UD1: CONCEPTOS BÁSICOS EN CIBERSEGURIDAD

CURSO DE ESPECIALIZACIÓN:
Ciberseguridad en entornos de las tecnologías de la información

Profesor:
Javier Morillas Zafra

Índice

1. Conceptos Básicos

1.1 Definición y alcance de la ciberseguridad

La seguridad en una empresa se tiene que dar en dos ámbitos:

- **Seguridad física:** su objetivo principal es proteger a la organización frente accesos no autorizados y ataques físicos a las instalaciones y equipos de la empresa.
- **Seguridad lógica:** su objetivo principal es proteger la información que maneja la empresa en medios digitales. Para ello se pueden tomar las siguientes acciones:
    - Limitar el acceso a programas a ficheros, por ejemplo, dotando de privilegios a los usuarios.
    - Gestionar la autorización de los usuarios en el acceso a la información.
    - Controlar la información que entra y sale del sistema de información.

La ciberseguridad se encarga de la seguridad lógica en las empresas. Para ello, define **un conjunto de medios y técnicas para proteger de ataques maliciosos a computadoras, servidores, datos, equipos electrónicos y datos.** Su finalidad, por tanto, será desarrollar **acciones y normas** que minimicen el riesgo de ataque centrándose en tres ejes principales:

- La **infraestructura** que soporta la información. Cualquier dispositivo electrónico con conexión a internet o algún tipo de red, disponen de accesos (puertas) mediante las cuales podrían sufrir algún tipo de ataque.
- A los **usuarios** que explotan la información. Hay que dotar a la organización de herramientas que permitan definir políticas de acceso a datos, privilegios en acciones, etc.
- A la **información**

La ciberseguridad tiene tres objetivos claros: **prevención, detención y recuperación.**

1.1.1 Ciberseguridad preventiva

La ciberseguridad se encarga de establecer medios que **garanticen la protección e inaccesibilidad al interior de nuestro dispositivo**.

Se trata del tipo de seguridad informática más común por el sencillo motivo de que la seguridad informática está tan avanzada que en la mayoría de los casos tendrá como **propósito que nuestros dispositivos, software y redes estén blindados ante cualquier tipo de amenaza**.

1.1.2 Ciberseguridad de detención

Ante la posibilidad de convertirnos en víctima de un ataque, es la ciberseguridad la encargada de **descubrir posibles fisuras que realmente pongan nuestros dispositivos y redes en riesgo.**

La detección puede suceder antes de que el ataque se produzca o cuando la amenaza ya esté dentro.

La ciberseguridad de detección es responsable de **descubrir cualquier tipo de acción fraudulenta contra nuestro sistema**: desde un intento de roba de contraseña hasta la extraña manipulación poco natural de la información o accesos sospechosos al sistema.

1.1.3 Ciberseguridad de recuperación

Si a pesar de establecer métodos de prevención y detección, el ataque consigue romper nuestras barreras, entonces adoptamos una estrategia de ciberseguridad de recuperación.

Este tipo de seguridad se encarga de **establecer los métodos para aislar y expulsar la amenaza** mediante los cauces que resulten lo menos dañinos posibles.

También realiza todas las tareas de restauración y recuperación, así como la implantación de nuevos métodos de protección que nos mantengan alerta ante futuros ataques de la misma naturaleza.

1.1.4 Como afecta la ciberseguridad al mundo actual

Como se ha indicado en apartados anteriores, cualquier dispositivo electrónico con conexión a una red o algún puerto de acceso a datos, son susceptibles de ataques malware. Por ello, debemos ser consciente de proteger tanto a empresas como a usuarios.

Es importante tener esto en cuenta para entender lo que es la ciberseguridad, ya que afecta a cada momento de tu vida.

La Ciberseguridad es una rama de la informática que ha ido ganando mayor importancia a medida que la globalización ha ido expandiéndose y las redes de comunicaciones a impregnado todos los ámbitos de la vida.

La seguridad informática a nivel empresarial gana importancia ya que aquí, sus efectos pueden ser especialmente perjudiciales: robo de datos sensibles, secuestro de sistemas, etc.

La seguridad informática tiene por objetivo protegernos de cualquier tipo de ataque, sea de manera activa, siendo consciente de las distintas medidas para evitar un ciberataque o de manera pasiva gracias a los protocolos de actuación que se están ejecutándo sin que nos demos cuenta.

