de las políticas nacionales al colaborar con todas las partes interesadas en la construcción de una cultura de ciberseguridad;
   - las principales fuentes de información y ayuda relacionadas con la construcción de una cultura de ciberseguridad;
   - las prácticas óptimas empleadas con éxito por los encargados de la formulación de políticas nacionales en la colaboración con todas las partes interesadas para organizar la ciberseguridad y desarrollar una cultura de seguridad;
   - los problemas singulares afrontados por los países en desarrollo al abordar la seguridad de redes y las prácticas óptimas para la resolución de estos problemas.

b) Examinar las prácticas óptimas para el establecimiento y explotación de capacidades de vigilancia, alerta, respuesta a los incidentes y recuperación tras los mismos, que puedan utilizar los Estados Miembros para establecer sus propias capacidades nacionales.

Elaborar uno o varios informes para los miembros sobre las cuestiones identificadas en el punto 3a) anterior, en los que se destaque que las redes de comunicación e información seguras son indispensables para la construcción de la sociedad de la información y para el desarrollo socioeconómico de todas las naciones.

4 Resolución 130 (Rev. Antalya, 2006) – Fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación

resuelve

atribuir gran prioridad a esta actividad en la UIT, teniendo en cuenta su competencia y conocimientos técnicos,

encarga al Secretario General y a los Directores de las tres Oficinas

1 que examinen:
   i) los trabajos llevados a cabo hasta el momento por la UIT y otras organizaciones pertinentes así como las iniciativas encaminadas a responder a las amenazas existentes y futuras con miras a crear confianza y seguridad en la utilización de las TIC como, por ejemplo, la lucha contra el correo no deseado;
   ii) con la ayuda de los grupos asesores, de conformidad con las disposiciones del Convenio y la Constitución de la UIT, los avances logrados en la aplicación de la presente Resolución y en el papel de la UIT como moderador/facilitador de la Línea de Acción C5 de la CMSI;

2 que, teniendo presente las disposiciones de la CMSI sobre el acceso universal y no discriminatorio a las TIC para todas las naciones, faciliten el acceso a los instrumentos necesarios para aumentar la confianza y la seguridad de todos los Estados Miembros en la utilización de las TIC;

3 que sigan utilizando el Portal de la Ciberseguridad para intercambiar información sobre iniciativas nacionales e internacionales relativas a la ciberseguridad en todo el mundo;

4 que presenten todos los años un informe al Consejo sobre estas actividades y formulen las propuestas del caso,

encarga al Director de la Oficina de Desarrollo de las Telecomunicaciones

1 que elabore, teniendo en cuenta los resultados de la CMDT-06 (Doha, 2006) y la reunión siguiente de conformidad con la Resolución 45 (Doha, 2006) de dicha Conferencia, los proyectos encaminados a mejorar la cooperación sobre la ciberseguridad y la lucha contra el correo no deseado, para dar respuesta a las necesidades de los países en desarrollo, en estrecha colaboración con los asociados correspondientes;

2 que, en el límite de los recursos existentes, proporcione el apoyo financiero y administrativo necesario para esos proyectos y que procure conseguir recursos adicionales (en efectivo o en especie) para su ejecución mediante acuerdos de colaboración;

3 que garantice la coordinación de esos proyectos en el marco de las actividades globales que la UIT lleva a cabo como moderador/facilitador de la Línea de Acción C5 de la CMSI;

4 que coordine esos proyectos con las actividades y los programas de las Comisiones de Estudio del UIT-D sobre este asunto;

5 que siga colaborando con las organizaciones que corresponda con miras a intercambiar las mejores prácticas y difundir información mediante, por ejemplo, talleres mixtos y reuniones de capacitación;

6 que presente todos los años un informe al Consejo sobre estas actividades y formule las propuestas del caso.

Sinopsis de las actividades del UIT-D encaminadas a la aplicación de la Línea de Acción C.5 de la CMSI – Creación de confianza y seguridad en la utilización de las TIC

1 Introducción

Las TIC tienen el potencial de ofrecer a los países en desarrollo servicios básicos a través de la cibersalud, la cibereducación, el comercio electrónico y el cibergobierno, en beneficio de sus ciudadanos, muchos de los cuales siguen sin tener acceso a infraestructuras físicas tales como hospitales, colegios y servicios de administración pública.

Hoy en día, ya se pueden realizar transacciones electrónicas entre médicos y pacientes, acceder a servicios de administración pública en línea y vender bienes y servicios por Internet a clientes remotos, gracias a los adelantos de las tecnologías de la información y las telecomunicaciones. El potencial de las aplicaciones de las TIC para solucionar algunos de los problemas de acceso a servicios básicos y potenciar la participación de los países en desarrollo en la sociedad de la información, puede hacerse realidad.

Los beneficios de la sociedad de la información para los gobiernos, empresas y ciudadanos sólo pueden materializarse plenamente si se abordan los problemas de seguridad y confianza, y se implementan soluciones para afrontar la ciberdelincuencia, crear legislación aplicable en esta materia, evitar la suplantación de identidades, preservar la privacidad de los datos y proteger los sistemas de información críticos. La gran dependencia de las TIC como vector de mejora del desarrollo socioeconómico y la velocidad a la que se puede acceder, manipular y destruir datos y sistemas con información crítica, han hecho que la ciberseguridad se sitúe a la cabeza de la lista de los problemas prioritarios que se plantean a la nueva sociedad de información y a la economía basada en el conocimiento.

2 Actividades e iniciativas

De acuerdo con el mandato adoptado por los miembros que participaron en la Conferencia de Plenipotenciarios y en las Conferencias y Asambleas Mundiales, y en sus funciones como moderadores/facilitadores para la Línea de Acción C.5, la UIT y sus asociados están emprendiendo muchas acciones dirigidas a la creación de confianza y seguridad en el empleo de las TIC.

En este Informe se describen someramente algunas de las acciones emprendidas y otras que se encuentran en proyecto. Estas acciones se clasifican en cinco áreas de actividad principales (**garantía de la seguridad de las aplicaciones TIC, legislación, estrategias políticas y creación de capacidad, concienciación** y **cooperación entre miembros**). Se presentan asimismo referencias a otras fuentes de información sobre actividades pertinentes al cumplimiento de los objetivos de la Línea de Acción C.5 de la CMSI y se invita a todas las partes interesadas a aunar sus esfuerzos en la creación de confianza y seguridad en las TIC.

2.1 Garantía de seguridad de las aplicaciones TIC – Implementación del proyecto

Los problemas de seguridad suponen un obstáculo para la utilización de las TIC en ciertos servicios esenciales tales como el cibergobierno, el comercio electrónico, los pagos electrónicos y la cibersalud, en los que es importante proteger los datos sensibles, garantizar la integridad de los datos y transacciones y establecer las identidades de las partes. Para hacer que el manifiesto potencial de las TIC para prestar servicios de valor añadido asequibles se convierta en realidad, hay que resolver estas cuestiones de seguridad y confianza e implementar soluciones de orden práctico.

Hay soluciones de orden práctico que incrementan el potencial de las TIC para prestar servicios críticos construidos sobre tecnologías de confianza y seguridad que han hecho posible en diversos países pasar de sencillos sistemas de difusión de información a la realización de transacciones críticas y a la prestación de una amplia gama de servicios a la población.

Gracias a la UIT, varios países en desarrollo se han implicado activamente en el despliegue y empleo de soluciones basadas en tecnologías de confianza y seguridad, extendiendo de este modo los beneficios de las TIC a ámbitos tales como el gobierno y los servicios sanitarios.

Se han ejecutado proyectos que utilizan tecnologías avanzadas de confianza y seguridad basadas en la infraestructura de claves públicas (PKI), entre ellas la autenticación biométrica, las tarjetas inteligentes, los certificados digitales UIT-T X.509 y las técnicas de firma digital, en **Barbados, Bhután**, **Bulgaria**, **Burkina Faso**, **Camboya**, **Camerún**, **Côte d'Ivoire**, **Georgia**, **Jamaica**, **Paraguay**, **Perú, Senegal**, **Turquía** y **Zambia**. En otros países la ejecución de estos proyectos está prevista para 2007 (http://www.itu.int/ITU-D/e-strategy/e-applications/archive04.html).

