UDS

Mi Universidad

LIBRO

*Nombre de la materia: GESTION DE SISTEMAS*

*Nombre de la Licenciatura: INGENIERIA EN SISTEMAS COMPUTACIONALES*

*Cuatrimestre: 5to.*

*Periodo*

Enero-Abril

## Marco Estratégico de Referencia

### Antecedentes históricos

Nuestra Universidad tiene sus antecedentes de formación en el año de 1979 con el inicio de actividades de la normal de educadoras "Edgar Robledo Santiago", que en su momento marcó un nuevo rumbo para la educación de Comitán y del estado de Chiapas. Nuestra escuela fue fundada por el Profesor Manuel Albores Salazar con la idea de traer educación a Comitán, ya que esto representaba una forma de apoyar a muchas familias de la región para que siguieran estudiando.

En el año 1984 inicia actividades el CBTiS Moctezuma Ilhuicamina, que fue el primer bachillerato tecnológico particular del estado de Chiapas, manteniendo con esto la visión en grande de traer educación a nuestro municipio, esta institución fue creada para que la gente que trabajaba por la mañana tuviera la opción de estudiar por las tardes.

La Maestra Martha Ruth Alcázar Mellanes es la madre de los tres integrantes de la familia Albores Alcázar que se fueron integrando poco a poco a la escuela formada por su padre, el Profesor Manuel Albores Salazar; Víctor Manuel Albores Alcázar en julio de 1996 como chofer de transporte escolar, Karla Fabiola Albores Alcázar se integró en la docencia en 1998, Martha Patricia Albores Alcázar en el departamento de cobranza en 1999.

En el año 2002, Víctor Manuel Albores Alcázar formó el Grupo Educativo Albores Alcázar S.C. para darle un nuevo rumbo y sentido empresarial al negocio familiar y en el año 2004 funda la Universidad Del Sureste.

La formación de nuestra Universidad se da principalmente porque en Comitán y en toda la región no existía una verdadera oferta Educativa, por lo que se veía urgente la creación de una institución de Educación superior, pero que estuviera a la altura de las exigencias de los

jóvenes que tenían intención de seguir estudiando o de los profesionistas para seguir preparándose a través de estudios de posgrado.

Nuestra Universidad inició sus actividades el 18 de agosto del 2004 en las instalaciones de la 4ª avenida oriente sur no. 24, con la licenciatura en Puericultura, contando con dos grupos de cuarenta alumnos cada uno. En el año 2005 nos trasladamos a nuestras propias instalaciones en la carretera Comitán – Tzimol km. 57 donde actualmente se encuentra el campus Comitán y el corporativo UDS, este último, es el encargado de estandarizar y controlar todos los procesos operativos y educativos de los diferentes campus, así como de crear los diferentes planes estratégicos de expansión de la marca.

## Misión

Satisfacer la necesidad de Educación que promueva el espíritu emprendedor, aplicando altos estándares de calidad académica, que propicien el desarrollo de nuestros alumnos, Profesores, colaboradores y la sociedad, a través de la incorporación de tecnologías en el proceso de enseñanza-aprendizaje.

## Visión

Ser la mejor oferta académica en cada región de influencia, y a través de nuestra plataforma virtual tener una cobertura global, con un crecimiento sostenible y las ofertas académicas innovadoras con pertinencia para la sociedad.

## Valores

- Disciplina
- Honestidad
- Equidad
- Libertad

## Escudo

El escudo del Grupo Educativo Albores Alcázar S.C. está constituido por tres líneas curvas que nacen de izquierda a derecha formando los escalones al éxito. En la parte superior está situado un cuadro motivo de la abstracción de la forma de un libro abierto.

## Eslogan

"Mi Universidad"

## ALBORES


Es nuestra mascota, un Jaguar. Su piel es negra y se distingue por ser líder, trabaja en equipo y obtiene lo que desea. El ímpetu, extremo valor y fortaleza son los rasgos que distinguen.

## Intervención Psicopedagógica.

**Objetivo de la materia:**

La coordinación en esta materia se va llevar a cabo por medio de la Comisión de Coordinación Vertical establecida para la misma, tal y como se describe en la sección Planificación de las enseñanzas.

**Criterios de evaluación:**

| No | Concepto | Porcentaje |
|---|---|---|
| 1 | Trabajos Escritos | 30% |
| 2 | Actividades áulicas | 20% |
| 3 | Examen | 50% |
| 4 | Total | 100% |
| 5 | Escala de calificación | 7- 10 |
| 6 | Mínima aprobatoria | 7 |

# INDICE

# UNIDAD I

# SISTEMAS ORIENTADOS A SERVICIOS

La arquitectura orientada a servicios (SOA) es el nexo que une las metas de negocio con el sistema de software. Su papel es el de aportar flexibilidad, desde la automatización de las infraestructura y herramientas necesarias consiguiendo, al mismo tiempo, reducir los costes de integración.

## 1.1.- Fundamentos de la orientación a servicios software.

La Arquitectura Orientada a Servicios (SOA, Service Oriented Architecture) supone una estrategia general de organización de los elementos de TI, de forma que una colección abigarrada de sistemas distribuidos y aplicaciones complejas se pueda transformar en una red de recursos integrados, simplificada y sumamente flexible. Un proyecto SOA bien ejecutado permite alinear los recursos de TI de forma más directa con los objetivos de negocio, ganando así un mayor grado de integración con clientes y proveedores, proporcionando una inteligencia de negocio más precisa y más accesible con la cual se podrán adoptar mejores decisiones, y ayuda a las empresas a optimizar sus procesos internos y sus flujos de información para mejorar la productividad individual. El resultado neto es un aumento muy notable de la agilidad de la organización.

Si bien una adopción de SOA bien planificada y ejecutada puede mejorar la capacidad de respuesta de las organizaciones, no todos los esfuerzos de orientación a servicios han resultado satisfactorios. Los proyectos de SOA han tenido un éxito limitado cuando los desarrolladores los han intentado resolver de abajo arriba: implantar SOA por el gusto de tener SOA sin tener una referencia clara del contexto de negocio en el que debe desplegarse es un proyecto sin principios organizativos y sin rumbo. El resultado será una implementación caótica que no aportará beneficio alguno a la empresa. Por otra parte, una estrategia de mega-implementación descendente (“top-down”) para SOA exige una inversión colosal de recursos y tiempo, de manera que cuando el proyecto se concluye, la solución probablemente ya no refleja las necesidades del negocio.

En contraste con estas visiones, Microsoft prefiere lo que denominamos una táctica "de término medio". En esta línea, los esfuerzos de SOA se dirigen a partir de una visión estratégica global y las necesidades de negocio, y se van completando mediante proyectos SOA incrementales, iterativos que se diseñan de forma que cumplan objetivos de negocio, respondiendo a una necesidad concreta cada vez. Microsoft lleva realizando proyectos SOA con éxito para sus clientes desde 1999, año en que se presentó el modelo de servicios Web y ha seguido en esta línea con las herramientas .NET Framework y SOA y con sus soluciones de diseño integradas en su plataforma de aplicaciones. Desde entonces, la visión de Microsoft sobre cómo aplicar SOA a las necesidades del mundo real ha ayudado a organizaciones de todos los tamaños a optimizar sus procesos de negocio a mejorar su agilidad y reducir sus ciclos de puesta en valor gracias a la aplicación de sus principios de diseño con SOA, sus buenas prácticas, herramientas y tecnologías.

Los sistemas informáticos tradicionales se han organizado en grandes bloques monolíticos que contienen tanto los procesos de negocio como sus funciones automatizadas. Así por ejemplo, el proceso de contratación de una póliza de seguro, y las funciones del cálculo de la prima y la emisión de los recibos, forman parte del mismo bloque.

Estos sistemas han conseguido una gran mejora de productividad en las empresas, automatizando procesos de negocio, pero su concepción monolítica hace que los cambios y adaptaciones a las nuevas necesidades tiendan a ser más lentos y costosos de lo deseable. En bastantes organizaciones esto provoca que los sistemas marchen por detrás de las necesidades de negocio.

Para conseguir un mayor nivel de agilidad es necesario poder combinar rápidamente los distintos componentes del sistema, algo a lo que la concepción monolítica tradicional plantea muchas restricciones. La arquitectura SOA separa los procesos de negocio de las funciones automatizadas y organiza estas últimas en módulos individuales catalogados en un diccionario de servicios que permiten su utilización por parte de toda la organización.

Pocos avances tecnológicos han despertado tanto interés como la arquitectura SOA, y es muy importante comprender exactamente el papel que ésta puede desempeñar a la hora de ayudar a las empresas a alcanzar el alto rendimiento. A menudo se suele caer en la tentación

de considerar los nuevos y esperados avances (como la arquitectura SOA) como la varita mágica para mejorar el funcionamiento de la empresa. Las nuevas tecnologías tienden a ser el objeto de este tipo de planteamientos, pero frecuentemente el resultado es decepcionante.

Sin embargo, SOA no es solamente una tecnología, sino una arquitectura que trata de estructurar las aplicaciones de negocio y la tecnología para responder de forma ágil y flexible a las demandas del mercado. No se trata de algo radicalmente nuevo, sino que se debería ver como la última fase (aunque muy importante) del proceso de evolución de la arquitectura tecnológica y de negocio de toda la empresa.

La importancia de la arquitectura SOA, y probablemente la razón por la que despierta tanto interés entre los directores de los departamentos de tecnología y entre los responsables de desarrollo, es que ofrece una oportunidad real de situar las tecnologías de la información en un nuevo nivel, convirtiéndolas en auténticos habilitadores del negocio.

La arquitectura SOA constituye la base que garantiza la agilidad del negocio, un prerrequisito fundamental para alcanzar el éxito en el actual mercado mundial, siempre tan competitivo. Esta agilidad es la capacidad de añadir, modificar y optimizar fácilmente los procesos de negocio mediante el aprovechamiento de las sinergias de servicios o procesos. Este aprovechamiento tiene el fin de crear una nueva gama de capacidades o productos, mediante la combinación de algunos elementos de los procesos de negocio actuales, y dando soporte así a nuevos segmentos de clientes, canales o mercados.

## 1.2.- Tecnologías para desarrollo de Servicios.

Los modelos y tecnologías de desarrollo web han evolucionado mucho en la última década, existen multitud de aplicaciones, frameworks, librerías, arquitecturas y sistemas de publicación en diferentes versiones que a su vez reciben cambios o mejoran con el tiempo.

El progreso también ha tenido lugar en lo relacionado con la administración de sistemas, servicios de alojamiento, técnicas de escalabilidad, monitorización y gestión de centros de procesos de datos.

Esta evolución ha dado lugar a la convergencia de una gran cantidad de tecnologías, herramientas y estilos arquitectónicos para desarrollar sitios web y aplicaciones, te contamos

los aspectos más importantes relacionados con ellos, y la manera en la que interactúan entre sí.

Un sitio o aplicación web puede crearse utilizando diferentes tecnologías que se dividen en dos grandes categorías:

Tecnologías de cliente: Son aquellas que permiten crear interfaces de usuario y establecer comunicación con el servidor basadas en HTML, CSS y JavaScript, en este caso, el navegador actúa como intérprete.