1.2 Áreas de actuación de la ciberseguridad

La ciberseguridad debe estar impregnada en todas las áreas de nuestro entorno laboral. Se debe prestar especial atención a las siguientes áreas de actuación:

- **Políticas de seguridad:** Se deberán establecer políticas de seguridad que deberán cumplir todos los empleados de la empresa. "**Una cadena** es tan fuerte como lo sea el más **débil** de los **eslabones** que la componen" *Thomas Reid.*
- **Identificación de vulnerabilidades:** utilizar pentesting y auditorias para identificar y eliminar vulnerabilidades.
- **Controlar el acceso a la información y dispositivos.**
- **Implementar mecanismos de protección.**
- **Aplicar servicios de seguridad externos.**

1.3 Ubicación de la ciberseguridad

La ciberseguridad agrupa dos campos claramente diferenciados que son la **seguridad de las redes y la seguridad de los sistemas de información**.

Cuando la tecnología es imprescindible se dedican grandes esfuerzos a que funcione. Las empresas tecnológicas desarrollan políticas para evitar incidentes y responder a los improvistos accidentales o intencionados. Una organización no puede permitirse:

- Perder información sensible.
- Parar la actividad de la empresa.

Estas acciones deben realizarse antes de que ocurran los incidentes/accidentes porque sino perderían el sentido de su planificación. En el caso de que ocurran evitar que no sean de gravedad y se pueda recuperar de manera ágil y rápido.

Las estrategias y acciones a tomar deben tomar las empresas deben ser adecuadas a su idiosincrasia y su entorno.

Entre las acciones **preventivas** que se puede realizar una empresa para evitar incidentes podemos destacar:

- **Realizar copias de seguridad**
- **Actualizar el software**
- **Controlar los accesos a los sistemas**
- **Gestionar las altas y bajas de usuarios**
- **Gestionar las contraseñas**
- **Gestionar los incidentes de seguridad**
- **Planificar la recuperación de los sistemas ante desastres**

Las empresas también deben diseñar acciones proactivas para prevenir incidentes o ataques. Esto supone valorar los posibles efectos adversos de los incidentes/ataques tanto a nivel de reputación como económico. Por ello, los esfuerzos en ciberseguridad deben ir dirigidos a las necesidades de la empresa.

La interdependencia de las empresas en su lucha contra la ciberdelincuencia hace que está sea más efectiva generando grandes beneficios:

- Proteger los datos de los clientes exigiendo esa protección a colaboradores, proveedores, etc.
- Cumplir las leyes y normativas dan seguridad a los clientes e inversores.

- Aliarse con otras empresas para crear una sinergia positiva para responder a incidentes y hacer frente común a ciberdelincuentes.

La tecnología avanza y el entorno cambia de manera vertiginosa en los tiempos actuales. La **mejora continua** en el campo de la ciberseguridad es **vital**, esto supone una actualización constante de las políticas de la empresa en materia de seguridad, realizando formación periódica a los empleados y revisar la eficacia de las estrategias.

1.4 Dimensiones de la seguridad y garantías que ofrece

1.4.1 Dimensiones o servicios de seguridad

Existe una frase que se ha hecho famosa dentro del mundo de la seguridad. Eugene Spafford, profesor de ciencias informáticas en la Universidad Purdue (Indiana, EEUU) y experto en seguridad de datos, dijo que "el único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él".

Hablar de seguridad informática en términos absolutos es imposible y por ese motivo se habla mas bien de fiabilidad del sistema, que, en realidad es una relajación del primer término.

Definimos la Fiabilidad como la probabilidad de que un sistema se comporte tal y como se espera de él.

En general, un sistema será **seguro** o **fiable** si podemos garantizar tres aspectos:

- **Confidencialidad:** acceso a la información solo mediante autorización y de forma controlada.
- **Integridad:** modificación de la información solo mediante autorización.
- **Disponibilidad: l**a información del sistema debe permanecer accesible mediante autorización.

Las amenazas y los mecanismos para contrarrestarlas afectan a estas medidas de **forma conjunta**. Si no **coexisten** estas tres medidas de manera simultanea no se garantiza la seguridad de la **información.**

¿Se debe aplicar los mismos recursos a estas dimensiones? No, según el entorno en que se trabaje se dará **prioridad a un aspecto** de la información pero nunca obviando las otras. Por ejemplo, si nuestro entorno es:

- Un servidor de archivos de red prevalecerá la **disponibilidad.**
- Un sistema militar prevalecerá la **confidencialidad de los datos.**
- Un entorno bancario prevalecerá **la integridad de los datos.**

1.4.2 Dimensiones preceptivas

1.4.2.1 Confidencialidad

En general el término 'confidencial' hace referencia a "Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas." (http://buscon.rae.es)

