CAPÍTULO 7: CONCEPTOS DE SEGURIDAD

Nuestro proyecto se implementa en un marco de operaciones de comercio electrónico. Por lo tanto requerimos un modelo que nos asegure que las operaciones que intervienen en él sean lo bastantes seguras como para no comprometer el proceso. Para ello, en este capítulo, definimos un modelo que marca las pautas para conseguir servicios seguros. Para introducir este tema expondremos un modelo genérico que definirá los conceptos involucrados.

En una sección posterior, limitaremos dicho modelo genérico para poder ajustarlo al comercio electrónico. Precisamente eso es lo que buscamos en el proyecto: dar seguridad a un sistema que implementa un servicio de comercio electrónico.

7.1.- Los servicios de seguridad

El documento de **ISO** que describe el *Modelo de Referencia OSI*, presenta en su *Parte 2* una *Arquitectura de Seguridad*. Según esta arquitectura, para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes **servicios de seguridad**:

- ***Autentificación de entidad par***: Este servicio autentifica la fuente de una unidad de datos. La autentificación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autentificar la una o la otra.

- ***Control de acceso***: Este servicio se utiliza para evitar el uso no autorizado de recursos.

- ***Confidencialidad de datos***: Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

- ***Integridad de datos***: Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor.

- ***No repudio***: Este servicio proporciona la prueba ante una tercera parte de que cada una de las entidades comunicantes han participado en una comunicación. Puede ser de dos tipos:

    - **Con prueba de origen**: Cuando el destinatario tiene prueba del origen de los datos.

    - **Con prueba de entrega**: Cuando el origen tiene prueba de la entrega íntegra de los datos al destinatario deseado.

Para proporcionar estos servicios de seguridad es necesario incorporar en los niveles apropiados del *Modelo de Referencia OSI* los siguientes **mecanismos de seguridad**:

- **Cifrado**: El cifrado puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar extremo a extremo o individualmente a cada enlace del sistema de comunicaciones.

  El mecanismo de cifrado soporta el servicio de confidencialidad de datos al tiempo que actúa como complemento de otros mecanismos de seguridad.

- **Firma digital**: Se puede definir la firma digital como el conjunto de datos que se añaden a una unidad de datos para protegerlos contra la falsificación, permitiendo al receptor probar la fuente y la integridad de los mismos. La firma digital supone el cifrado, con una componente secreta del firmante, de la unidad de datos y la elaboración de un valor de control criptográfico.

  La firma digital descrita por **ITU** y **OSI** en el *Entorno de Autentificación del Directorio* utiliza un esquema criptográfico asimétrico. La firma consiste en una cadena que contiene el resultado de cifrar con **RSA** aplicando la clave privada del firmante, una versión comprimida, mediante una función *hash* unidireccional y libre de colisiones, del texto a firmar.

  Para **verificar la firma**, el receptor descifra la firma con la clave pública del emisor, comprime con la función *hash* el texto original recibido y compara el resultado de la parte descifrada con la parte comprimida. Si ambas coinciden, el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.

  El mecanismo de firma digital soporta los servicios de integridad de datos, autentificación de origen y no repudio con prueba de origen. Para proporcionar el servicio de no repudio con prueba de entrega es necesario forzar al receptor a enviar al emisor un recibo firmado digitalmente.

- **Control de acceso**: Este mecanismo se utiliza para autentificar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a los recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el emisor está autorizado a comunicarse con el receptor y/o a usar los recursos de comunicación solicitados. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

El mecanismo de control de acceso soporta el servicio de control de acceso.

- **Integridad de datos**: Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad.

  Para proporcionar la integridad de una **unidad de datos** la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una información suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

  Para proporcionar integridad a una **secuencia de unidades de datos** se requiere, adicionalmente, alguna forma de ordenación explícita, tal como la numeración de secuencia, un sello de tiempo o un encadenamiento criptográfico.

  El mecanismo de integridad de datos soporta el servicio de integridad de datos.

- **Intercambio de autentificación**. Existen dos grados en el mecanismo de autentificación:

  - **Autentificación simple**: El emisor envía su nombre distintivo y una contraseña al receptor, el cual los comprueba.

  - **Autentificación fuerte**: Utiliza las propiedades de los criptosistemas de clave pública. Cada usuario se identifica por un nombre distintivo y por su clave secreta. Cuando un segundo usuario desea comprobar la autenticidad de su interlocutor deberá comprobar que éste está en posesión de su clave secreta, para lo cual deberá obtener su clave pública.

  Para que un usuario confíe en el procedimiento de autentificación, la clave pública de su interlocutor se tiene que obtener de una fuente de confianza, a la que se denomina Autoridad de Certificación. La **Autoridad de Certificación** utiliza un algoritmo de clave pública para certificar la clave pública de un usuario produciendo así un certificado.

  Un **certificado** es un documento firmado por una Autoridad de Certificación, válido durante el período de tiempo indicado, que asocia una clave pública a un usuario.

El mecanismo de intercambio de autentificación se utiliza para soportar el servicio de autentificación de entidad par.

7.2.- Seguridad en comercio electrónico

La seguridad, hasta ahora, nunca ha sido uno de los principales puntos a la hora de tener en cuenta el desarrollo y la evolución de Internet.

Parece que este detalle tiende a cambiar, y que la seguridad enfocada al comercio electrónico busca la seguridad de los datos de sus usuarios. La incorporación de mecanismos, técnicas y algoritmos adecuados para realizar transacciones electrónicas se hace necesaria para evitar los riesgos a los que nos exponemos.