Tecnologías de servidor: Permiten implementar comportamientos de la aplicación web en el servidor, los lenguajes de programación más utilizados son Java EE, .NET, PHP, Ruby on Rails, Python, Django, Groovy, Node.js, etc…

Tecnologías estándar del lado cliente

El W3C (World Wide Web Consortium) es una comunidad internacional que desarrolla estándares abiertos que aseguran el crecimiento de la web a largo plazo, tales como HTML5&CSS, Scripting and AJAX, normas de accesibilidad, gráficos, audio y vídeo, web semántica, XML y muchos más.

HTML: (Hypertext Markup Languaje) proporciona la información estructurada en secciones, párrafos, título, imágenes, etc… la versión actual el HTML5, y ofrece muchas librerías avanzadas para la inserción de contenidos multimedia, canvas, comunicaciones y concurrencia.

CSS: (Cascading Style Sheets) se encarga de la distribución de los elementos y su estilo con colores, tipos de letra, fondos, efectos, etc…en documentos HTML, XML, SVG o incluso interfaces de usuario de otras tecnologías.

Scripting: Gracias al scripting las páginas pueden programarse con distintos lenguajes de script, aunque principalmente se utiliza JavaScript, que modifica la página gracias a su capacidad de ejecutar código cuando se interactúa con ella.

JavaScript inicialmente era un lenguaje interpretado, pero actualmente también se ejecuta con máquinas virtuales en los navegadores aumentando la velocidad de ejecución y eficiencia de

memoria. Es de tipado dinámico y funcionalmente orientado a objetos (basado en prototipos).

Existen multitud de bibliotecas (APIS) para el desarrollo web y de aplicaciones, pero las más utilizadas son JQuery y Underscore.js.

DOM: Es el modelo de objetos del documento (Document Object Model) y consta de una librería (API) para manipular el documento HTML cargado en el navegador, permitiendo la gestión de eventos, o la inserción y eliminación de elementos.

Tecnologías no estándar para desarrollo web

Durante bastante tiempo la carencia de tecnologías abiertas para realizar diferentes acciones asociadas a comportamientos y contenidos multimedia hizo que algunas tecnologías propietarias ocuparan este hueco, siempre por iniciativa de empresas de desarrollo de software, a continuación, destacamos algunas de las más conocidas.

Adobe Flash: Se trata de una tecnología utilizada para incrustar contenido multimedia interactivo en páginas web que predominó durante mucho tiempo, gratuita para el usuario, pero de carácter propietario y cerrado para los desarrolladores, que deben pagar licencia para poder usarla, motivo principal por el que está cada vez más en desuso.

Java Applets: Los Applets de Java fueron los precursores de Flash, pero debido a prácticas anticompetitivas de Microsoft y de Sun Microsystems estaba más centrada en los servidores de aplicaciones, así que también hace tiempo que se encuentra en desuso.

Microsoft Silverligth: Fué durante tiempo la apuesta de Microsoft para competir con Adobe Flashs, pero el soporte era muy limitado en plataformas diferentes a Windows.

Tecnologías de servidor

Los estándares son muy importantes en los navegadores web (cliente) ya que es importante que la web sea compatible con cualquier dispositivo, sin embargo, estos estándares no son necesarios en el servidor, porque cada organización desarrollará su servidor con la tecnología que crean conveniente.

En el servidor se utilizan tecnologías propietarias o abiertas para el desarrollo de aplicaciones web, existen multitud de ellas, entre ellas las más usadas son PHP, Java EE y ASP.NET, y las menos usadas Ruby on Rails, Grails (Groovy), Django (Phyton), Perl, ColdFusion, hay muchas más, pero entre ellas comentamos a continuación las más destacadas.

Java EE: Es una tecnología basada en Java desarrollada por una coalición de empresas lideradas por Oracle, IBM, Red Hat, etc… muy utilizada a nivel empresarial, la mayoría de implementaciones y herramientas para desarrollo son software libre, y existen comunidades de desarrolladores y empresas que realizan complementos.

PHP: Es una tecnología con lenguaje propio, desarrollada por PHP Group y con licencia libre. Es la tecnología de lado de servidor con la que se han implementado más servidores en Internet, es multiplataforma y se integra normalmente con Apache y MySQL en entornos Linux gracias a un paquete llamado LAMP.

ASP.NET: Se trata de una versión evolucionada del ASP clásico, está integrada en la tecnología .NET de Microsoft junto con el lenguaje C#, tiene licencia propietaria y para plataformas Windows y una comunidad de desarrolladores má limitada que otras alternativas.

## 1.3.- Arquitecturas y tecnologías para orientación a servicios.

La Arquitectura Orientada a Servicios (SOA, siglas del inglés Service Oriented Architecture) es un estilo de arquitectura de TI que se apoya en la orientación a servicios. La orientación a servicios es una forma de pensar en servicios, su construcción y sus resultados. Un servicio es una representación lógica de una actividad de negocio que tiene un resultado de negocio específico (ejemplo: comprobar el crédito de un cliente, obtener datos de clima, consolidar reportes de perforación)

El estilo de arquitectura SOA se caracteriza por:

Estar basado en el diseño de servicios que reflejan las actividades del negocio en el mundo real, estas actividades forman parte de los procesos de negocio de la compañía.

Representar los servicios utilizando descripciones de negocio para asignarles un contexto de negocio.

Tener requerimientos de infraestructura específicos y únicos para este tipo de arquitectura, en general se recomienda el uso de estándares abiertos para la interoperabilidad y transparencia en la ubicación de servicios.

Estar implementada de acuerdo con las condiciones específicas de la arquitectura de TI en cada compañía.

Requerir un gobierno fuerte sobre las representación e implementación de servicios.

Requerir un conjunto de pruebas que determinen que es un buen servicio.

El desarrollo e implementación de una arquitectura SOA se rige por los principios descritos en el manifiesto SOA. Por otra parte, la aplicación de la orientación a servicios se divide en 2 grandes etapas:

Análisis orientado a servicios (Modelado de servicios)

Diseño orientado a servicios, El diseño orientado a servicios cuenta con 8 principios de diseño que se aplican sobre cada uno de los servicios modelados, esto principios de diseño son:

Contrato de servicio estandarizado: Los contratos de servicio cumplen con los mismos estándares de diseño.

Bajo acoplamiento: Los servicios evitan acoplarse a la tecnología que los implementa y a su vez reducen el acoplamiento impuesto a los consumidores.

Abstracción: Los contratos presentan la información mínima requerida y la información de los servicios se limita a los expuesto en el contrato.

Reusabilidad: Los servicios expresan y contienen lógica de negocio independiente del consumidor y su entorno, por lo tanto, se convierten en activos de la empresa.

Autonomía: Los servicios deben tener un gran control de los recursos tecnológicos sobre los cuales están implementados.

Sin estado: El servicio reduce el consumo de servicios al delegar el manejo de estados (sesiones) cuando se requiera.

Garantizar su descubrimiento: Lo servicios cuentan con metadata que permite descubrirlos e interpretar el servicio en términos de negocio.

Preparado para ser usado en composiciones: Los servicios pueden hacer parte de una composición sin importar el tamaño y complejidad de la misma.

## 1.4.- Garantía del nivel de servicio.

Los SLA (Service-Level Agrements) se han hecho imprescindibles en el mundo de los servicios. Su objetivo principal es estrechar las relaciones comerciales a través del compromiso mutuo entre proveedor y usuario.

Un acuerdo de nivel de servicio (siglas ANS), también conocidas por las siglas SLA (del inglés Service Level Agreement), es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.1

Básicamente el ANS establece la relación entre ambas partes: proveedor y cliente. Un ANS identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del proveedor, proporciona un marco de entendimiento, simplifica asuntos complicados, reduce las áreas de conflicto y favorece el diálogo ante la disputa.

También constituye un punto de referencia para el proceso de mejora continua, ya que el poder medir adecuadamente los niveles de servicio es el primer paso para mejorarlos y de esa forma aumentar los índices de calidad, KPI...

## 1.5.- Diseño, composición y coordinación de servicios.

En esencia una arquitectura orientada a servicios constituye un sistema distribuido, donde los componentes distribuidos son servicios independientes, abstraídos como unidades autónomas en una red de proveedores y consumidores.

Atendiendo a esta perspectiva, y teniendo en cuenta los principios SOA vistos, podremos introducir el proceso de diseño de servicios en SOA a través de tres etapas: Identificar servicio, Diseñar servicio e Implementar servicio.

Identificación de Servicios

El primer paso en el diseño en una arquitectura SOA es la identificación de funcionalidades que puedan ser expuestas como servicios. Para ello es importante detectar las funcionalidades de granularidad alta que cumplan los criterios para ser candidatas:

Fácilmente independizables y que permitan un bajo acoplamiento.

Alto potencial de reutilización.

Existen dos enfoques principales para abordar esta difícil e importantísima tarea de identificación de los servicios útiles, mediante una aproximación ascendente (Bottom-Up) y aproximación descendente (Top-Down).

Diseño del Servicio

Una vez identificados los servicios, se realizarán las tareas de la fase de diseño, donde: Definir los contratos de cada servicio, incluyendo: La interfaz y parámetros. Descripción de la funcionalidad. Políticas.

Restricciones.

Clasificar y Categorizar en función de su naturaleza. Por ejemplo, en servicios estratégicos para la empresa, servicios básicos, servicios de soporte, etc.

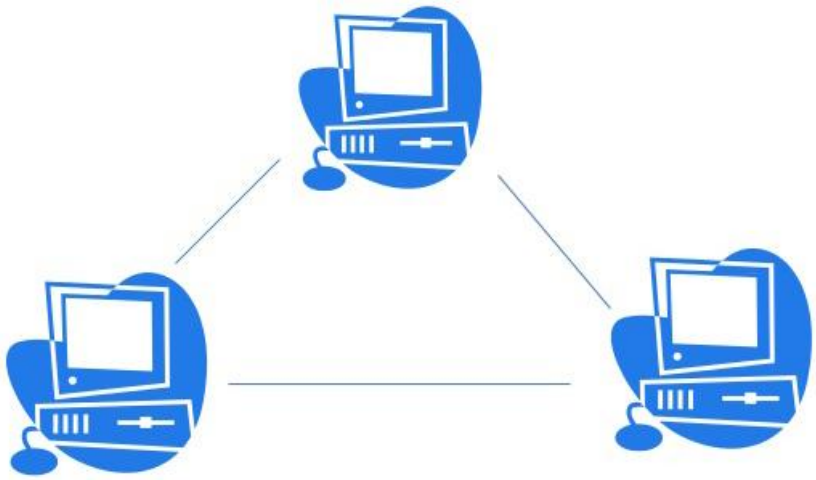
Diseño arquitectónico del sistema que permita satisfacer los requisitos, y establecer la estructura más adecuada a nivel lógico y físico, evitando confundir capas y niveles: Una arquitectura monolítica. O bien arquitectura Cliente/Servidor. Arquitectura en tres capas.