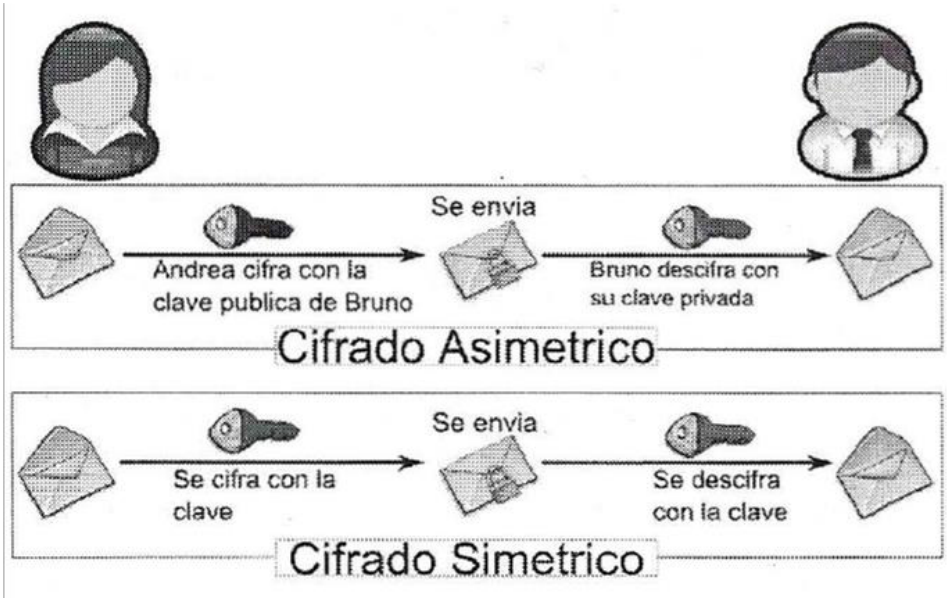
En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos mas típicos es el del ejército de un país. Además, es sabido que los logros mas importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Por otra parte, determinadas empresas a menudo desarrollan diseños que deben proteger de sus competidores. La sostenibilidad de la empresa así como su posicionamiento en el mercado pueden depender de forma directa de la implementación de estos diseños y, por ese motivo, deben protegerlos mediante mecanismos de control de acceso que aseguren la confidencialidad de esas informaciones.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes. Este cifrado puede ser simétrico o asimétrico.



Pero, incluso en esta circunstancia, existe un dato sensible que hay que proteger y es la clave de encriptación. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida y en función del tipo de mecanismo de encriptación utilizado, la clave puede/debe viajar por la red, pudiendo ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.

1.4.2.2 Integridad

En general, el término 'integridad' hace referencia a una cualidad de 'íntegro' e indica "Que no carece de ninguna de sus partes." y relativo a personas "Recta, proba, intachable.".

En términos de seguridad de la información, la integridad hace referencia a la la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información. La información es exacta y completa, es decir, **igual a la original**.

La integridad hace referencia a:

- la integridad de los datos (el volumen de la información)
- la integridad del origen (la fuente de los datos, llamada autenticación)

Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos.

Por ejemplo, cuando un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

1.4.2.3 Disponibilidad

En general, el término 'disponibilidad' hace referencia a una cualidad de 'disponible' y dicho de una cosa "Que se puede disponer libremente de ella o que está lista para usarse o utilizarse."

En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

En términos de seguridad informática “un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados”. Es decir, un sistema es disponible si permite no estar disponible.

Y un sistema 'no disponible' es tan malo como no tener sistema. No sirve.

Como resumen de las bases de la seguridad informática que hemos comentado, podemos decir que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.

Dependiendo del entorno de trabajo y sus necesidades se puede dar prioridad a un aspecto de la seguridad o a otro. En ambientes militares suele ser siempre prioritaria la confidencialidad de la información frente a la disponibilidad. Aunque alguien pueda acceder a ella o incluso pueda eliminarla no podrá conocer su contenido y reponer dicha información será tan sencillo como recuperar una copia de seguridad (si las cosas se están haciendo bien).

En ambientes bancarios es prioritaria siempre la integridad de la información frente a la confidencialidad o disponibilidad. Se considera menos dañino que un usuario pueda leer el saldo de otro usuario a que pueda modificarlo.

1.4.3 Dimensiones recomendables

1.4.3.1 No repudio

El **no repudio o irrenunciabilidad** provee garantía al receptor de una comunicación en cuanto que el mensaje fue originado por el emisor y no por alguien que se hizo pasar por este. Además, previene que el remitente o emisor del mensaje afirme que él no envió el mensaje.

En resumen, el no repudio en seguridad de la información es la **capacidad de demostrar o probar la participación de las partes** (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.

