ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ASIGNATURA: Línea de énfasis III

CORPORACIÓN UNIVERSITARIA REMINGTON
DIRECCIÓN PEDAGÓGICA

2011

CRÉDITOS

AUTOR

Elizabeth Díaz Duque
Ingeniera de Sistemas de la Universidad EAFIT Medellín
Especialista en Pedagogía de la Virtualidad de la Fundación Universitaria Católica del Norte
Diplomatura en Ambientes Virtuales de Aprendizaje
Me he desempeñado como jefe de Área de Informática y Tecnología del Colegio Gimnasio Los Pinares de Medellín, además soy docente de dicha asignatura (en inglés) durante los últimos 5 años
ediazduque@gmail.com

Nota: el autor certificó (de manera verbal o escrita) No haber incurrido en fraude científico, plagio o vicios de autoría; en caso contrario eximió de toda responsabilidad a la Corporación Universitaria Remington, y se declaró como el único responsable.

RESPONSABLES

Jorge Mauricio Sepúlveda Castaño
Director del programa Escuela de Ciencias Básicas e Ingeniería

Director Pedagógico
Octavio Toro Chica
dirpedagogica.director@remington.edu.co

Coordinadora de Medios y Mediaciones
Angélica Ricaurte Avendaño
mediaciones.coordinador01@remington.edu.co

GRUPO DE APOYO

Personal de la Unidad de Medios y Mediaciones
EDICIÓN Y MONTAJE
Primera versión. Febrero de 2011.

TABLA DE CONTENIDO

1. MAPA DE LA ASIGNATURA

LÍNEA DE ÉNFASIS III- REDES Y COMUNICACIONES

PROPÓSITO GENERAL DEL MÓDULO

Con este módulo de trabajo se pretende hacer una introducción a los estudiantes hacia los conceptos básicos que están en el campo de las "Redes y Comunicaciones", y que a través de las ejemplificaciones expuestas, los educandos pueden tener una idea general del manejo y el uso que se le da en las organizaciones a los sistemas de Redes y Comunicaciones.

OBJETIVO GENERAL

Introducir a los estudiantes en el contexto de las Redes y las Comunicaciones y que comprenda el concepto de seguridad a través del análisis de las fortalezas y las debilidades a las que las organizaciones están expuestos hoy en día

OBJETIVOS ESPECÍFICOS

- Entender la seguridad informática como el campo que da la garantía de que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.
- Describir panorámicamente los aspectos relevantes, involucrados en los Sistemas Distribuidos.
- Estructurar el modelo, el diseño y la evaluación de los sistemas de comunicaciones inalámbricos tanto con características de usuario estático como de usuario móvil.

UNIDAD 1	UNIDAD 2	UNIDAD 3
Seguridad en las redes Desarrollo conceptual-	Sistemas distribuidos Desarrollo conceptual-	Comunicaciones inalámbricas y servicios en la red Desarrollo conceptual

2. SEGURIDAD EN LAS REDES

OBJETIVO GENERAL

Entender la seguridad informática como el campo que da la garantía de que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

OBJETIVOS ESPECÍFICOS

- Introducir a los estudiantes en los conceptos base del campo de la seguridad en la redes dentro de una organización.
- Analizar el impacto del manejo de las redes y su implementación de seguridad dentro de cualquier organización.

Prueba Inicial

COMENCEMOS

Defina en sus propias palabras, lo que para usted es:

1. -Seguridad
2. -Redes
3. -Seguridad en las Redes

TEMAS

Conceptos y Definiciones
Impacto en las Organizaciones

2.1. Conceptos y Definiciones

Antes de comenzar, veamos el siguiente video introductorio al tema: “Innovación. Seguridad y Redes: Sistemas de detección de intrusos”, en:
http://www.youtube.com/watch?v=5rLfJhsO2CY

Hoy en día las diferentes organizaciones dependen cada vez más de sus redes informáticas, y cualquier problema que cause alguna afectación puede incurrir en problemas graves y hasta imposibilitar su modus operandi.