2.1.1 Georgia

En este proyecto de la UIT se abordan los problemas aplicando soluciones rentables para la transmisión segura, el acceso y el procesamiento de documentos oficiales digitalizados, incrementando de este modo la eficiencia y transparencia de los servicios de la administración. Se facilitaron a altos funcionarios del Ministerio de Transporte y Comunicaciones de Georgia soluciones para la mejora de la automatización del flujo de trabajo que permitían a dichos funcionarios la firma y difusión digital de documentos oficiales, sustituyendo de este modo los lentos y costosos métodos basados en papel. El control de acceso a la documentación sensible se realiza con soluciones de confianza y seguridad que comprueban la identidad de las personas autorizadas del Ministerio.

2.1.2 Paraguay

Este proyecto corresponde a una plataforma para la implementación de un mecanismo seguro y de confianza basado en Internet para los operadores y proveedores de servicio que intercambiaban información sensible (tal como la declaración de la renta) en formato electrónico con la agencia reguladora nacional (CONATEL). En este proyecto se utilizan soluciones TIC seguras y de alta confianza que optimizan el proceso de expedición de licencias a operadores de telefonía pública e incrementa la eficiencia en el proceso administrativo del regulador.

2.1.3 Barbados y Jamaica

Se ha ayudado a establecer un marco de política nacional para la utilización de los certificados digitales y para las operaciones de las autoridades de certificación. Entre las ayudas de la UIT figuran también la definición de las especificaciones de la tecnología y las directrices de la política para la implementación de una plataforma nacional en Barbados y Jamaica para la expedición y gestión de certificados digitales, prestando servicios de autenticación eficaces y garantizando la seguridad y la confianza en las transacciones de cibergobierno y cibernegocios. En Jamaica, tras la adopción de la Ley de Cibertransacciones por parte del Parlamento a finales de 2006, se facilitó la ayuda de expertos para garantizar que la plataforma de gestión de identidades y políticas afines fuera conforme con la legislación. Está previsto que esta infraestructura de claves públicas, financiada conjuntamente por la UIT y por el Gobierno de Jamaica, entre en funcionamiento en 2007.

2.1.4 Camerún

Este proyecto de la UIT permite la transmisión segura de documentación oficial sensible por Internet y proporciona servicios administrativos en línea basados en Internet a los ciudadanos de las zonas urbanas y remotas carentes de infraestructura administrativa física. Las soluciones utilizadas, basadas en las tecnologías de encriptación y de firma electrónica tales como la autenticación, la confidencialidad de datos, la integridad de datos y el no rechazo, han permitido dar respuesta a algunas de las amenazas de la ciberseguridad entre ellas la usurpación de identidad.

2.1.5 Bulgaria

La ayuda de la UIT para la puesta en práctica de una plataforma de ciberseguridad permite que la comunicación entre el Ministerio de Transporte y Telecomunicaciones, el Ministerio de Finanzas, el Consejo de Ministros y la Comisión de Regulación de las Comunicaciones (CRC) se realice con un alto grado de seguridad, gracias al uso de aplicaciones PKI y de aplicaciones habilitadas para PKI. Permite la interacción segura, eficiente y rentable entre los altos funcionarios del Gobierno, complementando de este modo las entrevistas personales e incrementando la productividad. Todos los datos intercambiados entre los funcionarios participantes están asegurados y firmados digitalmente utilizando técnicas de autenticación eficaces basadas en la confidencialidad, el no rechazo, la integridad de datos y el uso de certificados.

2.1.6 Turquía

Uno de los objetivos estratégicos de este proyecto es mejorar los servicios sanitarios de Turquía desarrollando un medio seguro de información sanitaria que permita a los servicios de sanidad (servicios sanitarios primarios y secundarios), a los profesionales de la salud y a los ciudadanos el acceso fácil y seguro a información sobre la salud utilizando las últimas TIC.

Las piedras angulares del proyecto son el desarrollo de sistemas de información sanitaria primaria para el sistema de médicos de familia, la implementación de registros sanitarios electrónicos y el desarrollo de sistemas interoperables entre los proveedores de servicios sanitarios, a saber, los centros de salud primaria, los hospitales y las agencias de seguros públicas y privadas.

2.1.7 Bhután

Para responder a las necesidades de la población rural sobre acceso a servicios que exigirían normalmente desplazarse durante varios días a la capital administrativa, la UIT implementó en Bhután una plataforma basada en la infraestructura de claves públicas que incorporaba tecnologías de autenticación biométrica, encriptación fuerte e integridad de datos. Esta plataforma de ciberseguridad, financiada por la UIT y el Gobierno de Bhután, proporciona servicios para la gestión y verificación de identidades, la autenticación basada en certificados, la firma digital, así como servicios de integridad y confidencialidad de datos. Gracias a la ayuda de la UIT, los usuarios remotos de Bhután podrán acceder a servicios críticos desarrollados sobre tecnologías de confianza y seguridad, extendiendo de este modo las capacidades y beneficios de las TIC a la prestación de servicios a las poblaciones rurales y urbanas.

2.1.8 Proyecto mundial sobre ciberseguridad y lucha contra el correo indeseado

La UIT organizó la primera reunión de Estados Miembros y Miembros de los Sectores para tratar del modo de mejorar la cooperación sobre ciberseguridad así como la lucha contra el correo indeseado. En este evento se pretendía conseguir principalmente los tres objetivos siguientes:

a) Alcanzar un entendimiento común y acaso el acuerdo en los dominios de la ciberseguridad y el correo indeseado, donde es imprescindible la adopción de un mecanismo que mejore la cooperación entre los Estados Miembros.
b) Identificar posibles mecanismos, entre otros un Memorándum de Entendimiento, para mejorar la cooperación entre los Estados Miembros en materia de ciberseguridad y correo indeseado.
c) Plantear propuestas a partir de las contribuciones de los miembros y recogerlas en un Informe a presentar a la Conferencia de Plenipotenciarios de 2006 para su consideración.

En la reunión, los miembros identificaron los principales problemas vitales para la cooperación mundial en materia de ciberseguridad y lucha contra el correo indeseado (véase la lista siguiente).

a) Concienciación básica.
b) Creación y promulgación de una legislación nacional eficaz.
c) Creación de capacidades personales e institucionales.
d) Puesta en vigor (dominio de creación de capacidad).
e) Creación de estrategias y políticas nacionales sobre seguridad.
f) Facilitar el intercambio de información entre países y entre las partes interesadas pertinentes.

g) Establecimiento de coordinadores nacionales.
h) Supervisión y evaluación del progreso de las iniciativas existentes.
i) Implementación de soluciones de respuesta, vigilancia y alerta ante incidentes.
j) Evaluación de las vulnerabilidades y amenazas a la ciberseguridad.
k) Preparar herramientas y aplicaciones efectivas para la red y la ciberseguridad.
l) Asociaciones.
m) Cooperación internacional.

Se acordó que la UIT desempeñara un papel primordial en la coordinación de las iniciativas existentes y en la provisión de un marco de reunión que aproximara las iniciativas existentes con objeto de dar respuesta a las necesidades de los países en desarrollo. El Informe de esta reunión se presentó en la Conferencia de Plenipotenciarios de la UIT de 2006, en Antalya, donde se ratificó como actividad clave de la UIT para la implementación de un mecanismo de cooperación en materia de ciberseguridad y lucha contra el correo indeseado. Este proyecto que habrá de ejecutarse en el marco de un proyecto mundial titulado: «Proyecto de mejora de la cooperación en materia de ciberseguridad y lucha contra el correo indeseado», tendrá una duración de cuatro años, comenzará en 2007 y formará parte del Plan Operacional del Sector de Desarrollo de la UIT para 2007.

En relación con dicho proyecto:

– En la ejecución del proyecto deberá tenerse en cuenta el mandato de la UIT en materia de ciberseguridad y lucha contra el correo indeseado.
– El proyecto debe encaminarse principalmente a ofrecer ayuda a los países en desarrollo en los ámbitos identificados por la reunión como vitales para la cooperación en el dominio de la ciberseguridad y la lucha contra el correo indeseado.
– En lo que se refiere a la legislación pertinente, considerar, en su caso, los trabajos correspondientes del Consejo de Europa para ayudar a los países a desarrollar una legislación nacional armonizada con el Convenio sobre Ciberdelincuencia.
– La ejecución de actividades en el marco de este proyecto debe basarse en la solicitud expresa de los países, con una relevancia especial de los países en desarrollo.
– Una vez desarrollado el proyecto, deberá presentarse a las posibles entidades de financiación, entre ellas los Estados Miembros y organizaciones internacionales o del sector privado tales como el Banco Mundial y la Comisión Europea.