Implementación

Finalmente, se selecciona la tecnología más adecuada que permita la implementación y despliegue de la funcionalidad identificada como servicio. Esta etapa lleva a cabo la construcción o suscripción, adaptación o integración de una funcionalidad existente a la arquitectura tecnológica seleccionada.

Durante todo el proceso es evidente que se deben respetar los principios SOA, y hacer efectivo en el diseño y la implementación los criterios de bajo nivel de acoplamiento, independencia y reutilización. Uno de los objetivos de SOA es aislar al servicio de la plataforma, sistema operativo, hardware, lenguaje, protocolo, localización, etc. En resumen, minimizar el acoplamiento de la unidad funcional.

## 1.6.- Redes de Computadores.



Una red de computadoras (también llamada red de ordenadores o red informática) es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de ordenadores es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo. Un

ejemplo es Internet, el cual es una gran red de millones de ordenadores ubicados en distintos puntos del planeta interconectados básicamente para compartir información y recursos.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP utilizado como base para el modelo de referencia OSI. Este último, concibe cada red como estructurada en siete capas con funciones concretas pero relacionadas entre sí (en TCP/IP se habla de cuatro capas). Debe recordarse que el modelo de referencia OSI es una abstracción teórica, que facilita la comprensión del tema, si bien se permiten ciertos desvíos respecto a dicho modelo.

Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

## 1.6.1.- Arquitecturas de comunicaciones.

La arquitectura de las comunicaciones es una estructura organizada jerárquicamente con el fin de permitir el intercambio de datos entre niveles lógicos semejantes en distintas máquinas o terminales de la misma o distinta red.

Al hablar de redes y de comunicaciones entre ordenadores resultan fundamentales 2 conceptos: Protocolos y Arquitectura de comunicación.

Los protocolos se utilizan para la comunicación entre entidades de diferentes sistemas. Ejemplos de entidades son programas de aplicación de usuario, paquetes de transferencia de ficheros, sistemas de manejo de BD y terminales. Ejemplo de sistemas son ordenadores, terminales y sensores remotos. Podemos decir, que una entidad es algo capaz de enviar o de recibir información y un sistema es un objeto que contiene una o más entidades. Para que 2 entidades puedan comunicarse han de hablar el mismo idioma, mediante una serie de convenciones entre estas, a este conjunto de convenciones se le denomina protocolo, que puede definirse como el conjunto de reglas que gobiernan el intercambio de datos entre 2 entidades.

Debido a la complejidad que requiere la comunicación entre 2 entidades de diferentes sistemas, encontramos implementadas las funciones de comunicación mediante un conjunto de protocolos estructurados. Esta organización de los protocolos se realiza mediante capas o niveles con objeto de simplificar su diseño. El propósito de cada capa es ofrecer ciertos servicios a las capas superiores.

La capa n en una máquina conversa con la capa n de la otra máquina. Las reglas y convecciones utilizadas en la conversación se conocen como protocolo de la capa n. A las entidades de una misma capa correspondiente a máquinas diferentes se le denomina procesos pares.

En la realidad, la transferencia de datos desde una capa n de una máquina a la capa n de otra máquina no se realiza directamente, sino que los datos son pasados a la capa inmediatamente inferior de la máquina y así sucesivamente hasta llegar a la capa 1, donde nos encontramos el medio físico, por donde se realiza la comunicación con la otra máquina.

Entre cada par de capas adyacentes hay una interfaz, la cual define los servicios y operaciones primitivas que la capa inferior ofrece a la superior. Al conjunto de capas con las interfaces y protocolos recibe el nombre de arquitectura de la red.

## 1.6.2.- Tecnologías de red.

Una red es una configuración de computadora que intercambia información. Pueden proceder de una variedad de fabricantes y es probable que tenga diferencias tanto en hardware como en software, para posibilitar la comunicación entre estas es necesario un conjunto de reglas formales para su interacción. A estas reglas se les denominan protocolos.

Un protocolo es un conjunto de reglas establecidas entre dos dispositivos para permitir la comunicación entre ambos.

EJEMPLOS DE TECNOLOGIAS DE RED:

Ethernet (también conocido como estándar IEEE 802.3) es un estándar de transmisión de datos para redes de área local que se basa en el siguiente principio:

Todos los equipos en una red Ethernet están conectados a la misma línea de comunicación compuesta por cables cilíndricos.

Se distinguen diferentes variantes de tecnología Ethernet según el tipo y el diámetro de los cables utilizados:

- 10Base2: el cable que se usa es un cable coaxial delgado, llamado thin Ethernet.
- 10Base5: el cable que se usa es un cable coaxial grueso, llamado thick Ethernet.
- 10Base-T: se utilizan dos cables trenzados (la T significa twisted pair) y alcanza una velocidad de 10 Mbps.
- 100Base-FX: permite alcanzar una velocidad de 100 Mbps al usar una fibra óptica multimodo (la F es por Fiber).
- 100Base-TX: es similar al 10Base-T pero con una velocidad 10 veces mayor (100 Mbps).
- 1000Base-T: utiliza dos pares de cables trenzados de categoría 5 y permite una velocidad de 1 gigabite por segundo.
- 1000Base-SX: se basa en fibra óptica multimodo y utiliza una longitud de onda corta (la S es por short) de 850 nanómetros (770 a 860 nm).
- 1000Base-LX: se basa en fibra óptica multimodo y utiliza una longitud de onda larga (la L es por long) de 1350 nanómetros (1270 a 1355 nm).

## 1.6.3.- Protocolos de comunicaciones.

Un protocolo de comunicaciones es un conjunto de normas que están obligadas a cumplir todos las máquinas y programas que intervienen en una comunicación de datos entre ordenadores sin las cuales la comunicación resultaría caótica y por tanto imposible.

A continuación, se esbozan algunos ejemplos de protocolos de comunicaciones con la intención de aclarar el concepto y la evolución de los mismos:

- Protocolos punto a punto.
- Comunicación entre redes.
- Protocolos de transmisión de paquetes.

- El protocolo TCP/IP.
- Protocolos punto a punto.

Son los protocolos más antiguos y elementales utilizados para la comunicación mediante una línea de datos entre dos únicos ordenadores. Algunas de sus normas básicas establecen los criterios siguientes:

Papel que asume cada una de las dos partes durante una sesión de comunicaciones, identificándose y definiendo el papel correspondiente al ordenador que ha iniciado la sesión y al que responde. Al primero se le llama "comando" y al segundo, "respuesta".

Manera de controlar la correcta recepción de los datos. Por ejemplo, añadiendo un carácter al final de cada mensaje que sea la suma total de BIT utilizados.

Tiempo máximo que debe pasar entre el envío de un mensaje y la recepción del acuse de recibo desde la estación receptora.

Número veces que se debe repetir un mensaje en caso de que, pasados los tiempos correspondientes, no se reciba el mensaje de acuse de recibo.

En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades (computadoras, teléfonos celulares, etc.) de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

También se define como un conjunto de normas que permite la comunicación entre ordenadores, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos y la forma en que la información debe procesarse.

Los sistemas de comunicación utilizan formatos bien definidos (protocolo) para intercambiar mensajes. Cada mensaje tiene un significado exacto destinado a obtener una respuesta de un rango de posibles respuestas predeterminadas para esa situación en particular. Normalmente,

el comportamiento especificado es independiente de cómo se va a implementar. Los protocolos de comunicación tienen que estar acordados por las partes involucradas. Para llegar a dicho acuerdo, un protocolo puede ser desarrollado dentro de estándar técnico. Un lenguaje de programación describe el mismo para los cálculos, por lo que existe una estrecha analogía entre los protocolos y los lenguajes de programación: «los protocolos son a las comunicaciones como los lenguajes de programación son a los cómputos. Un protocolo de comunicación, también llamado en este caso protocolo de red, define la forma en la que los distintos mensajes o tramas de bit circulan en una red de computadoras.

Por ejemplo, el protocolo sobre palomas mensajeras permite definir la forma en la que una paloma mensajera transmite información de una ubicación a otra, definiendo todos los aspectos que intervienen en la comunicación: tipo de paloma, cifrado del mensaje, tiempo de espera antes de dar a la paloma por 'perdida'... y cualquier regla que ordene y mejore la comunicación.

## 1.6.4.- Redes de área local.

Red de Área Local. Una red de área local, red local o LAN (del inglés local area network) es la interconexión de varias Computadoras y Periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con Repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar Datos y Aplicaciones. En definitiva, permite una conexión entre dos o más equipos.

El término red local incluye tanto el Hardware como el Software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

## 1.6.5.- Servicios telemáticos.

Son aquellos que, utilizando como soporte servicios básicos, permiten el intercambio de información entre terminales con protocolos establecidos para sistemas de interconexión abiertos. (Decreto modificatorio D.600-03): Forman parte de éstos, entre otros, los de telefax, publifax, teletex, videotex y datafax.

# UNIDAD II

# SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

El objetivo de la seguridad informática es mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por computadora.

## 2.1.- La seguridad en sistemas y redes.

La seguridad de redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red. Los usuarios eligen o se les asigna una identificación y contraseña u otra información de autenticación que les permite acceder a información y programas dentro de sus autorizaciones. La seguridad de red cubre una variedad de redes de computadoras, tanto públicas como privadas, que se usan en trabajos cotidianos; realizar transacciones y comunicaciones entre empresas, agencias gubernamentales e individuos. Las redes pueden ser privadas, como dentro de una empresa, y otras que pueden estar abiertas al público. La seguridad de las redes está presente en organizaciones, empresas y otros tipos de instituciones. Hace como su nombre indica: protege la red, además de proteger y supervisar las operaciones que se realizan. La forma más común y simple de proteger un recurso de red es asignándole un nombre único y la contraseña correspondiente.

La seguridad de redes empieza con la autenticación, usualmente con un nombre de usuario y una contraseña. Ya que esto requiere solamente autenticar un nombre de usuario, por ejemplo, con la contraseña, se utiliza el término autenticación de un factor. Con un doble factor de autenticación se utiliza algo que el usuario "tiene", por ejemplo, una llave de seguridad, una tarjeta de crédito o un teléfono celular; y con un factor triple de autenticación se usa algo que el usuario "es", por ejemplo, huella dactilar o reconocimiento de iris.

Una vez autenticado, un cortafuego aplica políticas de acceso, por ejemplo, asignar los servicios a los cuales pueden acceder los usuarios de la red. Aunque esta medida es efectiva

para prevenir acceso no autorizado, este componente puede fallar al revisar contenido que puede ser dañino, un ejemplo sería un gusano informático o un troyano que esté siendo transmitido en la red. Un antivirus o un Sistema de prevención de intrusos (SPI ) ayuda a detectar e inhibir la acción de un malware. Un sistema de prevención de intrusos, basado en anomalías, también puede monitorear la red, por ejemplo, usando wireshark se puede analizar tráfico en la red con propósitos de auditoría o para un análisis de alto nivel.

La comunicación entre dos hosts en una red puede ser encriptada para asegurar la privacidad.