Se puede hablar en este sentido de cuatro aspectos básicos de seguridad que conciernen al comercio electrónico: **autentificación**, **confidencialidad**, **integridad** y el **no-repudio**

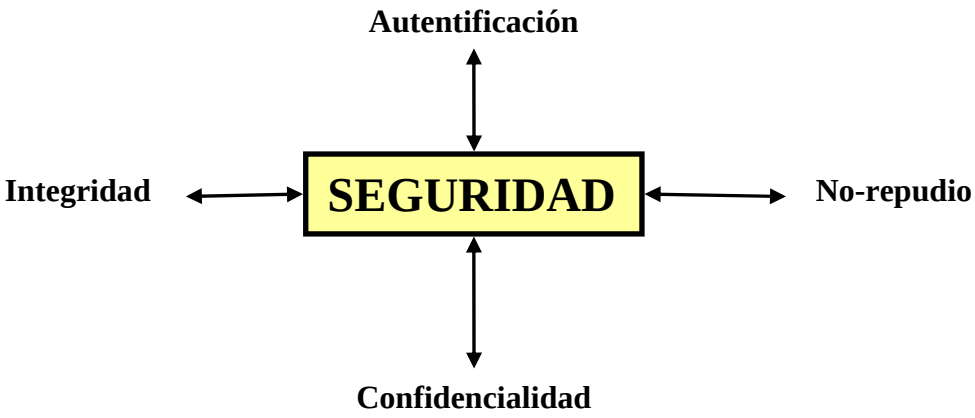

Figura 7. 1: Aspectos básicos de seguridad

7.2.1.- Autentificación

La **autentificación** es el proceso de verificar formalmente la identidad de las entidades participantes en una comunicación o intercambio de información. Por entidad se entiende tanto personas, como procesos o computadoras.

De otra manera, se puede decir que es el proceso por el que se comprueba la identidad de alguien o algo, para ver si es lo que dice ser. Ese “alguien” o “algo” se denomina **principal**. La autentificación requiere pruebas de identidad, denominadas **credenciales**. Por ejemplo, una aplicación cliente puede presentar una contraseña como sus credenciales. Si la aplicación cliente presenta las credenciales correctas, se asume que es quien dice ser.

Existen varias formas de poder autentificarse:

- basada en claves
- basada en direcciones
- criptográfica

De estas tres posibilidades la más segura es la tercera, ya que en el caso de las dos primeras es posible que alguien escuche la información enviada y pueda suplantar la identidad del emisor de información.

Desde otro punto de vista se puede hablar de **formas de autentificarse**, como puede ser a través de la biometría (huellas digitales, retina del ojo, la voz...), por medio de passwords o claves, y por último utilizando algo que poseamos, como un certificado digital.

Se llama **autentificación fuerte** a la que utiliza al menos dos de las tres técnicas mencionadas en el párrafo anterior, siendo bastante frecuente el uso de la autentificación biométrica, que como se indicó antes se basa en la identificación de personas por medio de algún atributo físico.

7.2.2.- Confidencialidad

La **confidencialidad** es la propiedad de la seguridad que permite mantener en secreto la información para que sólo los usuarios autorizados pueden manipularla. Igual que antes, los usuarios pueden ser personas, procesos, programas...

Para evitar que alguien no autorizado pueda tener acceso a la información transferida que recorre la Red, se utilizan técnicas de **encriptación** o **codificación de datos**.

Hay que mantener una cierta coherencia para determinar cuál es el grado de confidencialidad de la información que se está manejando, para así evitar un esfuerzo suplementario a la hora de decodificar una información previamente codificada.

7.2.3.- Integridad

La **integridad de la información** corresponde a lograr que la información transmitida entre dos entidades no sea modificada por un tercero y esto se logra mediante la utilización de firmas digitales.

Mediante una **firma digital** se codifican los mensajes a transferir, de forma que una función, denominada *hash*, calcula un resumen de dicho mensaje y se añade al mismo.

La **validación de la integridad del mensaje** se realiza aplicándole al original la misma función y comparando el resultado con el resumen que se añadió al final del mismo cuando se calculó por primera vez antes de enviarlo.

Mantener la integridad es importante para verificar que en el tiempo de viaje de la información por la Red, entre el sitio emisor y receptor, nadie no autorizado, ha modificado el mensaje.

7.2.4.- No-repudio

Los servicios de **no-repudio** ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información recibida.

Con este aspecto conseguimos que una vez que alguien ha mandado un mensaje no pueda renegar de él, es decir, no pueda negar que es el autor del mensaje. Para el comercio electrónico es importante ya que garantiza la realización de las transacciones para las entidades participantes.

Se aplica en ambos lados de la comunicación, tanto para no poder rechazar la autoría de un mensaje, como para no poder negar su recepción.

Es necesario identificar la información que debe conocer cada una de las entidades participantes en el proceso de comercio electrónico y con ello permitir la privacidad de forma fraccionada a las partes autorizadas para su uso.

7.2.5.- Conclusiones a la seguridad en comercio electrónico

Como conclusión podemos indicar que la combinación de estos cuatro aspectos mencionados, **autentificación**, **confidencialidad**, **integridad** y **no-repudio**, garantiza en cierto grado la seguridad en las transacciones electrónicas.

Conocer y aplicar conceptos, técnicas y algoritmos para implementar un sistema de seguridad es imprescindible para minimizar riesgos y así poder asegurar al usuario que el comercio electrónico es un mecanismo seguro en el cual puede confiar siempre que se trate con la delicadeza que requiere.