2.2 Legislación

Ayuda a los países en desarrollo para la redacción de leyes modelo y de leyes para la represión del correo indeseado

Los participantes en el Simposio Mundial de la UIT para organismos reguladores solicitaron la ayuda de la UIT para el desarrollo de legislación contra el correo indeseado. En el Capítulo 7 de la edición de 2006 de la publicación de la UIT *Tendencias en las Reformas de Telecomunicaciones* se describe y analiza el contenido de una ley modelo contra el correo indeseado cuyas disposiciones definen con el máximo detalle los códigos de conducta exigibles a los ISP. Estos códigos de conducta prohibirían a los clientes de los ISP la utilización de éstos como instrumento de correo indeseado y actos dolosos afines tales como la falsificación de direcciones de origen y la suplantación de identidad, así como la formalización de acuerdos entre redes pares con otros ISP que no respetasen códigos de conducta semejantes. El Capítulo 7 de ***Tendencias en las Reformas de Telecomunicaciones de 2006***, Stemming the International Tide of Spam, está disponible en línea en:
http://www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf

2.3 Políticas, estrategias y creación de capacidades

2.3.1 Talleres y seminarios

La UIT ha organizado talleres y seminarios a nivel nacional y regional sobre políticas y estrategias tecnológicas para la ciberseguridad en países tales como Azerbaiyán, Barbados, Camerún, Chile (para

los Estados de Mercosur), Letonia (para los Estados de la UE, CEI y Estados Bálticos), Mongolia, Pakistán, Paraguay, Perú (para la Región Andina de Latinoamérica), Rumania, Seychelles, la República Árabe Siria y Uzbekistán.

Se han organizado actividades específicas de creación de capacidades humanas e institucionales en materia de tecnología, política y estrategia de ciberseguridad en Camerún, Zambia, Barbados, Jamaica, Bulgaria, Bhután y Siria.

2.3.2 La reunión mundial

Se celebró en Ginebra una reunión mundial a la que asistieron cerca de 50 expertos de seguridad y más de 500 delegados en representación de 120 países, aproximadamente, para debatir las tecnologías, estrategias, políticas y cuestiones jurídicas relativas a la firma digital, la certificación digital y las soluciones de encriptación para los países en desarrollo.

2.3.3 Simposio Regional de la UIT sobre cibergobierno e IP para la Región Árabe

Entre los principales temas debatidos en este Simposio cabe citar la seguridad y la confianza, que condujeron a la Declaración de Dubai que hace hincapié en la necesidad de que la UIT continúe sus actividades relacionadas con la ciberseguridad de las ciberaplicaciones y servicios. A esta reunión asistieron encargados de formulación de las políticas de la Región Árabe para tratar cuestiones comunes y encontrar un marco común para afrontar los retos principales en materia de ciberseguridad. Se planificaron actividades de seguimiento para 2007 en áreas específicas de interés para la Región (tales como la gestión de identidades y la firma electrónica).

2.3.4 Simposio de Naciones Unidas durante la Conferencia y Exposición del Mundo de las TI Sanitarias

La UIT, la OMS, la UNESCO, el UNITAR y colaboradores de la industria organizaron un Simposio de Naciones Unidas durante la Conferencia y Exposición del Mundo de las TI Sanitarias en la que uno de los principales asuntos tratados fue la ciberseguridad en la sanidad. A este Simposio de Naciones Unidas celebrado en el Palexpo de Ginebra el 10 de octubre de 2006, asistieron miembros de cuatro Agencias de Naciones Unidas para tratar entre otros temas el papel crítico de la ciberseguridad en las transacciones y aplicaciones médicas y sanitarias. Para mayor información véase: http://www.worldofhealthit.org/about/about_partners.asp

2.4 Concienciación

2.4.1 Publicaciones y Artículos

Guide de la cybersecurité pour les pays en développement ©ITU 2006

Cybersecurity guide for developing countries ©ITU 2006

Guía de ciberseguridad para los países en desarrollo ©UIT 2006

Se trata de una guía de referencia sobre ciberseguridad para ayudar a los países en desarrollo y a los menos adelantados a crear capacidades locales y a fomentar la concienciación sobre algunos de los problemas clave para la sociedad de la información en materia de seguridad. En esta guía se explican algunos de los principales problemas, como el correo indeseado, los programas maliciosos (virus, gusanos y troyanos), la privacidad de los datos, la falta de autenticación y la necesidad de confidencialidad e integridad de los datos. Entre otros temas contemplados se encuentran estudios de casos prácticos sobre legislación para la ciberseguridad y ejemplos de métodos ya utilizados para proteger infraestructuras críticas. Las versiones de esta guía en inglés y francés pueden descargarse gratuitamente del sitio web del UIT-D: http://www.itu.int/ITU-D/e-strategy/publications-articles/

Research on Legislation in data privacy, security and the prevention of Cybercrime – ©ITU 2006 (Investigación sobre la legislación en materia de privacidad de datos, seguridad y prevención de la ciberdelincuencia) – ©UIT 2006

Ciertos aspectos de las TIC necesitan protegerse desde un punto de vista jurídico, especialmente en lo que se refiere a la legislación existente en materia de seguridad de datos y de derechos de la propiedad intelectual, y a las formas tradicionales de delitos cometidos sobre la nueva autopista de la información, tales como robo de identidad, fraude y extorsión. Es evidente que hay que revisar esta legislación y adaptarla a las TIC, y reconocer que existen nuevos tipos de delitos informáticos y se necesitan nuevos dispositivos de seguridad para autenticar los flujos de información.

Este trabajo de investigación aborda los imperativos jurídicos necesarios para proteger los intereses nacionales de los países en desarrollo y garantizar el desarrollo de las TIC y del comercio electrónico, garantizando al mismo tiempo la seguridad de las infraestructuras con la protección jurídica adecuada. Hay tres principios fundamentales aceptados como elementos de importancia de la ciberseguridad. Se trata de la confidencialidad, la integridad y la disponibilidad. Estos tres elementos tienen áreas comunes estrechamente relacionadas. A veces resulta difícil establecer los límites estrictos entre las diversas categorías y determinar qué tipo de legislación conviene aplicar en un área específica. Se puede descargar una copia de esta publicación en el sitio web de Ciberestrategias de la UIT: http://www.itu.int/ITU-D/e-strategy/publications-articles/

A New Guide for Developing Countries on Cybercrime ©ITU 2007 (Nueva Guía sobre ciberdelincuencia para los países en desarrollo) – ©UIT 2007

A finales de 2006 la UIT terminó de elaborar un nuevo documento de referencia destinado a despertar la conciencia sobre la cuestión de la ciberdelincuencia y facilitar la ejecución de actividades para la creación de capacidades humanas e institucionales. Se abordó asimismo la necesidad de desarrollar un entendimiento común en materia de ciberamenazas y sus contramedidas. Este documento de 160 páginas tiene por objeto primordial servir de guía y documentación de referencia a los países en desarrollo. Presenta una visión general de las diversas formas de ciberdelincuencia y de los perfiles de los ciberdelincuentes. Se explican las actuales vulnerabilidades de Internet y los ciberataques, las pruebas digitales, los principios básicos de la práctica judicial en materia informática y de las investigaciones informáticas y presenta un glosario terminológico sobre ciberdelincuencia y una completa lista de referencias. Esta nueva Guía y la anterior (sobre ciberseguridad) serán uno de los documentos base para las actividades en proyecto encaminadas a la creación de capacidades humanas e institucionales en materia de ciberseguridad y ciberdelincuencia. Esta Guía, originalmente publicada en inglés, se traducirá a los seis idiomas de la UIT y se facilitará a los países interesados durante el segundo trimestre de 2007, en formato papel y como documento electrónico disponible para su descarga en el sitio web de la UIT.