Para **garantizar el no repudio en seguridad informática** se necesitan establecer los siguientes mecanismos:

- **Identificación:** mecanismo o proceso que provee la capacidad de identificar a un usuario de un sistema.
- **Autenticación:** permite verificar la identidad o asegurar que un usuario es quien dice ser.

Se suele aplicar a:

- Contratos formales establecidos de manera telemática.
- Comunicación entre dos partes.
- Transferencia de datos.
- Acciones de los usuarios en un sistema informático.

Tipos de no repudio

1. **En origen:** consiste en garantizar que una persona envió un determinado mensaje. El remitente no puede negar que lo mandó, ya que el destinatario dispone de pruebas del envío.
2. **En destino:** avala que alguien recibió un determinado mensaje. En este caso, el destinatario no podrá rebatir que no lo recibió porque el remitente cuenta con pruebas de la recepción.

La firma electrónica

En seguridad informática y ciberseguridad **uno de los mecanismos más importante de no repudio** es la firma electrónica. Esta es el conjunto de datos asociados a un documento electrónico que identifican al firmante y dotan de validez legal al documento que se firma.

Para garantizar el no repudio, esta firma debe estar **vinculada exclusivamente a la persona que firma e identificarla unívocamente**. Además, la rúbrica debe realizarse a través de un medio electrónico o digital que el firmante tiene bajo su único control y vincularse a los datos que se firman de tal manera que no se puedan modificar sin ser detectados los cambios.

Las firmas deben cumplir los siguientes **requisitos técnicos** para que garanticen el no repudio:

- La clave de firma está asignada a una persona u organización identificable.
- La clave privada está únicamente bajo el control de la persona u organización que firma.

Los distintos tipos de firma electrónica son:

- **Simple:** Se trata de aceptar o rechazar el contenido de un documento, son típicas en las condiciones generales de uso, políticas de seguridad o privacidad…
- **Avanzada OTP:** La persona firmante recibe un código a través de un canal de comunicaciones distinto al de la operativa de firma (p. ej. móvil o correo electrónico) al momento de firmar. Es típica su utilización en compras electrónicas u operaciones de banca electrónica.
- **Biométrica:** La persona firma físicamente en una tablet o dispositivo electrónico. Se utiliza, por ejemplo, en el servicio de correo o transporte de paquetería, en las sucursales bancarias…
- **Certificado digital:** Se firma mediante un certificado que se apoya en un par de claves, una privada y una pública. Hay que aclarar que certificado digital no es lo mismo que firma electrónica. El certificado digital es un documento que **nos identifica en internet para poder realizar trámites online** y que permite la firma electrónica. Ejemplos de firma electrónica serían la firma realizada mediante el DNI electrónico o con los certificados digitales de persona física de la FNMT.

  La firma de un documento con un certificado digital de estas características garantiza que la persona que rubrica el documento es quien dice ser y que lo ha firmado ella. Cabe destacar que es necesaria la debida diligencia en la custodia de estos certificados digitales para que nadie tenga acceso a ellos y los pueda utilizar suplantando la identidad del propietario. Su **funcionamiento** es :

  - Se calcula el valor de *hash* (algoritmo matemático) del documento o mensaje a firmar.
  - El *hash* calculado del documento o mensaje se cifra con la clave privada del certificado digital del emisor.
  - Se transmite junto con el documento o mensaje.
  - El receptor recibe la transmisión y calcula el *hash* del mensaje o documento recibido y descifra con la clave pública el *hash* transmitido. Si coinciden, se garantiza la integridad (el mensaje no ha sido cambiado) y el no repudio, el remitente ha sido quien ha firmado el documento o mensaje.

Existen otros mecanismos de no repudio como el **correo electrónico**, el cual implementa mecanismos de seguimiento que garantizan que un remitente no pueda negar que envió un email y para que el destinatario no pueda decir que no lo ha recibido.

1.4.3.2 Control de acceso

El control de acceso es una forma de seguridad física que administra quién tiene acceso a un área en un momento dado. Los sistemas de control de acceso restringen el acceso a los usuarios autorizados y proporcionan un medio para realizar un seguimiento de quién entra y sale de las áreas seguras.

El control de acceso es una forma de limitar el acceso a un sistema o a recursos físicos o virtuales. En informática, el control de acceso es un proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios a los sistemas, recursos o información.

En los sistemas de control de acceso, los usuarios deben presentar credenciales antes de que se les otorgue acceso. Dentro de los sistemas físicos, estas credenciales pueden tener muchas formas, pero las credenciales que no se pueden transferir brindan la mayor seguridad.