Los honeypots, esencialmente recursos accesibles en la red que actúan como señuelos, pueden ser desplegados en una red para vigilar y como herramienta de vigilancia y alerta temprana, ya que los honeypots normalmente no se utilizan para fines legítimos. Las técnicas utilizadas por los atacantes que intentan comprometer estos recursos señuelo se estudian durante y después de un ataque, para observar las nuevas técnicas de intrusión. Dicho análisis puede ser usado para futuros reforzamientos en la seguridad de la red que está siendo protegida por ese honeypot. Un honeypot también puede dirigir la atención de un atacante lejos de servidores legítimos. Un honeypot alienta a los atacantes a gastar su tiempo y energía en el servidor señuelo mientras distrae su atención de los datos del servidor real. Similar a un honeypot, una honeynet es una red configurada con vulnerabilidad intencional. Su propósito es, también, el de invitar a los atacantes para que sus técnicas de ataque puedan ser analizadas y ese conocimiento pueda ser usado para aumentar la seguridad de la red. Una honeynet normalmente contiene uno o más honeypots.

## 2.2.- Incidencias y ataques a la seguridad.

Pasos a seguir ante un ataque informático

Los planes de acción para prevenir y gestionar un tienen que tener cuatro fases: la prevención, la detección, la recuperación y la respuesta.

Los despachos de abogados son un objetivo atractivo para los ciberdelincuentes. Por ello, tienen que elaborar planes de acción ante ciberataques con el fin de proteger su información,

el conocido "secreto profesional". El plan de acción deberá dividirse en cuatro fases: prevención, detección, recuperación y respuesta.

## 1. PREVENCIÓN:

Actualmente, resulta imposible crear un entorno informático inaccesible a delincuentes informáticos aunque si se puede constituir un entorno preventivo que dificulte el acceso a los hackers, incorporando medidas preventivas:

1. Medidas preventivas organizativas

- Desarrollar dentro de la organización buenas prácticas para la gestión de la fuga de información.
- Definir una política de seguridad y procedimientos para los ciclos de vida de los datos.
- Establecer un sistema de clasificación de la información.
- Definir roles y niveles de acceso a la información.
- Protección del papel. Desarrollo de políticas para la destrucción del papel, conservación de documentación, políticas de clean desk.
- Sistemas de control de acceso, físicas a las instalaciones e informáticas en los ordenadores y sistemas de comunicación (móviles y tablets)
- Control de los dispositivos extraíbles (pendrives, discos externos,…)
- Desarrollo de planes de formación en materia de ciberseguridad y seguridad de la información, buenas prácticas de los sistemas informáticos etc. Estos planes de formación deben tener como objetivo la sensibilización y la formación de los usuarios.
- Contratar ciberseguros cuya finalidad es proteger a las entidades frente a los incidentes derivados de los riesgos cibernéticos, el uso inadecuado de las infraestructuras tecnológicas y las actividades que se desarrollan en dicho entorno. Así, las principales garantías ofrecidas por el mercado asegurador son las siguientes:
- Responsabilidad civil frente a terceros perjudicados.
- Cobertura de los gastos materiales derivados de la gestión de los incidentes.

- Cobertura de las pérdidas pecuniarias ante la interrupción de la actividad derivada de un fallo de seguridad y/o sistemas.
- Cobertura de los gastos de asesoramiento legal en los que se debe incurrir para hacer frente a los procedimientos administrativos.
- Cobertura ante la denegación de acceso a otros sistemas.
- Acompañamiento en la gestión de la crisis.

Estos seguros suelen venir acompañados de servicios adicionales tales como son:

- El borrado de huellas e historial.
- La reparación de sistemas y equipos.
- La recuperación de datos.
- La descontaminación de virus.

A este respecto, cabe llamar la atención que estas garantías no suelen estar cubiertas por las pólizas de seguros tradicionales de Daños Materiales y Responsabilidad Civil. En este sentido, las entidades más expuestas al riesgo cibernético deben revisar sus seguros el objeto de garantizar que no existen gaps en la cobertura de sus posibles siniestros.

2. Medidas preventivas legales:

Medidas relativas a la adecuación y cumplimiento de la legislación aplicable (LOPD y RLOPD) que incluyen, fundamentalmente, (i) el establecimiento de una circular sobre los principios generales a observar en el tratamiento de datos de carácter personal por parte de los empleados que tengan acceso a datos de carácter personal en el desempeño de sus funciones, (ii) contar con un sistema adecuado de investigación de incidencias y violaciones de seguridad de los datos.

- Solicitud de aceptación de la política de seguridad por parte de los empleados.
- Cláusulas contractuales con empleados en relación a la custodia, conservación y utilización de la información.
- Cláusulas contractuales con terceros en materia de confidencialidad.

- El establecimiento de una política de uso de medios tecnológicos, que determine el alcance del uso de los dispositivos y medios puestos a disposición del empleado por parte de la empresa y las facultades del empresario en relación con el control de la actividad de los empleados, así como las consecuencias derivadas del incumplimiento de la misma.

2. DETECCIÓN:

El momento en el que se detecta un incidente de fuga de información es un momento crítico en cualquier entidad. Una buena gestión de la fase de detección del ataque informático puede suponer una reducción significativa del impacto del ataque.

Esta fase es muy importante, ya que muchas veces se tiene conocimiento de la irrupción una vez la información sustraída se revela al público o a la red, o el ciberdelinuente se pone en contacto con el despacho de abogados correspondiente, para revenderles la información, extorsionarles o amenazarles.

Las principales medidas en esta fase de detección son técnicas, pues resulta imprescindible contar con una continua monitorización de los sistemas que permita detectar cualquier entrada sospechosa. Sin embargo también podemos encontrar medidas legales y organizativas:

1. Medias de detección organizativas:

Diseñar un protocolo interno de gestión del incidente en el que se identifique un gabinete de crisis u órgano decisorio de las medidas a adoptar. Este órgano debe estar compuesto por personas con capacidad de decisión, que puedan decidir, gestionar y coordinar la situación con calma, evitando consecuencias adicionales negativas.

2. Medidas de detección legales:

Sin perjuicio de las obligaciones previstas por el nuevo Reglamento Europeo de Protección de Datos, se deberán registrar las incidencias o brechas de seguridad en el Documento de Seguridad que la empresa u organización debe desarrollar y mantener actualizado, de tal forma que quede constancia de (i) el tipo de incidencia, (ii) el momento en que se ha

producido o detectado, (iii) la persona que realiza la notificación, (iii) la persona o personas a quien se realiza la notificación, (iv) los efectos que se derivan de la incidencia, (v) las medidas correctoras que se han aplicado.

Además, si la empresa realizase un tratamiento de datos de nivel medio o nivel alto, se deberán registrar, además de los extremos ya mencionados, (i) los procedimientos de recuperación realizados, (ii) la persona o personas que realizó el proceso de recuperación, (iii) los datos que han sido restaurados.

## 3. RECUPERACIÓN

Una vez que se detecta una entrada ilegal en los sistemas informáticos del despacho es necesario llevar a cabo un plan organizado de recuperación, cuyo objetivo no es otro que recuperar el sistema y dejarlo tal y como estaba antes del incidente. Para ello se deben implantar medidas técnicas de recuperación de la información: backups de los sistemas, copias de seguridad etc.

Entre las medidas organizativas que se pueden desarrollar para la recuperación se encuentra la elaboración de planes de continuidad del negocio que contemplen situaciones excepcionales que puedan producirse por ataques informáticos y que abarquen situaciones tanto de robo de información, como de bloqueo del sistema e incluso de borrado de datos. Además, se recomienda realizar un informe por un perito externo de cara a la presentación de una denuncia ante las autoridades, que permita recoger todas las pruebas que faciliten una posterior investigación.

## 4. RESPUESTA

En el momento que un despacho de abogados sufre un ataque informático se ve en la necesidad de dar respuesta al hecho acontecido. Ya no sólo dar respuesta e información a sus clientes, sino que también debe informar a los trabajadores, a terceros y encontrarse en predisposición de denunciar el hecho acontecido. Para ello se debe poner en marcha una estrategia de comunicación integral que abarque cada una de estas áreas. Y es que un paso fundamental ante un ataque informático, es minimizar la difusión de la información sustraída.

1. Respuestas a clientes:

Ante un ataque informático, es necesario poner en conocimiento de nuestros clientes el incidente ocurrido. En este sentido, el nuevo Reglamento General de Protección de Datos establece en su artículo 34 que se deberá comunicar a los interesados sin dilación debida toda violación de la seguridad que afecte a sus datos personales, siempre que entrañe un alto riesgo para los derechos y libertades de las personas físicas titulares de los datos objeto de la vulneración. La norma no define qué debe entenderse por "alto riesgo", por lo que ante la duda, lo aconsejable será informar a los interesados. Sin perjuicio de lo anterior, no será precisa la notificación, si (1) se han implementado medidas de seguridad apropiadas (p.ej., encriptación); o (2) si se han adoptado medidas que impiden que el riesgo elevado se llegue a materializar; o (3) la comunicación supone un esfuerzo desproporcionado.

En caso de que no aplique ninguna de las anteriores excepciones, la comunicación deberá incluir, como mínimo, (i) el nombre y los datos de contacto del delegado de protección de datos de la entidad o de otro punto de contacto en el que pueda obtenerse más información, (ii) las posibles consecuencias de la violación de la seguridad de los datos personales, y (iii) una descripción en un lenguaje sencillo las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Para ello se debe elaborar unas comunicaciones adecuadas a la situación concreta, atendiendo al número de clientes afectados, a la información sustraída y al daño ocasionado. Además de mostrar la disponibilidad y accesibilidad necesaria a todos nuestros clientes, como, por ejemplo, poniendo un teléfono de asistencia específico o designando a una persona concreta para dar respuesta a las susceptibles dudas y cuestiones que puedan surgir.

2. Respuestas dentro de la organización:

Igualmente, se debe hacer una comunicación a los empleados. En primer lugar, para que tengan capacidad de dar respuesta a clientes que puedan preguntar directamente a sus abogados de contacto, elaborando un discurso común y ordenado para toda la organización;

y en segundo lugar, para crear un sentimiento de concienciación de los empleados, que les permita sentirse parte del proceso y a la vez, permita al despacho localizar puntos por los que los ciberdelincuentes han podido tener acceso al sistema informático. Y es que no podemos olvidar, que un gran número de ataques informáticos se producen a través de dispositivos móviles de empleados, por conexiones a redes wifi inseguras o por el uso de contraseñas fáciles de descifrar.

3. Respuestas a terceros:

Dentro del plan de comunicación ante este tipo de incidentes, un punto fundamental es las comunicaciones con terceros, y estas pueden ser de varios tipos:

- Respuestas a medios de comunicación que se han hecho eco del hecho acontecido: mostrando tranquilidad e informando del control de la situación, así como anunciando las medidas legales que se tomaran al efecto y dando respuesta a las preguntas que pudiesen suscitarse.

- Comunicación con los sitios (medios, web, canales de noticias,…) que puedan haber publicado parte de información sustraída: anunciando que se trata de una información confidencial que ha sido sustraída de manera ilícita, solicitando su retirada a la mayor brevedad posible y pidiendo la colaboración del medio para la posible detección e identificación de los ciberdelincuentes.