2.5 Cooperación entre los miembros

Para facilitar el intercambio de experiencias y las prácticas óptimas entre sus miembros, la UIT ofrece la plataforma de la Comisión de Estudio del Sector de Desarrollo (UIT-D) donde los miembros pueden acordar planteamientos comunes para la resolución de problemas en materia de ciberseguridad y lucha contra el correo indeseado. En septiembre de 2006 se celebró la primera reunión de la Cuestión de la Comisión de Estudio del UIT-D relativa a la ciberseguridad y se aprobó el programa de trabajo para este nuevo ciclo. En el periodo 2006-2009 el programa de trabajo y los resultados previstos de esta Cuestión de la Comisión de Estudio del UIT-D comprenden, entre otros, lo siguientes:

a) Estudiar, catalogar, describir y concienciar sobre:
   - las cuestiones principales afrontadas por los decisores de las políticas nacionales al colaborar con todas las partes interesadas en la construcción de una cultura de ciberseguridad;
   - las principales fuentes de información y ayuda relacionadas con la construcción de una cultura de ciberseguridad;
   - las prácticas óptimas empleadas con éxito por los encargados de la formulación de políticas nacionales en la colaboración con todas las partes interesadas para organizar la ciberseguridad y desarrollar una cultura de seguridad;
   - los problemas singulares afrontados por los países en desarrollo al abordar la seguridad de redes y las prácticas óptimas para la resolución de estos problemas.

b) Examinar las prácticas óptimas para el establecimiento y explotación de capacidades de vigilancia, alerta, respuesta a los incidentes y recuperación tras los mismos, que puedan utilizar los Estados Miembros para establecer sus propias capacidades nacionales.

Elaborar uno o varios informes para los miembros, sobre las cuestiones identificadas en el punto 3a) anterior, en los que se destaque que las redes de comunicación e información seguras son indispensables para la construcción de la sociedad de la información y para el desarrollo socioeconómico de todas las naciones.

3 Resumen

La ciberseguridad es una cuestión que debe preocupar a todas las naciones y ser objeto de un planteamiento serio por parte de las mismas. En los países en desarrollo, las aplicaciones TIC construidas sobre plataformas seguras y de alta confianza pueden ofrecer servicios críticos a la población en ámbitos tales como la sanidad, las finanzas, la administración pública y el comercio.

Los países desarrollados también pueden disfrutar de estos beneficios, además de dar respuesta a la necesidad de proteger sus infraestructuras críticas y salvaguardar las transacciones y datos sensibles.

Los retos afrontados en esta área sólo pueden abordarse eficazmente mediante la cooperación y colaboración entre los gobiernos, la industria, las organizaciones internacionales, la sociedad civil y otros interesados pertinentes. El fomento de la concienciación sobre los retos y oportunidades, la creación de capacidades locales, la elaboración de legislación aplicable, la ejecución de proyectos que aporten soluciones seguras y de alta confianza y la elaboración de las oportunas políticas son algunas de las principales áreas en las que los asociados deben colaborar para alcanzar el objetivo común de una sociedad de la información integradora, segura y mundial, para todos.

La UIT, en el marco de su mandato, está emprendiendo iniciativas a través de la ejecución de proyectos, la facilitación del intercambio de información, la creación de capacidades, la concienciación y la instalación de una plataforma de cooperación y colaboración para abordar las cuestiones de la ciberseguridad a nivel mundial. Con el ánimo de progresar en el logro de los objetivos identificados por la CMSI, la UIT invita a todos los colaboradores interesados a aunar sus esfuerzos para crear seguridad y confianza en el empleo de las TIC.

Anexo D – Principales cuestiones en materia de seguridad de las que se ocupa el UIT-T durante el periodo 2005-2008

Extraído del sitio
http://www.itu.int/ITU-T/studygroups/com17/cuestiones.html

Cuestiones asignadas a la Comisión de Estudio 17 del UIT-T (periodo de estudio 2005-2008)

Comisión de Estudio 17: Seguridad, lenguajes y aplicaciones informáticas de telecomunicación

Cuestión 2/17 – Servicios de directorio, sistemas de directorio y clave pública/certificados de atributos

2.1 Servicios de directorio

a) ¿Qué definiciones y nuevos perfiles de servicio es necesario adoptar para aprovechar técnicas de directorio tan extendidas como X.500 y LDAP, por ejemplo?

b) ¿Qué modificaciones hay que introducir en las Recomendaciones de las series E y F y qué nuevas Recomendaciones hay que elaborar para especificar las mejoras a introducir en las definiciones y perfiles de servicio de directorio existentes y para corregir sus defectos?

2.2 Sistemas de directorio

a) ¿Qué mejoras hay que introducir en el directorio para adaptarlo a las necesidades de los usuarios actuales y potenciales, para obtener por ejemplo más homogeneidad en las informaciones de directorio en los sitios en las que están reproducidas, soportar el funcionamiento sobre agregados asociados de atributos de directorio especificados por el usuario, mejorar el rendimiento de recuperación de grandes números de resultados devueltos, y resolver la confusión provocada por la diversidad de proveedores de servicios de directorio que contienen información diferente con nombres idénticos?

b) ¿Qué otras mejoras es necesario introducir en el directorio para permitir el interfuncionamiento con servicios implementados con ayuda de la especificación LDAP del IETF, incluida la utilización eventual de XML para el acceso a directorios, así como su soporte?

c) ¿Qué otras mejoras hay que introducir en el directorio y en los certificados de atributos y de claves públicas para permitir su utilización en entornos de recursos limitados, por ejemplo, las redes hercianas y las redes multimedios?

d) ¿Qué otras mejoras hay que introducir en el directorio para potenciar su integración en dominios tales como los servicios de red inteligente, de redes de telecomunicaciones y de directorios públicos?

e) ¿Qué modificaciones hay que introducir en las Recomendaciones de la serie X.500 y cuáles son las nuevas Recomendaciones a elaborar para perfilar la definición de las mejoras del directorio y solucionar sus imperfecciones?

El estudio dedicado a los sistemas de directorio se realizará en cooperación con el JTC 1 de la ISO/CEI en el marco de los trabajos dedicados a la ampliación de la norma ISO/CEI 9594, texto común con las Recomendaciones X.500-X.530. Por otra parte se mantendrá la vinculación y estrecha cooperación con el IETF, especialmente en el dominio del LDAP.

2.3 Certificados de atributos y de claves públicas

a) ¿Qué otras mejoras cabe introducir en los certificados de atributos y de claves públicas para permitir su utilización en entornos de recursos limitados tales como las redes hercianas y las redes multimedios?

b) ¿Qué otras mejoras hay que introducir en los certificados de atributos y de claves públicas para hacerlos más útiles en dominios tales como la biometría, la autenticación, el control de acceso y el comercio electrónico?

c) ¿Qué modificaciones cabe introducir en la Recomendación X.509 para perfilar la definición de las mejoras de la Recomendación X.509 y solucionar sus imperfecciones?

El estudio dedicado a los certificados de atributos y de claves públicas se realizará en cooperación con el JTC 1 de la ISO/CEI en el marco del trabajo de que dedica a la extensión de la norma ISO/CEI 9594-8, texto común con la Recomendación X.509. Por otra parte se mantendrá la vinculación y estrecha cooperación con el IETF, especialmente en los dominios de la PKI.

Cuestión 4/17 – Proyecto de seguridad de los sistemas de comunicaciones (Continuación de la Cuestión G/17)

El amplio dominio de la seguridad cubre una gran diversidad de temas. La seguridad puede aplicarse prácticamente a la totalidad de los aspectos de las tecnologías de las telecomunicaciones y de la información. Las exigencias de seguridad pueden especificarse con arreglo a uno de los dos métodos siguientes:

– El método ascendente, en virtud del cual los expertos del dominio elaboran medidas de seguridad destinadas a reforzar y proteger el dominio de red que les incumbe, por ejemplo, la biometría, la criptografía, etc. Este método es el más generalizado pero como el estudio de la seguridad se efectúa en las distintas organizaciones, queda fragmentado.

– El método descendente ofrece una visión estratégica y de alto nivel de la seguridad. En este método es indispensable tener una idea general de la situación. Este método es también el más complejo ya que resulta más difícil encontrar expertos con conocimientos detallados de cada parte de la red y de sus exigencias de seguridad, que expertos en el tema que posean un conocimiento específico en uno o dos dominios.