Por ejemplo, una tarjeta clave puede actuar como control de acceso y otorgar al portador acceso a un área clasificada. Debido a que esta credencial se puede transferir o incluso robar, no es una forma segura de manejar el control de acceso.

Un método más seguro para el control de acceso implica la autenticación en dos factores. La persona que desea acceder debe mostrar credenciales y un segundo factor para corroborar la identidad. El segundo factor podría ser un código de acceso, un PIN o incluso una lectura biométrica.

Para la seguridad informática, el control de acceso incluye la autorización, autenticación y auditoría de la entidad que intenta obtener acceso. Los modelos de control de acceso tienen un sujeto y un objeto. El sujeto, el usuario humano, es el que intenta obtener acceso al objeto, generalmente el software.

Una lista de control de acceso contiene una lista de permisos y los usuarios a quienes se aplican estos permisos.

1.5 Protección de la información

Los controles de seguridad son medidas que se aplican en una organización para definir las dimensiones de seguridad de la información. Estos controles afectan al **personal técnico de la organización, empleados y a la organización de la empresa.**

1.5.1 Controles básicos a implantar

1.5.1.1 Autenticación

La Autenticación nos permite la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una contraseña. Pero, cada vez más se están utilizando otras técnicas mas seguras.

Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña)
2. Por lo que uno tiene (una tarjeta magnética)
3. Por lo que uno es (las huellas digitales)

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar mas de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger.

La técnica más usual (aunque no siempre bien) es la autenticación utilizando contraseñas. Este método será mejor o peor dependiendo de las características de la contraseña. En la medida que la contraseña sea más grande y compleja para ser adivinada, más difícil será burlar esta técnica.

Además, la contraseña debe ser confidencial. No puede ser conocida por nadie más que el usuario. Muchas veces sucede que los usuarios se prestan las contraseñas o las anotan en un papel pegado en el escritorio y que puede ser leído por cualquier otro usuario, comprometiendo a la empresa y al propio dueño, ya que la acción/es que se hagan con esa contraseña es/son responsabilidad del dueño.

Para que la contraseña sea difícil de adivinar debe tener un conjunto de caracteres amplio y variado (con minúsculas, mayúsculas y números). El problema es que los usuarios difícilmente recuerdan contraseñas tan elaboradas y utilizan (utilizamos) palabras previsibles (el nombre, el apellido, el nombre de usuario, el grupo musical preferido, ...), que facilitan la tarea a quién quiere entrar en el sistema sin autorización.

Otros mecanismos de autenticación que se utilizan en la actualidad son las tarjetas inteligentes, certificados y firmas digitales, biometría... Todos estos mecanismos están asociados con controles de acceso a los recursos

1.5.1.2 Autorización

La Autorización es el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

El mecanismo o el grado de autorización puede variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.

Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente.

En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos.

Por otra parte, solo se debe dar autorización a acceder a un recurso a aquellos usuarios que lo necesiten para hacer su trabajo, y si no se le negará. Aunque también es posible dar autorizaciones transitorias o modificarlas a medida que las necesidades del usuario varíen.

1.5.1.3 Administración

La Administración es la entidad que establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.

Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema.

La administración de la seguridad informática dentro de la organización es una tarea en continuo cambio y evolución ya que las tecnologías utilizadas cambian muy rápidamente y con ellas los riesgos.

Normalmente todos los sistemas operativos que se precian disponen de módulos específicos de administración de seguridad. Y también existe software externo y específico que se puede utilizar en cada situación.

1.5.1.4 Auditoría y registro

La Auditoría es el mecanismo para la continua vigilancia de los servicios en producción y para ello se recaba información y se analiza.

Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización.

Definimos el Registro como el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo.

Pero auditar y registrar no tiene sentido sino van acompañados de un estudio posterior en el que se analice la información recabada.

Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo.

1.5.1.5 Mantenimiento de la integridad

El Mantenimiento de la integridad de la información es el conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada.

Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos está: uso de antivirus, encriptación y funciones 'hash'

1.5.2 Medidas de ciberseguridad

Las empresas, independientemente de su tamaño, deben preocuparse cada vez más por su ciberseguridad. Deben aplicar una serie de medidas en sus equipos, dispositivos y redes para evitar o dar respuesta a ataques cibernéticos. Y los empleados deben también ser partícipes de esas actuaciones.