4. Denuncias:

1. Comunicaciones a la AEPD

En relación con la notificación a la Agencia de Protección de Datos de una brecha de seguridad, con carácter previo a la aprobación del nuevo Reglamento General de Protección de Datos Europeo, tan sólo estaban obligados a acometerla los operadores de telecomunicaciones.

No obstante, con la aplicación del nuevo Reglamento General de Protección de Datos todas las empresas que hayan sufrido una brecha de seguridad, independientemente del sector al que pertenezcan, se encuentran obligadas a realizar una notificación expresa a la Agencia

Española de Protección de Datos sin demora, en un plazo máximo de72 horas siempre que sea posible. La notificación dirigida a la Agencia deberá incluir: (i) naturaleza del incidente; (ii) identidad y datos de contacto del delegado de protección de datos;(iii) consecuencias del incidente; y (iv) medidas correctoras propuestas o adoptadas.

Una vez transcurrido este plazo, y en caso de que no hubiera realizado la notificación, se deberá notificar asimismo a la Agencia Española de Protección de Datos las causas de la dilación o retraso.

2. Denuncias ante la Policía, la Guardia Civil o el Juzgado

Actualmente tanto la Guardia Civil con el Grupo de Delitos Telemáticos y la Policía con la Brigada de Investigación Tecnológica perteneciente a la UDEF, disponen de equipos de trabajo, especialmente formados para la investigación de estos ciberdelitos, es más, incluso disponen de grupos de trabajo que investigan y focalizan su trabajo, únicamente a delitos informáticos cometidos en el seno de empresas. Además, es absolutamente necesario que ante el descubrimiento de un ataque informático se proceda a la denuncia del hecho ante las autoridades competentes.

4. OTRAS MEDIDAS ACCESORIAS

Por último, debemos atender a otras medidas accesorias que se pueden implementar dentro de nuestro despacho de abogados y que van a contribuir a crear un entorno de seguridad y concienciación en materia de prevención, detección, recuperación y respuesta ante ataques informáticos como:

- Atender a las buenas prácticas de la ISO 19600 en materia de Compliance.
- Atender a las buenas prácticas de la ISO 27001 en materia de seguridad de la información.
- Apoyarse en terceros expertos independientes que puedan ayudarnos tanto en el desarrollo de todo el proceso, desde el desarrollo de políticas internas, como en la

custodia de información, como a la hora de actuar ante alguno de los incidentes expuestos.

## 2.3.- Criptología.

La criptología (del griego κρύπτος (kryptós): 'oculto' y λόγος (logos): 'estudio') es, tradicionalmente, la disciplina que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas.

Con la aparición de las tecnologías de la información y la comunicación y el uso masivo de las comunicaciones digitales, se han producido un número creciente de problemas de seguridad. El objetivo de la criptología se ha generalizado para estudiar las técnicas que se encargan de proporcionar seguridad a la información.

Los campos en los que se divide la criptología son:

- Criptografía. Se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.
- Criptoanálisis. Se ocupa de conseguir capturar el significado de mensajes construidos mediante criptografía sin tener autorización para ello. Podríamos decir que el criptoanálisis tiene un objetivo opuesto al de la criptografía. Su objetivo es buscar el punto débil de las técnicas criptográficas para explotarla y así reducir o eliminar la seguridad que teóricamente aportaba esa técnica criptográfica. A cualquier intento de criptoanálisis se le llama ataque. Un ataque tiene éxito, y se dice que el sistema se ha roto, cuando el atacante consigue romper la seguridad que la técnica criptográfica aporta al sistema.
- Esteganografía. Se ocupa de ocultar mensajes con información privada por un canal inseguro, de forma que el mensaje no sea ni siquiera percibido. Normalmente el mensaje es escondido dentro de datos con formatos de video, imágenes, audio o mensajes de texto. Los usos más frecuentes de estas técnicas son: transmitir cierta información entre entidades sin que sea detectada por terceros, inclusión de

información imperceptible en objetos digitales (Ej imágenes, vídeos, audios) para permitir un mayor control del uso de esos objetos digitales (por ejemplo, para implementar huellas digitales o marcas de agua.

- Estegoanálisis. Se ocupa de detectar mensajes ocultos con técnicas esteganográficas. Podríamos decir que el estegoanálisis tiene un objetivo opuesto al de la esteganografía. Su objetivo es buscar el punto débil de las técnicas esteganográficas para explotarlas y así reducir o eliminar la seguridad que teóricamente aportaba esa técnica esteganográfica. A cualquier intento de estegoanálisis se le llama ataque. Un ataque tiene éxito, y se dice que el sistema se ha roto, cuando el atacante detecta que se ha usado esteganografía y por tanto puede obtener el mensaje.

Algunos autores utilizan el término estegología al compendio de esteganografía y estegoanálisis.

## 2.4.- La seguridad en los datos de carácter personal.

Las Normas y controles relativos al uso de los Sistemas de Información, afectarán al uso y mantenimiento de los Recursos disponibles en los Sistemas de información, mediante los cuales se puede tener acceso a Datos de Carácter Personal.

Normas de Seguridad Generales:

- Estará disponible un Registro de Usuarios Autorizados para utilizar los ficheros existentes en los sistemas de información.
- Es obligación de los usuarios de los sistemas de información cumplir la normativa vigente y lo dispuesto en el documento de seguridad.
- Todos los usuarios autorizados, dispondrán de un código de usuario particular asociado a una contraseña que sólo conoce el usuario. El código de usuario y la contraseña serán absolutamente personales e intransferibles.
- Se prohíbe la instalación, por parte de los usuarios, de cualquier aplicación o producto informático en los sistemas de información, sin la autorización expresa del responsable de seguridad.

- No se permite la utilización de recursos de los sistemas de información con fines privados o con cualquier otro fin diferente a los estrictamente laborales, sin la correspondiente autorización del responsable del fichero.
- Se prohíbe la conexión a redes externas (Internet y servicios similares) desde equipos que contengan o tengan acceso a datos personales, sin la autorización previa del responsable del fichero, salvo que estén implementadas medidas técnicas que garanticen la seguridad de dicha conexión.

# UNIDAD III

# SISTEMAS OPERATIVOS

El objetivo principal de un sistema operativo es lograr que el sistema de computación se use de manera cómoda, y el objetivo secundario es que el hardware de la computadora se emplee de manera eficiente.

## 3.1.- Estructura interna del Sistema Operativo.

1. Componentes de un sistema operativo

• Administración de procesos

• Administración de memoria

• Subsistema de Entrada/Salida

• Administración de Almacenamiento secundario

• Subsistema de archivos

• Sistema de protección

Administración de Procesos

Para comenzar debemos saber que es un proceso. Un proceso es un programa en memoria + CPU + acceso a dispositivos + otros recursos. Notemos que un proceso necesita de ciertos recursos (como CPU, memoria, archivos, dispositivos de E/S, etc.) para realizar su tarea.

Podemos ver entonces que un proceso es una entidad activa, mientras que un programa una entidad pasiva.

Sabiendo entonces que es un proceso, podemos decir entonces que el sistema operativo es el encargado de su administración. Es el encargado de proveer servicios para que cada proceso pueda realizar su tarea. Entre los servicios se encuentran:

• Crear y destruir procesos

• Suspender y reanudar procesos

• Proveer mecanismos para la sincronización y comunicación entre procesos

• Proveer mecanismos para prevenir dead-locks o lograr salir de ellos.

Administración de Memoria

La memoria es un área de almacenamiento común a los procesadores y dispositivos, donde se almacenan programas, datos, etc. El sistema deberá administrar el lugar libre y ocupado, y será el encargado de las siguientes tareas:

• Mantener que partes de la memoria están siendo usadas, y por quien.

• Decidir cuales procesos serán cargados a memoria cuando exista espacio de memoria disponible, pero no suficiente para todos los procesos que deseamos.

• Asignar y quitar espacio de memoria según sea necesario.

Subsistema de Entrada/Salida

El sistema operativo deberá ocultar las características específicas de cada dispositivo y ofrecer servicios comunes a todos. Estos servicios serán, entre otros:

• Montaje y desmontaje de dispositivos

• Una interfaz entre el cliente y el sistema operativo para los device drivers.

• Técnicas de cache, buffering y spooling.

• Device drivers específicos

Administración de Almacenamiento secundario

Dado que la memoria RAM es volátil y pequeña para todos los datos y programas que se precisan guardar, se utilizan discos para guardar la mayoría de la información. El sistema operativo será el responsable de:

• Administrar el espacio libre

• Asignar la información a un determinado lugar

• Algoritmos de planificación de disco (estos algoritmos deciden quien utiliza un

determinado recurso del disco cuando hay competencia por él)

Subsistema de Archivos

Proporciona una vista uniforme de todas las formas de almacenamiento, implementando el concepto de archivo como una colección de bytes. El Sistema Operativo deberá

proveer métodos para:

• Abrir, cerrar y crear archivos

• Leer y escribir archivos

Sistema de protección

Antes que nada, tener en cuenta que por protección nos referimos a los mecanismos por los que se controla el acceso de los procesos a los recursos.

En un sistema multiusuario donde se ejecutan procesos de forma concurrente se deben tomar medidas que garanticen la ausencia de interferencia entre ellos. Estas medidas deben incorporar la posibilidad de definir reglas de acceso, entre otras cosas.

Servicios del Sistema Operativo

El sistema brindará un entorno de ejecución de programas donde se dispondrá de un conjunto de servicios. Los servicios principales serán:

• Ejecución de programas (el SO deberá ser capaz de cargar un programa a memoria y ejecutarlo. El programa deberá poder finalizar, de forma normal o anormal)

• Operaciones de E/S (el SO deberá proveer un mecanismo de acceso ya que por eficiencia y protección los usuarios no accederán directamente al dispositivo)

• Manipulación del Sistema de archivos (se deberá tener acceso al sistema de archivos y poder, como mínimo, leer, escribir, borrar y crear)

• Comunicación entre procesos (los procesos deberán poder comunicarse, ya sea que estén en el mismo computador o el diferentes)

• Manipulación de errores (el sistema deberá tomar decisiones adecuadas ante eventuales errores que ocurran, como fallo de un dispositivo de memoria, fallo en un programa, etc.)

Estructura del Sistema

Las estructuras internas de los sistemas operativos pueden ser muy diferentes, ya que se debe tener en cuenta las metas de los usuarios (fácil uso, confiable, rápido, etc.) y las del sistema (fácil de diseñar, implementar y mantener, eficiente, etc.).

Veremos 3 posibles diseños del sistema.

• Sistema Monolítico

Estos sistemas no tienen una estructura definida, sino que son escritos como una colección de procedimientos donde cualquier procedimiento puede invocar a otro.

Ejemplos de estos sistemas pueden ser MS-DOS o Linux (aunque incluye algo de capas). Es importante tener en cuenta que ningún sistema es puramente de un tipo.

• Sistema en capas

El diseño se organiza en una jerarquía de capas, donde los servicios que brinda una capa son consumidos solamente por la capa superior. La capa 0 es del Hardware y la N es la de los procesos de Usuario.