– Otra solución consiste en combinar los dos métodos citados, entendiendo que la coordinación inevitable. Esta manera de proceder suele plantear numerosos problemas debido a los diferentes intereses y programas que hay que tener en cuenta.

La presente Cuestión pretende fijar grandes principios, garantizando asimismo la coordinación y la organización de toda la gama de actividades a desplegar en el dominio de la seguridad de las comunicaciones en el UIT-T. El método descendente se utilizará en colaboración con otras Comisiones de Estudio y otras organizaciones de normalización. Este proyecto pretende implementar un método que se centre más en el nivel de los proyectos y de las estrategias.

Cuestiones

a) ¿Cuáles son los resultados que cabe esperar del proyecto en materia de seguridad de los sistemas de comunicación?

b) ¿Cuáles son los procesos, materias objeto de estudio, métodos de trabajo y plazo previsto para obtener los resultados esperados en el marco del proyecto?

c) ¿Qué colecciones de textos y manuales sobre la seguridad deberá elaborar y actualizar la UIT?

d) ¿Qué talleres sobre la seguridad habrá que organizar?

e) ¿Qué medidas hay que adoptar para conseguir establecer relaciones eficaces con otras organizaciones de normalización a fin de progresar en el dominio de la seguridad?

f) ¿Cuáles son las principales etapas y los criterios determinantes de éxito?

g) ¿Cómo estimular el interés de los Miembros del Sector y de las administraciones para animarlos a proseguir los esfuerzos invertidos en el dominio de la seguridad?

h) ¿Cómo actuar para que las funciones de seguridad capten más atención del mercado?

i) ¿Cómo hacer para que los gobiernos entiendan mejor que resulta indispensable y urgente proteger los intereses económicos a nivel mundial, que dependen de una infraestructura robusta y segura de las telecomunicaciones?

Cuestión 5/17 – Arquitectura y marco genérico de la seguridad

Es necesario definir requisitos y soluciones de seguridad adaptados a las amenazas de seguridad para el entorno de las comunicaciones y la evolución de las medidas de seguridad para contrarrestarlas.

Es necesario estudiar la seguridad para los nuevos tipos de redes, así como para los nuevos servicios.

Cuestiones

a) ¿Cómo debería definirse una solución completa y general de la seguridad de las comunicaciones?

b) ¿Cuál es la arquitectura de una solución completa y general de la seguridad?

c) ¿Cuál es el marco de aplicación de la estructura de seguridad para crear una solución de seguridad?

d) ¿Cuál es el marco de aplicación de la arquitectura de seguridad para evaluar (y consecuentemente mejorar) una solución de seguridad existente?

e) ¿Cuáles son los fundamentos de la arquitectura para la seguridad?

   i) ¿Cuál es la arquitectura de seguridad de las nuevas tecnologías?

   ii) ¿Cuál es la arquitectura que garantiza la seguridad extremo a extremo?

   iii) ¿Cuál es la arquitectura de seguridad en el entorno móvil?

   iv) ¿Qué arquitecturas de seguridad técnica se requieren? Por ejemplo:

      a) ¿Qué arquitectura de seguridad para sistemas abiertos?

      b) ¿Qué arquitectura de seguridad en las redes IP?

      c) ¿Qué arquitectura de seguridad en las NGN?

f) ¿Cómo modificar las Recomendaciones que definen el modelo de seguridad de capa superior y capa inferior para adaptarlas a la evolución de condiciones, y qué nuevas Recomendaciones se requieren?

g) ¿Cómo organizar las normas de arquitectura en relación con las Recomendaciones sobre seguridad existentes?

h) ¿Cómo modificar las Recomendaciones que definen el marco de seguridad para adaptarlas a las nuevas tecnologías, y qué nuevas Recomendaciones marco se requieren?

i) ¿Cómo se aplican los servicios de seguridad para suministrar soluciones de seguridad?

Cuestión 6/17 – Ciberseguridad

Se han introducido numerosos mecanismos de protección y detección, como los cortafuegos y los sistemas de detección de intrusión (IDS, *intrusion detection systems*), pero la mayoría sólo consideran los aspectos técnicos. Si bien estas soluciones técnicas son importantes, es necesario dedicar más atención y debate a la ciberseguridad desde el punto de vista de la normalización internacional.

Cuestiones

Han de estudiarse las siguientes esferas de la ciberseguridad:

- procesos para la distribución, compartición y divulgación de información sobre vulnerabilidad;
- procedimiento normalizado para el tratamiento de problemas en el ciberespacio;
- estrategia para la protección de la infraestructura crítica de la red.

Cuestión 7/17 – Gestión de la seguridad

Cuestiones

a) ¿Cómo identificar y gestionar los riesgos de seguridad en los sistemas de telecomunicaciones?

b) ¿Cómo identificar y gestionar los activos de información para los sistemas de telecomunicaciones?

c) ¿Cómo identificar los temas de gestión específicos para los operadores de telecomunicaciones?

d) ¿Cómo construir un sistema de gestión de la seguridad de la información (ISMS) para los operadores de telecomunicaciones que sea compatible con las normas ISMS existentes?

e) ¿Cómo han de tratarse y gestionarse los problemas de seguridad que se presenten en las telecomunicaciones?

Cuestión 8/17 – Telebiometría
(Continuación de una parte de la Cuestión K/17)

Cuestiones

a) ¿Cómo pueden mejorarse la identificación y autenticación de los usuarios mediante métodos de telebiometría seguros?

b) ¿Cómo utilizará el UIT-T el nuevo capítulo de la norma Fisiología CEI 60027, «Physiological subset», para obtener los elementos de un modelo de categorización de dispositivos telebiométricos seguros?

c) ¿Qué sistema de referencia de niveles de seguridad ha de utilizarse para aportar soluciones telebiométricas seguras en orden jerárquico?

d) ¿Cómo identificar temas relacionados con las tecnologías de autenticación biométrica para las telecomunicaciones?

e) ¿Cómo identificar los requisitos de las tecnologías de autenticación biométrica para las telecomunicaciones basados en una tecnología criptográfica como PKI?

f) ¿Cómo identificar un modelo y un procedimiento de autenticación biométrica para las telecomunicaciones basados en una tecnología criptográfica como PKI?

Cuestión 9/17 – Servicios de comunicación seguros
(Continuación de una parte de la Cuestión L/17)

Cuestiones

a) ¿Cómo identificar y definir los servicios de comunicaciones seguros en las comunicaciones móviles o los servicios web?

b) ¿Cómo identificar y tratar las amenazas que acechan a los servicios de comunicaciones?

c) ¿Cuáles son las tecnologías de seguridad para sustentar los servicios de comunicaciones seguros?

d) ¿Cómo ha de mantenerse la interconectividad segura entre servicios de comunicaciones?

e) ¿Qué técnicas de seguridad son necesarias para los servicios de comunicaciones seguros?

f) ¿Qué técnicas o protocolos de seguridad son necesarios para los nuevos servicios web seguros?

g) ¿Qué protocolos de aplicación seguros son apropiados para ofrecer servicios de comunicaciones seguros?

h) ¿Cuáles son las soluciones de seguridad globales para los servicios de comunicaciones seguros y sus aplicaciones?

Anexo E – Referencias bibliográficas

Texto de referencia que presenta de manera didáctica las normas de seguridad del mundo de las telecomunicaciones elaboradas por el UIT-T:

> Security in telecommunications and information technology: an overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunication. UIT–T; octubre de 2004 sitio web: *http://www.itu.int/itudoc/itu-t/86435.html*

Otras obras de referencia

Anderson Ross, Security Engineering, A Guide To Building Dependable Distributed Systems, Wiley, 2001, ISBN 0-471-38922-6

Bishop Matt, Computer security: art and science, Addisson-Wesley, 2002, ISBN 0-201-44099-7

Black Uyless, Internet Security Protocols, Protecting IP Traffic, Pentice Hall, ISBN 0-13-014249-2

Denning Dorothy E., Information Warfare and Security, Addison-Wesley, 1999, ISBN 0-201-43303-6

Dufour Arnaud, Ghernaouti-Hélie Solange; Internet – PUF, Que sais-je? N° 3073 – ISBN: 2-13-053190-3

Ferguson Niels, Schneier Bruce, Practical Cryptography, Wiley, 2003, ISBN 0-471-22357-3

Ghernaouti-Hélie Solange; Internet & Sécurité – PUF Que sais-je? N° 3609 – ISBN: 2-13-051010-8

Ghernaouti-Hélie Solange; Sécurité informatique et réseaux, cours et exercices corrigés – Dunod 2006.