Estas son las principales medidas que las empresas deben adoptar en materia de ciberseguridad:

1. **Actualización de dispositivos y equipos**
2. **Elaborar una política de ciberseguridad**
3. **Protegerse frente al malware**
4. **Realizar copias de seguridad**
5. **Establecer controles de acceso**
6. **Proteger la red corporativa**
7. **Proteger la red inalámbrica (WIFI)**
8. **Proteger los dispositivos móviles**
9. **Gestionar los soportes de almacenamiento**
10. **Registrar y analizar la actividad**

1.6 Cibercriminales

La ciberdelincuencia es un sector en auge. Los sistemas informáticos tanto públicos como privados, son constantemente atacados por cibercriminales con dos objetivos claros:

- **Secuestro de la empresa/organización**
- **Robo de información**

1.6.1 Actividades malintencionadas

En la actualidad existen distintas organizaciones que utilizan las tecnologías de la información para crear un mercado de cibercriminalidad. No se necesitan conocimientos especificas para poder llevar a cabo acciones maliciosas, basta con tener dinero para contratar a alguien para que realice el trabajo por nosotros.

Entre las actividades que realizan estas organizaciones podemos destacar las de índole económico para enriquecerse de forma ilícita:

- Robo de datos bancarios.
- Secuestro de información para pedir un rescate.
- Secuestro de sistemas.
- Espionaje industrial. Infección de equipos o creación de botnet(Una botnet es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto) para espiar.

1.6.2 Industria del cibercrimen

El CaaS (Crime as a Service) es una asociación de grupos cuya principal actividad es la cibercriminalidad. Están organizados con medios técnicos y humanos. Ofrecen **servicios delictivos** a cambio de dinero, utilizando para ello, medios tecnológicos más avanzados que los destinados a prevenirlos. Por desgracia, la ciberseguridad siempre esta varios pasos por detrás de los cibercriminales.

Estas organizaciones realizan técnicas de marketing y comunicación para difundir y publicitar sus actividades. El lugar escogido suele ser la **deepweb** pero también pueden publicitarse por plataformas de video y redes sociales. Incluso algunas llegan a los telediarios por la magnitud de sus acciones. Como ejemplo reciente podemos destacar el secuestro del gaseoducto de la empresa Colonial Pipeline, por parte de unos ciberdelincuentes rusos.

Estas organizaciones ganan muchísimo dinero, se estima que sus beneficios rondan el 0,8% del PIB mundial. El cobro lo suelen hacer mediante cuentas falsas o situadas en paraísos fiscales, intermediarios, criptomonedas.

Se aprovechan del anonimato que les proporciona distintas herramientas tecnológicas para esconder su identidad y las acciones que realizan.

- Suplantación de identidad de terceros.
- Proxis anónimos
- Darknet: red Tor, Freenet, I2P o ZeroNet

Los servicios más demandados por el CaaS son:

- **Malware como servicio (MaaS):** diseño de software malicioso a la carta.
- **Fraude en transacciones económicas:** el pago online con tarjetas de crédito robadas o clonadas.
- **Blanqueo online de capitales:** mediante transferencias bancarias a cuentas abiertas con identidad falsa, utilizando muleros, tarjetas prepago,…
- **Delitos relacionados con ingeniería social:** secuestro de cuentas en redes sociales para cobrar un rescate o robar información sensible.
- **Campañas de spam**

- **Campañas de phishing:** robar información sensible (sobre todo datos bancarios) aprovechando la buena fe o desconocimiento tecnológico de las personas.

Ejemplos de precios (Trend Micro)

Servicio	Precio
Códigos de activación de sistemas operativos (Windows) o aplicaciones (MS Office)	**4,4€** (5$)
Intrusión de páginas web	**245€**
Acceso a cuentas de Facebook, Twitter o Gmail	**114€** (130$)
Datos de tarjeta Mastercard	**30€** (35$)
Campaña de spam (1 millón de correos electrónicos)	**8,7€** (10$)
Ataque DDoS	**8,7€** (10$) la hora **131€** (150$) la semana **1.050€** (1.200$) al mes
Infectar un equipo con un virus (troyano)	**4,4€** (5$)

1.6.3 Ciberseguridad como un valor seguro

Las empresas deben percibir el peligro de no estar asegurados en la red y por ello la necesidad de invertir en ciberseguridad. Las empresas deben considerar la ciberseguridad como un valor añadido. Los clientes e inversores suelen tener muy en cuenta la **resiliencia** ante ataques y la confiabilidad.

Para que un cliente confíe en una empresa, esta no debe verse afectada por incidentes de seguridad como:

- Que pongan en peligro la **información propia** del **cliente.**
- **Incumplimiento** de las **obligaciones** con la **administración.**

¿Cómo crear valor con la ciberseguridad?