• Sistema con micronúcleo

La idea consiste en tener un núcleo que brinde los servicios mínimos de manejo de procesos, memoria y que provea la comunicación entre procesos. Todos los restantes servicios se construyen como procesos separados del micronúcleo, que ejecutan en modo usuario.

Estos sistemas tienen como ventaja un diseño simple y funcional, que aumenta la portabilidad y la escalabilidad. Para agregar un nuevo servicio no es necesario modificar el núcleo, y es más seguro ya que los servicios corren en modo usuario.

## 3.2.- Servicios del Sistema Operativo.

Los servicios son programas o aplicaciones cargadas por el propio sistema operativo. Estas aplicaciones tienen la particularidad que se encuentran corriendo en segundo plano

• Por defecto, con la instalación, se instalan y ejecutan una cierta cantidad de servicios. De más está decir, que, dependiendo de nuestras necesidades, podemos necesitarlos a todos o no.

• Como sabemos, mientras más aplicaciones tengamos ejecutándose consumimos más recursos, por lo tanto, vamos a tratar de deshabilitar lo que no utilizamos.

Interfaz de Usuario

Casi todos los sistemas operativos disponen de una interfaz de usuario (UI, user interface), que puede tomar diferentes formas. Uno de los tipos existentes es la interfaz de línea de comandos (CLI, command-line interface) que usa comandos de texto, y por otra parte se utiliza una interfaz gráfica de usuario (GUI, graphical user interface) compuesta por ventanas.

Ejecución de Programas

El sistema tiene que poder cargar un programa y ejecutar dicho programa. Todo programa debe poder terminar su ejecución, de forma normal o anormal (indicando un error).

Operaciones de E/S

Un programa en ejecución puede necesitar llevar a cabo operaciones de E/S, dirigidas a un archivo o dispositivo de E/S. Para ciertos dispositivos es deseable disponer de funciones especiales. Por cuestión de eficiencia y protección, los usuarios no pueden controlar de

modo directo los dispositivos de E/S; el sistema operativo debe proporcionar medios para realizar la E/S.

Manipulación del sistema de archivos

El sistema de archivos tiene una importancia especial. Obviamente, los programas necesitan leer y escribir en archivos y directorios. También necesita crearlos y borrarlos usando su nombre, realizar búsquedas en un determinado archivo o presentar la información contenida en un archivo. Algunos programas incluyen mecanismos de gestión de permisos para conceder o denegar el acceso a los archivos o directorios dependiendo de quién es el propietario.

Comunicaciones

Hay muchas circunstancias en las que un proceso necesita intercambiar información con otro. Dicha comunicación puede tener lugar entre procesos que se están ejecutando en la misma computadora o entre procesos en computadoras diferentes conectadas por red. Las comunicaciones se pueden implementar utilizando memoria compartida, procedimiento en el que el sistema operativo transfiere paquetes de información entre unos procesos y otros.

Detección de errores

El sistema operativo necesita detectar constantemente los posibles errores. Estos errores pueden producirse en el hardware del procesador y de memoria, en un dispositivo de E/So en los programas de usuario. Para cada tipo de error, el sistema operativo debe llevar a cabo la operación apropiada para asegurar el funcionamiento correcto y coherente.

Asignación de recursos

Cuando hay varios usuarios, o hay varios trabajos ejecutándose al mismo tiempo, deben asignarse a cada uno de ellos los recursos necesarios. El sistema operativo gestiona muchos tipos diferentes de recursos; algunos pueden disponer de código de software especial que gestionen su asignación, mientras que otros pueden tener código que gestione de forma mucho más general su solicitud y liberación.

## 3.3.- Programación de Sistemas.

Los programadores de sistemas informáticos escriben programas para controlar el funcionamiento interno de los ordenadores, lo que implica diseñar programas que sean eficientes, rápidos y versátiles. Dedican mucho tiempo a probar los programas, y también puede instalar, personalizar y dar soporte a estos sistemas operativos.

Los programadores de sistemas informáticos realizan tareas de investigación, diseño y desarrollo de programas que controlan el funcionamiento interno de los ordenadores y redes informáticas. Los programadores de sistemas informáticos escriben programas que sean rápidos, versátiles y eficientes, a menudo siguiendo las especificaciones proporcionadas por un analista de sistemas informáticos. También pueden instalar, personalizar y dar soporte a estos sistemas operativos.

Su objetivo es hacer que los sistemas informáticos (hardware y software) funcionen de forma más eficiente. Esto incluye el estudio de los ordenadores manejan los datos y textos, envían información a impresoras y se vinculan a los sistemas de telecomunicaciones.

Si un programa de aplicaciones (por ejemplo, uno que permita un equipo para administrar nóminas) no funciona tan rápida o eficientemente como debería, el programador de sistemas informáticos debe analiza el sistema operativo y el equipo para ver si puede ajustarse con el fin de mejorar el rendimiento de la aplicación.

Los programadores de sistemas informáticos suelen comenzar cada proyecto mediante la representación en forma de diagramas, con el fin de descomponer el proyecto en una serie de pasos, que luego se puedan seguir en un orden lógico.

El programador traduce estos pasos en las instrucciones escritas en lenguaje informático. Se trata de un trabajo muy técnico que utiliza un lenguaje computacional muy complicado.

Los programadores de sistemas informáticos pasan mucho tiempo probando y mejorando el programa, y eliminando errores (depuración). Se encargan de la producción de diagramas y

notas del programa para ayudar a los escritores técnicos, que son responsables de redactar los manuales de usuario.

Los programadores de sistemas informáticos también pueden realizar tareas técnicas, tales como asegurarse de que el software nuevo o actualizado funciona correctamente con los sistemas existentes. Pueden aconsejar a los analistas de sistemas y programadores de aplicaciones sobre qué tareas adicionales se pueden añadir al sistema o sobre la necesidad de instalar un nuevo sistema.

Aparte de los sistemas computacionales, los programadores de sistemas informáticos trabajan en todo tipo de equipos operativos, incluyendo impresoras, organizadores electrónicos personales y equipos de telecomunicaciones. Pueden trabajar para las empresas que producen estos artículos, así como escribir o adaptar sistemas operativos.

## 3.4.- Administración del Sistema Operativo.

Puede utilizar mandatos para gestionar la copia de seguridad y el inicio del sistema, cerrar el sistema, los shells y entornos del sistema, los recursos del sistema y otros componentes de AIX.

La gestión del sistema operativo es la tarea de la persona a la que normalmente se denomina, en la documentación de UNIX, administrador del sistema. Desafortunadamente, sólo unas cuantas actividades del administrador del sistema son lo suficientemente sencillas para denominarse correctamente administración. Esta publicación y las guías relacionadas están pensadas para ayudar a los administradores del sistema en sus numerosas obligaciones.

Este sistema operativo proporciona su propia versión de soporte de gestión del sistema para promocionar el fácil uso y mejorar la seguridad y la integridad.

Interfaces de gestión del sistema disponibles

Además de la administración del sistema convencional de la línea de mandatos, este sistema operativo proporciona las interfaces SMIT.

Datos vitales del producto de software

Determinada información de los productos de software y sus opciones instalables se mantiene en la base de datos de Datos Vitales del Producto de Software (SWVPD).

Actualizaciones del sistema operativo

El paquete del sistema operativo se divide en catálogos de archivos, en los que cada catálogo de archivo contiene un grupo de archivos relacionados lógicamente que se pueden entregar al cliente. Cada catálogo de archivos se puede instalar y actualizar individualmente.

Arranque del sistema

Cuando se inicia el sistema operativo base, el sistema inicia un conjunto de tareas complejo. Bajo condiciones normales, estas tareas se realizan automáticamente.

Copia de seguridad del sistema

Una vez que el sistema esté en marcha, la siguiente consideración que debe tener en cuenta debe ser hacer copia de seguridad de los sistemas de archivos, directorios y archivos. Si hace copia de seguridad de los sistemas de archivos, puede restaurar los archivos o los sistemas de archivos en caso de que el disco duro se cuelgue. Hay métodos diferentes para hacer copia de seguridad de la información.

Cierre del sistema

El mandato shutdown es la manera más segura y minuciosa de detener el sistema operativo.

Entorno del sistema

El entorno del sistema es principalmente el conjunto de variables que definen o controlan determinados aspectos de la ejecución del proceso.

Datos de medida de uso de AIX (etiquetas de SLM) para IBM License Metric Tool

Las etiquetas de Software License Metric (SLM) generadas por el sistema operativo AIX sirven como datos de medida de uso empleados por IBM® License Metric Tool. Los datos de medida de uso registran la información de virtual CPU (vCPU) que representa el número de CPU virtuales que están en línea en el sistema.

AIX Runtime Expert

AIX Runtime Expert proporciona un conjunto de acciones simplificadas que se pueden utilizar sobre una única consolidación para recopilar, aplicar y verificar el entorno de ejecución para una o varias instancias de AIX.

Mandatos y procesos

Un mandato es una petición para realizar una operación o para ejecutar un programa. Un proceso es un programa o mandato que se ejecuta realmente en el sistema.

Gestión del sistema colgado

La gestión del sistema colgado permite a los usuarios ejecutar aplicaciones importantes para la actividad continuamente mientras mejora la disponibilidad de la aplicación. La detección del sistema colgado alerta al administrador del sistema de posibles problemas y permite al administrador iniciar la sesión como root o rearrancar el sistema para resolver el problema.

Gestión de procesos

El proceso es la entidad que el sistema operativo utiliza para controlar el uso de los recursos del sistema. Las hebras pueden controlar el consumo de tiempo del procesador pero la mayoría de herramientas de gestión del sistema siguen necesitando que el usuario haga referencia al proceso en el que se ejecuta una hebra, en lugar de la propia hebra.

Contabilidad del sistema

El programa de utilidad de contabilidad del sistema permite recopilar datos e informar acerca del uso individual y de grupo de distintos recursos del sistema.

Controlador de recursos del sistema

El Controlador de recursos del sistema (SRC) proporciona un conjunto de mandatos y subrutinas para facilitar la creación y control de subsistemas al gestor y programador del sistema.

Archivos del sistema operativo

Los archivos se utilizan para toda la entrada y salida (E/S) de información del sistema operativo, para estandarizar el acceso al software y al hardware.

Shells del sistema operativo

La interfaz con el sistema operativo se denomina shell.

Seguridad del sistema operativo

La finalidad de la seguridad del sistema consiste en proteger la información que se almacena en el sistema.

Entorno de usuario

Cada nombre de inicio de sesión tiene su propio entorno del sistema.

Consulta de sistemas BSD

Este apéndice está dirigido a los administradores del sistema que están familiarizados con los sistemas operativos 4.3 BSD UNIX o System V. Esta información explica las diferencias y similitudes entre estos sistemas y AIX.

Redirección de la entrada y la salida

El sistema operativo AIX permite manipular la entrada y salida (E/S) de datos hacia y desde el sistema utilizando mandatos y símbolos de E/S específicos.

Recuperación de kernel de AIX

Desde AIX 6.1, se pueden recuperar opcionalmente los errores del kernel en determinadas rutinas, lo que evita la inactividad no planificada del sistema.