Panko Raymond, Sécurité des systèmes d'information et des réseaux, Pearson Education (version française), 2004

Poulin Guillaume, Soyer Julien, Trioullier Marc-Éric, Sécurité des architectures Web, «ne pas prévoir c'est déjà gémir», Dunod, 2004.

Schneier Bruce, Beyond Fear, Thinking Sensibly About Security In An Uncertain World, Copernicus Books, 2003, ISBN 0-387-02620-7

Schneier Bruce, Secrets et mensonges, la sécurité numérique dans un monde en réseau, Vuibert, (version française) 2001, ISBN 2-711786-846

Schneier Bruce, Cryptographie Appliquée, Algorithmes, protocoles et codes source en C, 2ème édition, Vuibert, 2001, ISBN 2-7117-8676-5 – version française de Schneier Bruce, Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition, Wiley, 1996, ISBN 0-471-11709-9

Singh Simon, Histoire des codes secrets, JC Lattès, 1999, ISBN 2-7096-2048-0

Stallings William, Cryptography And Network Security, principles and practice, Prentice Hall, 1999, ISBN 0-13-869017-0

Stallings William, Network And Internetwork Security, principles and practice, Prentice Hall, 1995, ISBN 0-13-180050-7

Stallings William, Network Security Essentials, applications and standards, Prentice Hall, 2000, ISBN 0-13-016093-8

Sitios de referencia

Sitios en francés:

Sitio web del Primer Ministro (F): http://www.premier-ministre.gouv.fr

Ver especialmente el apartado *Technologie de l'information dans la thématique: communication.*

Sitio web http://www.internet.gouv.fr: : dedicado al desarrollo de la sociedad de la información.

Portal de la Administración francesa: http://www.service-public.gouv.fr. A partir de este sitio se puede llegar a todos los servicios en línea y especialmente en el apartado «*se documenter*»

Sitio del servicio público relativo al derecho: http://www.legifrance.gouv.fr

Sitio de la dirección de la documentación francesa: http://www.ladocfrancaise.gouv.fr

Sitio web http://www.foruminternet.org/: : Espacio de información y de debate sobre el derecho y sobre Internet y las redes

Sitio de la Comisión Nacional de la Informática y de las Libertades (F): http://www.cnil.fr

Sitio de la Oficina Central de la lucha contra la delincuencia en las tecnologías de la información y de la comunicación (F): http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic

Observatorio de seguridad de los sistemas de información y de las redes: http://www.ossir.org

Sitio del Clusif: www.clusif.asso.fr. Panorama de la ciberdelincuencia:

https://www.clusif.asso.fr/fr/production/ouvrages/

Otros sitios web de interés

Sitio web del CERT: www.cert.org

Sitio web del NIST: http://www.nist.gov; sitio del National Institute of Standards and Technology (NIST), (*Instituto Nacional de Normas y Tecnología*) de Estados Unidos

Sitio web de la NSA: http://www.nsa.gov; sitio de la National Security Agency (*Agencia Nacional de Seguridad*) de Estados Unidos

Sitio web del CSE: http://www.cse.dnd.ca; Centro de la Seguridad de las Telecomunicaciones de Canadá

Sitio web del CESG: http://www.cesg.gov.uk; de la National Technical Authority for Information Assurance (*Autoridad Nacional Técnica para la Seguridad de la Información*) del Reino Unido

Sitio web del BSI: http://www.bsi.bund.de. El BSI es la Oficina Federal de la Seguridad de la Información de Alemania. Este sitio web está en inglés y en alemán

Sitio web del DSD: http://www.dsd.gov.au; sitio del Defence Signals Directorate (*Dirección de Señales de Defensa*) existente en Australia y Nueva Zelanda. Este sitio web se dedica a la vigilancia digital y a la seguridad de la información

El National White Collar Crime Center (*Centro Nacional contra la delincuencia entre los empleados*): IFCC – Internet fraud complaint Center (*Centro de quejas sobre fraude en Internet*): http://www1.ifccfbi.gov/index.asp; Internet Fraud (*Fraude en Internet*) – Crime Report (*Informes sobre delitos*) – 2004 http://www1.ifccfbi.gov/strategy/2004_IC3Report.pdf

Boletines de noticias

Criptograma de de Bruce Schneier [schneier@COUNTERPANE.COM]
CRYPTO-GRAM-LIST@LISTSERV.MODWEST.COM

Info carta del Foro de derechos sobre Internet
infolettre@listes.foruminternet.org

US-CERT Security Bulletins (*Boletines de seguridad de US-CERT*) [security-bulletins@us-cert.gov]
security-bulletins@us-cert.gov

Carta informativa de la ciberpolicía http://cyberpolice.over-blog.com/cyberpolice.over-blog.com [newsletter@over-blog.com]

Anexo F – Directrices sobre la seguridad de los sistemas y redes de información para una cultura de la seguridad – OCDE –

Prefacio

El grado de utilización de los sistemas y redes de información y el entono de las tecnologías de la información en su conjunto han evolucionado espectacularmente desde 1992, fecha en la que la OCDE publicó sus *Líneas directrices sobre seguridad de los sistemas de información*. Esta evolución constante presenta ventajas significativas pero exige asimismo que los gobiernos, las empresas y otras entidades, así como los usuarios individuales que desarrollan, poseen, suministran, gestionan, mantienen y utilizan los sistemas y redes de información (partes interesadas), dediquen mucha más atención a la seguridad.

Los ordenadores personales, cada vez más potentes, las tecnologías convergentes y la enorme difusión de Internet han sustituido a los antiguos sistemas autónomos de capacidad limitada conectados normalmente en redes cerradas. Hoy en día, las partes interesadas están cada vez más interconectadas y estas conexiones superan las fronteras nacionales. Además, Internet soporta infraestructuras vitales tales como la energía, los transportes y las actividades financieras y desempeña un papel primordial en el modo en que las empresas ejecutan sus actividades, los gobiernos prestan servicios a los ciudadanos y a las empresas y los ciudadanos se comunican e intercambian información. La naturaleza y el tipo de tecnologías que constituyen la infraestructura de comunicación y de información también han evolucionado notablemente. El número y naturaleza de dispositivos de acceso a esta infraestructura se ha multiplicado y diversificado, incluyendo terminales de acceso fijo, inalámbrico y móvil. Un porcentaje cada vez mayor de los accesos se efectúa por medio de conexiones «permanentes». En consecuencia, la naturaleza, el volumen y el carácter sensible de la información intercambiada han aumentado de manera significativa.

Debido al incremento de la conectividad, los sistemas y redes de información están cada vez más expuestos a amenazas y vulnerabilidades más numerosos y diversos, lo que plantea nuevos problemas de seguridad. Estas directrices van dirigidas pues al conjunto de las partes interesadas en la nueva sociedad de la información y plantean la necesidad de una toma de conciencia y una comprensión de las acuciantes cuestiones de seguridad, así como la necesidad de desarrollar una «cultura de la seguridad».

F.1 Hacia una cultura de la seguridad

Estas directrices responden a un entorno en constante evolución y apelan al desarrollo de una cultura de la seguridad – lo que significa prestar una gran atención a la seguridad durante el desarrollo de los sistemas de información y de las redes y adoptar nuevos modos de pensar y un nuevo comportamiento cuando se utilizan sistemas y redes de información así como en el marco de los intercambios que en ellos se producen. Las directrices marcan una ruptura clara con la época en la que la seguridad no intervenía más que de manera incidental en la concepción y utilización de las redes y sistemas de información. Las partes interesadas son cada vez más dependientes de los sistemas de información, de las redes y de los servicios vinculados a aquéllas, que deben ser totalmente fiables y seguros. Sólo un planteamiento que tenga debidamente en cuenta los intereses de todas las partes interesadas y la naturaleza de los sistemas, redes y servicios afines, puede permitir garantizar una seguridad eficaz.