La creación de valor de la ciberseguridad en clave de negocio, es comprender que las propuestas innovadoras con tecnología se enmarcan en el modelo de los sistemas socio-técnicos. Este marco conceptual entiende que todo desarrollo tecnológico se estructura en cuatro niveles los cuales deben articularse entre sí para producir el efecto deseado en los clientes. Los cuatro niveles son:

- Nivel físico – Almacenamiento de datos
- Nivel de aplicaciones – Procesamiento de datos
- Nivel de negocio – Uso de los datos
- Nivel de comportamiento – Generación de los datos

El tratamiento de los datos en cada uno de los niveles es la esencia misma del flujo de la información que se crea por cuenta de una mayor conectividad y la convergencia entre lo físico, lo lógico y lo biológico. De esta forma, la creación de valor por parte de

la ciberseguridad a nivel empresarial deberá articular la iniciativa innovadora con los aquellos que reconocen su valor y participan de su materialización: el cliente, los empleados y los proveedores.

Figura 1. Ciberseguridad empresarial. Creación de valor para clientes, empleados y proveedores

	CREACIÓN DE VALOR		
CIBERSEGURIDAD EMPRESARIAL	**CLIENTES** (*Confianza*)	**EMPLEADOS** (*Flexibilidad*)	**PROVEEDORES** (*Productividad*)
Nivel de comportamientos (*Generación de datos*)	Opciones de seguridad y control personalizadas	Manejo de conflicto de intereses	Patrones de amenazas
Nivel de negocios (*Uso de datos*)	Alertas personalizadas basadas en perfiles	Perfiles de acceso flexibles	Analítica de tendencias y alertas
Nivel de aplicaciones (*Procesamiento de datos*)	Monitoreo y seguimiento de transacciones	Interfases y conexiones personalizadas	Cajas de arena de validación y control
Nivel físico (*Almacenamiento de datos*)	Transparencia en el almacenamiento de los datos	Repositorios de datos compartimentalizados	Anillos de seguridad y compartimentalización del almacenamiento

La estrategia de ciberseguridad deberá estar centrada al menos a cinco elementos claves:

- Invertir en mejorar las capacidades de sus empleados mediante **formación.**
- Establecer **recursos tecnológicos** para **prevenir los efectos** del cibercrimen.
- Incorporar la ciberseguridad a la **cultura de la organización**.
- Compartir las **mejores prácticas** sobre amenazas de forma **interna** y con **otras compañías** de su cadena de valor.
- Establecer **contramedidas** para evitar ciberataques.

La información de los equipos de las empresas puede ser aprovechada por ciberdelincuentes. **No hay víctima pequeña.** Si la información de la empresa no es útil al ciberdelincuente puede aprovechar la **infraestructura TIC empresarial** (utilizándola como bots) para:

- Para inundar de **spam** la red.
- Realizar **ataques** contra otras compañías.
- **Criptoanálisis** de monedas...

1.6.4 Evolución de la ciberseguridad

La evolución de la ciberseguridad ha ido de la mano de los avances en las tecnologías de la comunicación.

En la década de los 70, la seguridad en las empresas estaba centrada en garantizar el buen uso de la información por parte de los empleados confiando en el sentido común para garantizar la seguridad de la organización. Sin embargo y debido a la inclusión y

evolución de la tecnología, aparecieron nuevos riesgos que hicieron que esta "seguridad" quedara obsoleta.

- Empleados poco conocedores de los riesgos asociados a la información que manejan.
- No existían copias de seguridad generalizadas.
- Medidas de seguridad físicas inadecuadas e insuficientes.

Uno de los principales motivos por los que el avance de la tecnología propulsó un cambio en la tendencia de seguridad de las empresas vino motivado principalmente por los virus que se convirtieron en los principales motores de crecimiento para la seguridad de la información a nivel mundial debido a la globalidad de sus objetivos

La popularización de los ordenadores personales en los años 80 llevó al desarrollo de las primeras herramientas de ciberataque y sentó las bases de las futuras amenazas. Así aparecía en escena la primera generación de ciberamenazas caracterizada por la capacidad de réplica de los programas maliciosos. A pesar de que Internet aún no se había extendido, el malware llegaba a los ordenadores a través de disquetes, CDs o memorias USB. Ante el impacto de los ataques de virus, se empezó a trabajar en los primeros productos comerciales de **antivirus** tradicionales.

En los años 80 los sistemas informáticos de las empresas disponían de pocas medidas de seguridad, comenzaron a comercializarse los antivirus y empezaron a contratar guardias de seguridad para la protección de ciertas instalaciones

La segunda generación de ataques surgió en la década de 1990, a partir de la adopción de Internet por parte de usuarios y empresas. La conectividad nos unió a todos y los hackers se profesionalizaron especializándose en robar dinero, empezaron a usar técnicas que fueron las precursoras de las que utiliza la ciberdelincuencia actual. Para hacer frente a esta segunda generación, se desarrolló el primer ***firewall*** de "inspección de estado" de la industria.