# UNIDAD IV

# SISTEMAS DISTRIBUIDOS

Los objetivos principales que buscan los sistemas distribuidos son la Transparencia, Fiabilidad (disponibilidad y coherencia), Rendimiento, Escalabilidad, Flexibilidad y Seguridad. Cada uno de los distintos modelos de sistemas distribuidos requieren diferentes facetas de estos objetivos.

## 4.1.- Infraestructura y arquitectura de los sistemas distribuidos.

La organización de los sistemas distribuidos depende mayormente de los componentes de software que constituyen al sistema. Estas arquitecturas de software establecen como son organizados varios componentes del software y cómo interactúan entre ellos.

La implementación de un sistema distribuido requiere de la división e identificación de los componentes de software y su instalación en máquinas reales. La implementación e instalación final de la arquitectura de software se conoce como arquitectura de software.

Existen varias configuraciones de componentes y conectores que definen el estilo arquitectónico de un sistema distribuido. Los estilos más importantes son:

• Arquitecturas en capas

• Arquitecturas basadas en objetos

• Arquitecturas centradas en datos

La idea básica tras el estilo arquitectónico en capas es simple: los componentes están organizados en forma de capas, en la que un componente en una determinada capa puede llamar a componentes en la capa inmediata inferior. Una observación clave es que el control generalmente fluye de capa en capa: las peticiones van de arriba abajo y los resultados de abajo a arriba.

Instancias de arquitecturas

Ya que se ha discutido brevemente sobre algunos estilos arquitectónicos comunes, se verá cómo muchos sistemas distribuidos están organizados, considerando la manera en que sus componentes de software fueron establecidos. El determinar que componentes de software se usarán, cómo interactuarán y cómo se distribuirán es lo que se conoce como una instancia de arquitectura también llamada arquitectura de sistema.

Arquitecturas Cliente-Servidor

A pesar de las diferencias en cuanto a varios aspectos de los sistemas distribuidos, solo hay un aspecto en los que muchos expertos coinciden: pensar en términos de clientes que

solicitan servicios a servidores ayuda a entender y administrar la complejidad de los sistemas distribuidos.

La importancia de una arquitectura distribuida

El rendimiento de los ordenadores para realizar procesamiento de datos y almacenar información va relacionado con sus prestaciones de hardware y con el software que utilicen. Una forma de incrementar este rendimiento es utilizando sistemas distribuidos donde un conjunto de ordenadores independientes funciona como uno solo a ojos del usuario, incrementando la capacidad y velocidad de procesamiento y almacenamiento, de forma notoria. Los sistemas distribuidos son independientes de los componentes que lo forman aportando una gran fiabilidad y garantizando una alta disponibilidad.

Son muchos los usos que tienen este tipo de arquitecturas entre los que podemos destacar los sistemas de bases de datos distribuidas, el servicio de world wide web o las aplicaciones cloud de Google.

Qué es un sistema distribuido y sus características

Se define como sistema distribuido a un conjunto o grupo de equipos que son independientes entre sí y que actúan como un único equipo de forma transparente y que tienen como objetivo la descentralización del procesamiento o el almacenamiento de información.

La distribución distribuida permite obtener grandes prestaciones con un coste razonablemente bajo. En la actualidad, la mayoría de sistemas informáticos son distribuidos y no dependen de un único nodo o equipo para funcionar.

Las principales características de un sistema distribuido son:

Concurrencia. Una arquitectura distribuida permite que sea utilizada por todos los usuarios que interactúan en la red.

Modularidad. Esta característica permite que los sistemas distribuidos sean escalables, teniendo capacidad para crecer de forma simple y eficiente.

Transparencia. Proporcionando a los usuarios y las aplicaciones una visión de los recursos del sistema como si se tratase de una única máquina o equipo.

No depende de los componentes. Un sistema distribuido no depende de los distintos componentes hardware que lo forman, ya que, si alguno falla, los demás continúan con los procesos sin que el sistema se vea interrumpido o sufra pérdidas de datos.

Apertura. La arquitectura distribuida permite añadir nuevos servicios que compartan los recursos existentes sin perjudicar los servicios que ya se están ejecutando. Por eso deben estar diseñados sobre protocolos estándar que permitan utilizar hardware y software de distintos fabricantes o desarrolladores.

Carencia de reloj global. Las coordinaciones para la transferencia de mensajes entre los diferentes equipos para la resolución de una o varias tareas, no tienen una temporización general, es decir, se encuentra distribuida a los componentes.

Ventajas y desventajas de una arquitectura distribuida

Ventajas de la arquitectura distribuida

Utilizar un conjunto de ordenadores independientes para que realicen procesos o almacenen datos como si se tratase de un único equipo ofrece una serie de beneficios entre los que podemos destacar:

Incrementa la eficacia

Los sistemas distribuidos permiten afrontar problemas y proyectos que necesitan de procesamientos complejos de forma más eficiente y a un menor coste. El uso de múltiples nodos para procesar una o múltiples tareas supone un mayor rendimiento al optimizar la distribución del mismo en los diferentes sitios de la red.

Mayor tolerancia a los errores

Una arquitectura distribuida tiene una mayor tolerancia a los fallos, ya que al caer un nodo la información se encontrará en otros. Se trata de un sistema mucho más robusto que uno

centralizado debido a esta tolerancia a los fallos sin que se vean afectados los procesos o los datos.

Al estar distribuida la carga de trabajo en muchos nodos distintos, ante el fallo de uno de ellos los demás no se verán afectados y el sistema continúa funcionando, lo que permite afirmar que los sistemas distribuidos son más confiables que los centralizados.

Proporciona una mayor velocidad

Una arquitectura distribuida se caracteriza por proporcionar una mayor velocidad en el procesamiento. Por ejemplo, si se realiza una consulta a una base de datos, los procedimientos se dividen entre los distintos nodos, obteniendo una respuesta mucho más rápida que si se realiza con un único nodo.

Flexibilidad y escalabilidad

Un sistema distribuido puede ser ampliado de forma horizontal en caso de necesidad de incremento de alguna de sus características, como procesamiento (CPU), almacenamiento o memoria RAM. En lugar de aumentar de forma vertical la capacidad de los equipos, el sistema distribuido se aumenta de forma horizontal añadiendo un nuevo nodo. Un sistema distribuido puede añadir recursos para satisfacer las nuevas demandas sobre el sistema.

Desventajas de la arquitectura distribuida

A pesar de las enormes ventajas de los sistemas distribuidos, hay algunos inconvenientes relacionados con este tipo de arquitecturas como pueden ser:

Mayor nivel de complejidad

En comparación con los sistemas centralizados, los distribuidos tienen un mayor nivel de complejidad a la hora de diseñarlos, configurarlos y gestionarlos de forma eficiente.

Seguridad

Los sistemas distribuidos conectan muchos nodos a través de la red y son muchos los usuarios que acceden a la misma, lo que lleva aparejado un aumento del riesgo en la integridad y privacidad de los datos y las comunicaciones.

Precisamente por este motivo es necesario adoptar medidas de seguridad adicionales para este tipo de arquitectura, de modo que se pueda compensar el riesgo de potenciales ataques, o en caso de producirse, mitigar sus efectos.

Mayor esfuerzo

La gestión de un sistema distribuido requiere de un mayor esfuerzo por parte de los administradores, ya que el sistema puede incluir máquinas que dispongan de diferentes sistemas operativos o distintas versiones de los mismos. Hacer funcionar toda esta arquitectura de forma eficiente es mucho más complicado que en un sistema único centralizado y requiere del uso de protocolos estándar.

En qué casos es recomendable la arquitectura distribuida

La arquitectura distribuida es utilizada hoy en día en la mayoría de sistemas informáticos existentes como:

Aplicaciones comerciales como software bancarias o sistemas de gestión de grandes empresas tipo SAP o aplicaciones CRM.

Servicios en la nube como correo electrónico, almacenamiento cloud, o world wide web.

Contenido multimedia incluyendo enseñanza online, videojuegos multijugador o servicios de videoconferencia.

Sistemas informáticos complejos que incluyan base de datos distribuidas, telecomunicaciones, sistemas operativos distribuidos, servidores de ficheros y lenguajes de programación.

Los sistemas distribuidos se han convertido en la arquitectura más utilizada en la actualidad para diseñar y construir sistemas informáticos. Consisten en ordenadores separados físicamente unos de otros que cuentan con sus propias especificaciones de hardware y su sistema operativo individual, pero que se comunican a través de una red para funcionar como un sistema único.

La arquitectura distribuida permite realizar procesos con mayor velocidad y eficiencia, disponiendo de una gran tolerancia a fallos, pues la caída de uno de los equipos que la forman no interrumpe el funcionamiento general del sistema. Sin embargo, la gestión de este tipo de sistemas es mucho más compleja que la realizada en sistemas centralizados.

## 4.2.- Mecanismos de comunicación de bajo nivel.

La comunicación entre procesos, en inglés IPC (Inter-process Communication) es una función básica de los sistemas operativos. Los procesos pueden comunicarse entre sí a través de compartir espacios de memoria, ya sean variables compartidas o buffers, o a través de las herramientas provistas por las rutinas de IPC. La IPC provee un mecanismo que permite a los procesos comunicarse y sincronizarse entre sí, normalmente a través de un sistema de bajo nivel de paso de mensajes que ofrece la red subyacente.

La comunicación se establece siguiendo una serie de reglas (protocolos de comunicación). Los protocolos desarrollados para internet son los mayormente usados: IP (capa de red), protocolo de control de transmisión (capa de transporte) y protocolo de transferencia de archivos, protocolo de transferencia de hipertexto (capa de aplicación).

Los procesos pueden estar ejecutándose en una o más computadoras conectadas a una red. Las técnicas de IPC están divididas dentro de métodos para: paso de mensajes, sincronización, memoria compartida y llamadas de procediemientos remotos (RPC). El método de IPC usado puede variar dependiendo del ancho de banda y latencia (el tiempo desde el pedido de información y el comienzo del envío de la misma) de la comunicación entre procesos, y del tipo de datos que están siendo comunicados.

El sistema operativo provee mínimamente dos primitivas, enviar y recibir, normalmente llamadas send y receive. Asimismo, debe implementarse un enlace de comunicación entre los procesos de la comunicación. Este enlace puede ser unidireccional o multidireccional según permita la comunicación en solo uno o en varios sentidos.

Tipos de comunicación

La comunicación puede ser:

Síncrona o asíncrona

Persistente (persistent) o momentánea (transient)

Directa o indirecta

Simétrica o asimétrica

Con uso de buffers explícito o automático

Envío por copia del mensaje o por referencia

Mensajes de tamaño fijo o variable

Síncrona

Quien envía permanece bloqueado esperando a que llegue una respuesta del receptor antes de realizar cualquier otro ejercicio.

Asíncrona

Quien envía continúa con su ejecución inmediatamente después de enviar el mensaje al receptor.

Persistente

El receptor no tiene que estar operativo al mismo tiempo que se realiza la comunicación, el mensaje se almacena tanto tiempo como sea necesario para poder ser entregado (Ej.: e-Mail).