Cada parte interesada tiene una misión importante que desempeñar para garantizar la seguridad. Las partes interesadas, en función de sus respectivas misiones, deben ser sensibles a los riegos vinculados a la seguridad y ser conscientes de las medidas preventivas aplicables, deben asumir su responsabilidad y adoptar medidas para mejorar la seguridad de los sistemas y redes de información.

La instauración de una cultura de la seguridad necesitará al mismo tiempo un impulso y una gran participación y deberá traducirse en el refuerzo de la prioridad otorgada a la planificación y gestión de la seguridad, así como en la comprensión de la exigencia de seguridad por parte de todos los participantes. Las cuestiones de seguridad deben despertar la preocupación y el sentido de la responsabilidad a todos los niveles del gobierno y de las empresas y en todas las partes interesadas. Estas directrices constituyen una base para los trabajos encaminados a instaurar una cultura de seguridad en el conjunto de la sociedad. Las partes interesadas deberán asimismo intentar que la seguridad llegue a formar parte integral de la concepción y de la utilización de todos los sistemas y redes de información. Estas directrices proponen que todas las partes interesadas adopten y fomenten una «cultura de la seguridad» que guíe la reflexión, decisión y acción en torno al funcionamiento de los sistemas y redes de información.

F.2 Fines

El objeto de las directrices es el siguiente:

- Promover entre todas las partes interesadas una cultura de seguridad como medio de protección de los sistemas y redes de información
- Reforzar la sensibilización a los riegos para los sistemas y redes de información, a las políticas, prácticas, medidas y procedimientos disponibles para afrontar estos riesgos, así como a la necesidad de adoptarlos y ponerlos en práctica.
- Promover entre todas las partes interesadas una mayor confianza en los sistemas y redes de información y en la manera en que éstos se instalan y utilizan.
- Crear un marco general de referencia que ayude a las partes interesadas a comprender la naturaleza de los problemas vinculados a la seguridad y a respetar los valores éticos en la elaboración e implementación de políticas, prácticas, medidas y procedimientos coherentes para la seguridad de los sistemas y redes de información.
- Promover entre todas las partes interesadas la cooperación y compartición de informaciones oportunas para la elaboración e implementación de políticas, prácticas, medidas y procedimientos para la seguridad.
- Promover la toma en consideración de la seguridad como objetivo importante entre todas las partes interesadas asociadas a la elaboración e implementación de normas.

F.3 Principios

Los nueve principios expuestos a continuación se complementan y deben ser considerados conjuntamente. Se dirigen a las partes interesadas a todos los niveles, entre ellos el político y el operacional. Las responsabilidades de las partes interesadas contempladas en estas directrices varían según el papel de aquéllas. Todas las partes interesadas pueden beneficiarse de acciones de sensibilización, educación, compartición de informaciones y formación destinadas a facilitar una mejor comprensión de las cuestiones de seguridad y la adopción de mejores prácticas en este ámbito. Los esfuerzos destinados a reforzar la seguridad de los sistemas y redes de información deben respetar los valores de una sociedad democrática, en particular la necesidad de la libre circulación sin cortapisas de la información y de los principios básicos de respeto de la vida privada de los individuos[62].

[62] Además de las presentes directrices sobre seguridad, la OCDE ha elaborado una serie de recomendaciones complementarias sobre las directrices relativas a otros aspectos importantes de la sociedad mundial de la información. Éstas se centran en la vida privada (*Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, 1980) y en la criptografía (*Lignes directrices régissant la politique de cryptographie*, OCDE, 1997). Las presentes directrices sobre seguridad deben leerse junto con las otras directrices mencionadas.

1) Sensibilización

Las partes interesadas deben concienciarse de la necesidad de garantizar la seguridad de los sistemas y redes de información y de las acciones que pueden emprender para reforzar la seguridad.

La sensibilización a los riegos y a las medidas correctivas disponibles constituye la primera línea defensiva para garantizar la seguridad de los sistemas y redes de información. Los sistemas y redes de información pueden quedar expuestos a riegos tanto internos como externos. Las partes interesadas deben comprender que los fallos de seguridad pueden afectar gravemente a los sistemas y redes bajo su control pero también, debido a la interconectividad e interdependencia, a los de un tercero. Las partes interesadas deben prestar la máxima atención a la configuración de sus sistemas, las actualizaciones disponibles para estos últimos y el lugar que ocupan en las redes, las prácticas óptimas que pueden aplicar para reforzar la seguridad, así como las necesidades de las otras partes interesadas.

2) Responsabilidad

Las partes interesadas son responsables de la seguridad de los sistemas y redes de información.

Las partes interesadas son tributarias de los sistemas y redes de información interconectadas, tanto locales como mundiales. Deben comprender su responsabilidad en la seguridad de estos sistemas y redes y dar cuenta individualmente en función del papel que les corresponde. Deben examinar y evaluar periódicamente sus propias políticas, prácticas, medidas y procedimientos para garantizar su adaptación al entorno. Aquellos que desarrollan, conciben y suministran productos y servicios deben tener en cuenta la seguridad de los sistemas y redes y difundir informaciones apropiadas, principalmente las actualizaciones pertinentes, de modo que los usuarios puedan comprender mejor las funciones de seguridad de los productos y servicios y sus responsabilidades en la materia.

3) Reacción

Las partes interesadas deben actuar con prontitud en un espíritu de cooperación para prevenir, detectar y responder a los incidentes de seguridad.

Debido a la interconectividad de los sistemas y redes de información y la facilidad con que los daños pueden propagarse rápida y masivamente, las partes interesadas deben reaccionar con prontitud en un espíritu de cooperación a los incidentes de seguridad. Deben intercambiar sus informaciones sobre las amenazas y vulnerabilidades de manera apropiada y aplicar procedimientos para una cooperación rápida y eficaz destinada a prevenir, detectar los incidentes de seguridad y responder a los mismos. Cuando esto está permitido puede implicar intercambios de información y cooperación transfronteriza.

4) Ética

Las partes interesadas deben respetar los intereses legítimos de las otras partes interesadas.

Los sistemas y redes de información son omnipresentes en nuestras sociedades y las partes interesadas deben ser concientes del perjuicio que pueden causar a un tercero por acción u omisión. Así pues, una conducta ética resulta indispensable; por este motivo las partes interesadas deben esforzarse en elaborar y adoptar prácticas ejemplares y promover comportamientos que tengan en cuenta los imperativos de seguridad y respeten los intereses legítimos de las otras partes interesadas.

5) Democracia

La seguridad de los sistemas y redes de información debe ser compatible con los valores fundamentales de una sociedad democrática.

La puesta en práctica de la seguridad debe respetar los valores reconocidos por las sociedades democráticas y, especialmente, la libertad de intercambio de pensamientos e ideas, la libre circulación de la información, la confidencialidad de la información y de las comunicaciones, la adecuada protección de las informaciones de carácter personal y la apertura y transparencia.

6) Evaluación de los riesgos

Las partes interesadas deben evaluar los riesgos.

La evaluación de los riesgos permite poner al descubierto las amenazas y vulnerabilidades y debe ser suficientemente amplia para abarcar todos los factores internos y externos de importancia tales como la tecnología, los factores físicos y humanos, las políticas y servicios de terceros con repercusión sobre la seguridad. La evaluación de los riesgos permitirá determinar el nivel aceptable de riesgos y facilitará la selección de medidas de control adecuadas para gestionar el riesgo de perjuicios posibles para los sistemas y redes de información teniendo en cuenta la naturaleza e importancia de la información a proteger. La evaluación de los riesgos debe tener en cuenta el perjuicio a los intereses de terceros o el causado por un tercero que hace posible la creciente interconexión de los sistemas de información.

7) Concepción y puesta en práctica de la seguridad

Las partes interesadas deben integrar la seguridad como elemento esencial de los sistemas y redes de información.