En la década de los 90, se hacía un uso de internet sin la concienciación adecuada de los empleados, la información se almacenaba en dispositivos extraíbles con pocas medidas de seguridad y la seguridad física en las instalaciones seguía siendo insuficientes.

En los años 2000 llegó la tercera generación de amenazas, los ciberdelincuentes explotaban vulnerabilidades informáticas de sistemas operativos, hardware y aplicaciones. Era un campo totalmente nuevo y las vulnerabilidades aparecían por todas partes. También tuvo una gran relevancia la adopción masiva del email y las posibilidades de ingeniería social que ofrecía. Se combinaron *firewalls* y antivirus para proteger los sistemas de los ciberataques, asentando la base de las infraestructuras de seguridad empresariales de hoy en día. Pero la protección proporcionada comenzó a caer frente a la velocidad a la que los ataques evolucionaban en sofisticación e impacto.

Comenzaban a aparecer ataques dirigidos a las herramientas encargadas de proteger la información y la red corporativa. El uso de las redes sociales comienza a extenderse de forma masiva. Por otro lado, empiezan a producirse los riesgos de seguridad derivados de empleados insatisfechos y los fraudes online

En la década del 2010, los ciberataques alcanzaron niveles de sofisticación sin precedentes. Los criminales se unieron en organizaciones profesionales y empezaron a desarrollar malware de día cero. Los ciberataques se volvieron sigilosos y difíciles de identificar, los virus podían estar ocultos en todos los sitios, desde documentos adjuntos, información comercial falsa hasta archivos de imagen. Todo lo que un usuario tenía que hacer para caer en la trampa era hacer clic en el documento malicioso y su dispositivo se infectaba. Los ataques de cuarta generación consiguieron que la seguridad basada en la detección dejase de ser eficaz para proteger a las empresas al no poder reconocer las amenazas desconocidas. Ante esta situación, se desarrollaron soluciones de seguridad avanzada con tecnología de prevención de amenazas para bloquearlas antes de que pudieran actuar.

En esta década, los dispositivos móviles de las empresas disponían de pocas medidas de seguridad que impidan la fuga de información de la corporativa. Empiezan los planes sólidos de concienciación de los empleados sobre seguridad de la información, al igual que empieza a haber un mayor control relacionado con la privacidad de la información para evitar su fuga. Se empiezan a usar herramientas de cifrado de información a nivel corporativo y personal. Y nacen las primeras leyes de protección de infraestructuras críticas.

La quinta generación de ataques surgió con fuerza a principios de 2017 cuando aparecieron en escena herramientas de hackeo filtradas de la industria militar. Este malware dio lugar a ataques con múltiples vectores que causaron importantes pérdidas no sólo económicas sino también para la reputación de grandes empresas. El malware actual puede propagarse por toda la infraestructura TI desde un sólo dispositivo. Tuvo especial relevancia WannaCry que afectó a 300.000 ordenadores en 150 países, y NotPetya, que causó pérdidas de 300 millones de dólares.

El teletrabajo y el uso compartido de la información en la nube se convierten en una tendencia global. Los electrodomésticos disponen ya de acceso a Internet y los riesgos amplían su alcance, el riesgo ahora está en casa.

Ante la nueva generación de amenazas, y atendiendo a las distintas herramientas que la tecnología pone a nuestro alcance, se ha comenzado a explorar motores basados en Inteligencia Artificial. Mediante el uso de tecnologías de IA se puede emular y automatizar la intuición de un analista, los algoritmos pueden analizar millones de indicadores conocidos y buscar otros similares. Como resultado, se puede producir un *feed* en inteligencia de amenazas que favorece la prevención de ataques antes de que ocurran por primera vez.

1.7 Bibliografía

Para la elaboración de esta unidad didáctica se han utilizado los siguientes recursos:

- Apuntes proporcionados por la escuela de organización industrial en el curso de Ciberseguridad para formadores.
- https://hard2bit.com/blog/como-ha-evolucionado-la-ciberseguridad-en-los-ultimos-25-anos-y-como-ha-sido-la-evolucion-de-seguridad-en-las-empresas/

UD1: Conceptos Básicos en Ciberseguridad

- https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella
- https://www.xataka.com/basics/red-tor-que-como-funciona-como-se-usa
- *https://www.incibe.es*
- https://ciberseguridad.com/
- http://recursostic.educacion.es/observatorio/web/