Momentánea (transient)

El mensaje se descarta si el receptor no está operativo al tiempo que se realiza la comunicación. Por lo tanto, no será entregado.

Directa

Las primitivas enviar y recibir explicitan el nombre del proceso con el que se comunican. Ejemplo:

enviar (mensaje, A) envía un mensaje al proceso A

Es decir, se debe especificar cuál va a ser el proceso fuente y cuál va a ser el proceso Destino.

Las operaciones básicas Send y Receive se definen de la siguiente manera: Send (P, mensaje); envía un mensaje al proceso P (P es el proceso destino). Receive (Q, mensaje); espera la recepción de un mensaje por parte del proceso Q (Q es el proceso fuente).

Nota: Receive puede esperar de un proceso cualquiera, un mensaje, pero el Send sí debe especificar a quién va dirigido y cuál es el mensaje.

Indirecta

La comunicación Indirecta: Es aquella donde la comunicación está basada en una herramienta o instrumento ya que el emisor y el receptor están a distancia.

Simétrica

Todos los procesos pueden enviar o recibir. También llamada bidireccional para el caso de dos procesos.

Asimétrica

Un proceso puede enviar, los demás procesos solo reciben. También llamada unidireccional. Suele usarse para hospedar servidores en Internet.

Uso de buffers automático

El transmisor se bloquea hasta que el receptor recibe el mensaje (capacidad cero).

## 4.3.- Servicios de sistema para entornos distribuidos.

Más allá de los esfuerzos por construir estándares para mejorar la interoperabilidad y de la existencia de plataformas Web mucho más accesibles al programador y al usuario, el desarrollo de aplicaciones distribuidas a gran escala, seguía adoleciendo de problemas de integración.

La idea de construcción de aplicaciones integradas permitió que las organizaciones desarrollen software que resuelva cada parte de su negocio y se integre con aplicaciones que gestionen la parte administrativa de dicho negocio. En este sentido la idea de integración de aplicaciones comienza a cobrar un sentido muy relevante.

En este contexto surgen los sistemas ERP (Enterprise Resource Planning) que proveen variada funcionalidad integrada por un único repositorio de datos.

No se tardó demasiado en intentar agregar valor a los desarrollos de las organizaciones aportando sistemas de CRM(Customer Relationship Management) o sistemas de DataWareHouse que requieren algún tipo de integración con los sistemas de índole operativa o propia del negocio.

Esta integración se enfoca principalmente en la integración vía el modelo de datos. Este tipo de integración ha sufrido una evolución e incluye diversas variantes que se describen a continuación.

Integración Punto a Punto

Se basa en integración uno a uno sustentada generalmente por un middleware asincrónico basado en colas de mensajes. Si bien es un esquema de alta disponibilidad, dada por el mecanismo de comunicación, es rígido y difícil de adaptar a los cambios, además de resultar muy costoso de gestionar, monitorear y extender. Es una arquitectura accidental, completamente sincrónica, de grano grueso y poco escalable.

Mecanismo de integración por adaptadores Mediador de mensajes Este mecanismo de integración representa una evolución del modelo anterior hacia una generalización del hub permitiendo extraer la lógica de la integración fuera de las aplicaciones. Se define declarativamente la forma de comunicación de las aplicaciones y se traslada al mediador o " broker " la lógica necesaria para producir las transformaciones que generen salidas válidas para el otro extremo. Utiliza colas para garantizar la distribución de los mensajes, que se manejan con un esquema de publicador/suscriptor. Esto asegura que el tráfico que se genera sea solamente el requerido.

## 4.4.- Diseño de aplicaciones distribuidas.

Aplicación hecha de distintos componentes que se ejecutan en entornos de ejecución separados, generalmente sobre diferentes plataformas conectadas por una red.

Las aplicaciones distribuidas típicas son las cliente/servidor (two-tier), cliente/middleware/servidor (middleware o three-tier) y multitier.

Es una aplicación con distintos componentes que se ejecutan en entornos separados, normalmente en diferentes plataformas conectadas a través de una red. Las típicas aplicaciones distribuidas son de dos niveles (cliente-servidor), tres niveles (cliente-middleware-servidor) y multinivel.

El diseño de aplicaciones modernas involucra la división de una aplicación en múltiples capas; la interface de usuario, la capa media de objetos de negocios, y la capa de acceso a datos. Puede ser útil identificar los tipos de procesamiento que podemos esperar que una aplicación realice. Muchas aplicaciones pueden, al menos, hacer lo siguiente:

Cálculos u otros procesos de negocios.

Ejecución de reglas de negocios.

Validación de datos relacionados al negocio.

Manipulación de datos.

Ejecución de las reglas de datos relacional.

Interactuar con aplicaciones externas o servicios.

Interactuar con otros usuarios.

Nosotros podemos tomar estos tipos de servicios y generalizarlos dentro de los tres grupos o capas que a continuación se resumen:

Interfase de usuario (Capa de Presentación)

Interactuar con otros usuarios.

Interactuar con aplicaciones externas o servicios.

Procesos de negocios (Capa de Negocios)

Cálculos u otros procesos de negocios.

Ejecución de reglas de negocios.

Validación de datos relacionados al negocio.

Procesos de datos (Capa de Servicios de Datos).

Manipulación de datos.

Ejecución de las reglas de datos relacional.

La división de estos procesos de aplicaciones y su distribución entre diferentes procesos cliente/servidor es conocido como Procesamiento Distribuido. Generalizando estos procesos dentro de estas tres categorías o capas es una distribución lógica y no refleja necesariamente alguna opción de diseño físico sobre computadoras, terminales u otros equipos. Usted puede desarrollar una aplicación cliente/servidor distribuida basada sobre estas tres capas de Presentación, Lógica de Negocios y Servicios de Datos y tener la aplicación entera corriendo sobre una simple computadora. Alternativamente, usted puede esparcir estas tres capas a través de un gran número de diferentes computadoras sobre una red. De cualquier forma usted ha desarrollado una aplicación cliente/servidor de tres capas.

Capa de Presentación.

La capa de Presentación provee su aplicación con una interfase de usuario(IU). Aquí es donde su aplicación presenta información a los usuarios y acepta entradas o respuestas del usuario para usar por su programa. Idealmente, la IU no desarrolla ningún procesamiento de negocios o reglas de validación de negocios. Por el contrario, la IU debería relegar sobre la capa de negocios para manipular estos asuntos. Esto es importante, especialmente hoy en día, debido a que es muy común para una aplicación tener múltiples IU, o para sus clientes o usuarios, que le solicitan que elimine una IU y la remplace con otra. Por ejemplo, usted

puede desarrollar una aplicación Win32 (un programa en Visual Basic) y entonces solicitársele remplazarla con una página HTLM., quizás usando tecnología ASP.

Una de las mayores dificultades y factores importantes cuando desarrollamos aplicaciones cliente/servidor es mantener una separación completa entre la presentación, la lógica de negocios y los servicios de datos. Es muy tentador para los desarrolladores mezclar una o más capas; poniendo alguna validación u otro proceso de negocios dentro de la capa de presentación en vez de en la capa de negocios.

Capa de Negocios.

Toda aplicación tiene código para implementar reglas de negocios, procesos relacionados a los datos o cálculos y otras actividades relativas a los negocios. Colectivamente este código es considerado para formar la capa de negocios. Otra vez, uno de los principios del diseño lógico cliente/servidor, la lógica de negocios debe mantenerse separada de la capa de presentación y de los servicios de datos. Esto no significa necesariamente que la lógica de negocios está en cualquier parte, por el contrario, esta separación es en un sentido lógico.

Hay muchas formas de separar la lógica de negocios. En términos orientados a objetos, usted debería encapsular la lógica de negocios en un conjunto de objetos o componentes que no contienen presentación o código de servicios de datos. Teniendo separada lógicamente su lógica de negocios de ambas, la capa de presentación y servicios de datos, usted ganará en flexibilidad en término de donde usted puede almacenar físicamente la lógica de negocios. Por ejemplo, usted puede seleccionar almacenar la lógica de negocios sobre cada estación de cliente, u optar por ejecutar la lógica de negocios sobre un servidor de aplicaciones, permitiendo a todos los clientes acceder a un recurso centralizado.

Los objetos de negocios son diseñados para reflejar o representar sus negocios. Ellos se convierten en un modelo de sus entidades de negocios e interrelaciones. Esto incluye tanto objetos físicos como conceptos abstractos. Estos son algunos ejemplos de objetos del mundo real: un empleado, un cliente, un producto, una orden de compra.

Todos estos son objetos en el mundo físico, y la idea en su totalidad detrás de usar objetos de negocios de software, es crear una representación de los mismos objetos dentro de su

aplicación. Sus aplicaciones pueden hacer que estos objetos interactúen unos con otros como ellos lo hacen en el mundo real. Por ejemplo, un empleado puede crear una orden de compra a un cliente que contiene una lista de productos. Siguiendo esta lógica usted puede crear objetos de negocios de una orden conteniendo el código necesario para administrarse a si mismo, así usted nunca necesitará replicar código para crear ordenes, usted solo usará el objeto. Similarmente, un objeto cliente contiene y administra sus propios datos. Un buen diseño de un objeto cliente contiene todos los datos y rutinas necesitadas para representarlo a través del negocio completo, y puede ser usado a través de toda la aplicación de ese negocio.

No toda la lógica de negocio es la misma. Alguna lógica de negocio es un proceso intensivo de datos, requiriendo un eficiente y rápido acceso a la base de datos. Otras no requieren un frecuente acceso a los datos, pero es de uso frecuente por una interfase de usuario robusta para la validación en la entrada de campos u otras interacciones de usuarios. Si nosotros necesitamos una validación al nivel de pantallas y quizás cálculos en tiempos real u otra lógica de negocios, pudiéramos considerar este tipo de lógica de negocios para ser parte de la IU, ya que en su mayor parte es usada por la interfase de usuario.

Una alternativa de solución es dividir la capa de lógica de negocios en dos:

Objetos de negocios de la IU.

Objetos de negocios de datos.

Un ejemplo del objeto Empleado de la capa objetos de negocios de la IU proveerá propiedades y métodos para usar por el diseñador de la interfase de usuario. Ejemplo de propiedades y métodos pudieran ser: IDEmpleado, Nombre, Dirección, etc., y como métodos crear una de compra, etc. El objeto Empleado de la capa de objetos de negocios de datos será responsable de los mecanismos de persistencias, interactuar con la base de datos. Los objetos de esta capa son considerados sin estado, solo poseen métodos.

Capa de Servicios de Datos.

Muchas aplicaciones interactúan con datos, los almacenan en alguna forma de bases de datos. Hay algunas funciones básicas que son comunes a todos los procesos. Estas incluyen:

Crear datos,

leer datos,

actualizar datos y

eliminar datos.

Adicionalmente, nosotros tenemos servicios más avanzados disponibles, tales como: búsquedas, ordenamientos, filtrados, etc.

## Bibliografía básica y complementaria:

Sistemas Operativos Distribuidos Andrew S. Tanenbaum. 1996, Prentice-Hall Capítulo 1

Última edición en inglés: Distributed Systems: Principles and Paradigms 2002, Prentice-Hall