Los sistemas, redes y políticas deben concebirse, ponerse en práctica y coordinarse de manera adecuada para optimizar la seguridad. Una de las direcciones más importantes, aunque no exclusiva, de este esfuerzo debe ser la concepción y adopción de medidas de protección y soluciones adecuadas a fin de prevenir o limitar los posibles perjuicios vinculados a las vulnerabilidades y amenazas identificadas. Las medidas de protección y las soluciones deben ser a la vez técnicas y no técnicas y proporcionadas al valor de la información de los sistemas y redes de información de la organización. La seguridad debe constituir un elemento fundamental de todos los productos, servicios, sistemas y redes y formar parte integral de la concepción y arquitectura de los sistemas. Para el usuario final, la concepción e implementación de la seguridad consiste esencialmente en seleccionar y configurar productos y servicios para sus sistemas.

8) La gestión de la seguridad

Las partes interesadas deben adoptar un planteamiento global de la gestión de la seguridad.

La gestión de la seguridad debe basarse en la evaluación de los riegos y ser dinámica y global a fin de cubrir todos los niveles de actividad de las partes interesadas y todos los aspectos de sus operaciones. Asimismo debe incluir, anticipadamente, respuestas a las amenazas emergentes y contemplar la prevención, detección y resolución de incidentes, la recuperación de los sistemas, el mantenimiento permanente, el control y la auditoría. Las políticas de seguridad de los sistemas y redes de información, prácticas, medidas y procedimientos en materia de seguridad deben coordinarse e integrarse para crear un sistema coherente de seguridad. Las exigencias de la gestión de la seguridad dependen del grado de participación, del papel de la parte interesada, de los riesgos en juego y de las características del sistema.

9) Revaluación

Las partes interesadas deben examinar y revaluar la seguridad de los sistemas y redes de información e introducir las modificaciones oportunas en sus políticas, prácticas, medidas y procedimientos de seguridad.

Continuamente se descubren vulnerabilidades y amenazas nuevas o nuevas versiones de las existentes. Todas las partes interesadas deben revisar, revaluar y modificar continuamente todos los aspectos de la seguridad para hacer frente a estos riegos en evolución.

Recomendación del Consejo sobre las directrices en materia de seguridad de los sistemas y redes de información para una cultura de la seguridad

EL CONSEJO,

Visto el Convenio de la Organización de Cooperación y Desarrollo Económicos de fecha 14 de diciembre de 1960, y especialmente sus Artículos 1 b), 1 c), 3 a) et 5 b);

Vista la Recomendación del Consejo relativa a las directrices sobre la protección de la vida privada y los flujos transfronterizos de datos de carácter personal, de fecha 23 de septiembre de 1980 [C(80)58(Final)];

Vista la Declaración sobre los flujos transfronterizos de datos adoptada por los gobiernos de los Países Miembros de la OCDE el 11 de abril de 1985 [C(85) 139, Anexo];

Vista la Recomendación del Consejo relativa a las directrices sobre la política de criptografía de fecha 27 de marzo de 1997 [C(97)62/FINAL];

Vista la Declaración Ministerial relativa a la protección de la vida privada sobre las redes mundiales, de fecha 7-9 de diciembre de 1998 [C(98)177/FINAL, Anexo];

Vista la Declaración Ministerial sobre la autenticación para el comercio electrónico, de fechas 7-9 de diciembre de 1998 [C(98)177/FINAL, Anexo];

Reconociendo que los sistemas y redes de información se utilizan cada vez más y adquieren un valor creciente para los gobiernos, empresas, demás organizaciones y usuarios individuales;

Reconociendo que el papel cada vez más importante que desempeñan los sistemas y redes de información en la estabilidad y eficiencia de las economías nacionales y de los intercambios internacionales, así como en la vida social, cultural y política y la acentuación de la dependencia de las mismas imponen esfuerzos particulares para proteger y promover la confianza que les rodea;

Reconociendo que los sistemas y redes de información y su expansión a escala mundial vienen acompañados de nuevos riesgos cada vez más numerosos;

Reconociendo que los datos e informaciones conservadas o transmitidas sobre los sistemas y redes de información quedan expuestos a amenazas debido a los diversos medios de acceso sin autorización, a la utilización, apropiación abusiva, alteración, transmisión de código malicioso, denegación de servicio o destrucción que exigen medidas de protección apropiadas;

Reconociendo que es importante sensibilizar más sobre los riesgos que afectan a los sistemas y redes de información así como sobre las políticas, prácticas, medidas y procedimientos disponibles para afrontar dichos riesgos, y fomentar comportamientos apropiados en la medida en que constituyen una etapa esencial en el desarrollo de una cultura de la seguridad;

Reconociendo que conviene revisar las políticas, prácticas, medidas y procedimiento actuales para contribuir a que respondan adecuadamente a los desafíos en constante evolución que plantean las amenazas a las que quedan expuestas los sistemas y redes de información;

Reconociendo que es interés común la promoción de la seguridad de los sistemas y redes de información por una cultura de la seguridad que fomenta la coordinación y cooperación internacional adecuada a fin de responder a los desafíos planteados por los perjuicios que pueden provocar los fallos de seguridad de las economías nacionales, intercambios internacionales y a la participación en la vida social, cultural y política;

Reconociendo por otra parte que las *Directrices sobre la seguridad de los sistemas y redes de información: hacia una cultura de la seguridad*, que figuran como Anexo a la Recomendación, son de aplicación voluntaria y no afectan a los derechos soberanos de los Estados;

Y reconociendo que el objeto de estas directrices no es sugerir que existe una solución única cualquiera en materia de seguridad, ni que haya políticas, prácticas, medidas y procedimientos particulares adaptados a una situación determinada, sino más bien ofrecer un marco más general de principios de modo que se favorezca una mejor comprensión del modo en que las partes interesadas pueden al mismo tiempo beneficiarse del desarrollo de una cultura de la seguridad y contribuir a la misma;

PRECONIZA la aplicación de estas *Directrices sobre la seguridad de los sistemas y redes de información: hacia una cultura de la seguridad* por los gobiernos, empresas, demás organizaciones y usuarios individuales que desarrollan, poseen, suministran, gestionan, mantienen y utilizan los sistemas y redes de información;

RECOMIENDA a los países Miembros:

Establecer nuevas políticas, prácticas, medidas y procedimientos o modificar las existentes para reflejar y tener en cuenta las *Directrices sobre la seguridad de los sistemas y redes de información: hacia una cultura de la seguridad*, adoptando y promoviendo una cultura de la seguridad, conforme a las citadas directrices;

Emprender acciones de consulta, de coordinación y de cooperación a nivel nacional e internacional para la puesta en práctica de estas directrices;

Difundir las directrices a todos los sectores público y privado, especialmente a los gobiernos, empresas, demás organizaciones y usuarios individuales, para promover una cultura de la seguridad y fomentar en todas las partes interesadas la asunción de una actitud responsable y la adopción de las medidas necesarias en función de los papeles que desempeñan;

Poner estas directrices a disposición de los países que no son miembros, con la mayor rapidez posible y como mejor corresponda;

Volver a examinar las directrices cada cinco años, a fin de promover la cooperación internacional sobre las cuestiones vinculadas a la seguridad de los sistemas y redes de información;

ENCARGA al Comité de la política de información, de informática y de comunicaciones de la OCDE a conceder su apoyo a la puesta en práctica de estas directrices.

La presente Recomendación viene a sustituir la Recomendación del Consejo relativa a las directrices sobre la seguridad de los sistemas de información de 26 de noviembre de 1992 [C(92)188/FINAL].

Evolución histórica de este procedimiento

Las directrices sobre seguridad se concluyeron en 1992 y se volvieron a examinar en 1997. El examen actual emprendido en 2001 por el Grupo de Trabajo sobre seguridad de la información y vida privada (GTSIVP), en el marco del mandato otorgado por el Comité de política de información, informática y comunicaciones (PIIC) y acelerado como consecuencia de la tragedia del 11 de septiembre.

La redacción la emprendió un Grupo de Expertos del GTSIVP reunido en Washington DC, los días 10 y 11 de diciembre de 2001, en Sydney los días 12 y 13 de febrero de 2002 y en París los días 4 y 6 de marzo de 2002. El GTSIVP se reunió los días 5 y 6 de marzo de 2002, 22 y 23 de abril de 2002 y 25 y 26 de junio de 2002.

Las presentes *Directrices de la OCDE sobre seguridad de los sistemas y redes de información: hacia una cultura de la seguridad* ha sido adoptadas como Recomendación del Consejo de la OCDE con ocasión de su 1037ª sesión de 25 de julio de 2002.