Una de las principales causas para que esto suceda es la falta de medidas en los protocolos de seguridad, y que esto cada vez más se convierte en un grave problema que se nos crece día a día de una manera muy rápida, pues el número de personas que quieren atacar las diferentes redes de las organizaciones es cada vez más alto y además estos cada vez se vuelven más especializados con el fin de cada vez obtener mejores resultados en sus operaciones.

Ahora es muy importante tener en cuenta y no pasar por alto la misma organización de la red, pues su misma complejidad puede dificultar la detección oportuna de errores o problemas de seguridad y permitir entonces sus ajustes o corrección.

En nuestro medio se han ido aumentando diferentes tipos de acciones que violan la seguridad de los recursos de los sistemas; algunos conocidos como “Hackers” y otros como “Crackers”, han hecho que en nuestro vocabulario aparezcan nuevos términos, que se vuelven del uso común de usuarios y también de quienes tienen a cargo la administración de las redes.

En el momento de organizar y plantearse en qué elementos del sistema deben estar ubicados los servicios de seguridad, podríamos definir dos aspectos fundamentales para ello.

1. La protección de los sistemas de transporte de datos: aquí el administrador asume total responsabilidad, con la que le garantice al usuario la recepción de la información de una manera segura.
2. Algunos ejemplos de cómo hacer esto es la implementación de servicios MTAs (Mail Transport Agents), o la instalación de un firewall para defender el acceso a una parte protegida de alguna red.

3. Aplicaciones Seguras Extremo a Extremo: miremos entonces el ejemplo de un correo electrónico. Enviar un mail o correo es simplemente enviar un mensaje cuyo contenido ha sido encapsulado previamente al envío, y así el mensaje puede atravesar sistemas poco fiables y no muy homogéneos, pero sin perder la validez de los servicios de seguridad provistos.

En este caso el usuario final es el encargado de asegurar el mensaje, también es cierto que el responsable de la seguridad en la organización que provee su cuenta de mensajería, le debe proporcionar una herramienta amigable para ello.

Este mismo análisis puede usarse para el uso de aplicaciones como videoconferencia, accesos a bases de datos remotas, entre otras.

En estos dos aspectos que analizamos, un problema grande que debe tenerse en cuenta es la administración de "claves o passwords".

COCEPTOS DE SEGURIDAD

- La seguridad informática hoy por hoy a tomado gran fuerza, puesto que las diferentes plataformas informáticas que existen, nos plantean diferentes condiciones.

- Existe la posibilidad de interconexión a través de las redes y esto ha ampliado los horizontes que nos permiten explorar la organización más allá de sus muros; pero esta situación también ha dejado que nuevas amenazas para los sistemas aparezcan cada día.

- Muchas organizaciones de carácter gubernamental o de otros, han dirigido el uso adecuado de estas tecnologías a través del desarrollo de directrices que son documentos que permiten hacer recomendaciones con el fin de tener mejor provecho de las ventajas que estas tecnologías ofrecen y así evitar los malos usos. Esto es una gran ayuda para cualquier empresa, pues es una manera de asegurar los bienes y servicios de la misma.

- Las políticas de seguridad se han vuelto entonces una de las herramientas de la organización con la cual se pretende sensibilizar a los miembros de la organización sobre la importancia del buen manejo de la información de la organización y su buen funcionamiento.

¿QUÉ VALOR TIENEN LOS DATOS?

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su carácter de intangible, caso opuesto al de los equipos, la documentación o las aplicaciones.

Cuando hablamos de darle valor a la información hablamos, por ejemplo, a qué tan peligroso es enviar la información de mi tarjeta de crédito a través de Internet para hacer una compra, en una red gigantesca donde viajan no únicamente los 16 dígitos de mi tarjeta de crédito sino millones de datos más.

Pero ya esto es un tema bastante complicado que se debe analizar mucho más afondo, pues muchos expertos dicen que es incluso más peligroso entregarle la tarjeta al empleado de un almacén o hacer una transacción telefónica con ella.

El peligro como tal se enfoca no en el envío de la información sino una vez que ésta más de la muchos otros miles de clientes reposa en una base de datos de una compañía, con un único acceso no autorizado a esta base de datos, es posible que alguien obtenga no únicamente mis datos y los de mi tarjeta, sino que tendrá acceso a los datos y tarjetas de todos los clientes de esta compañía.

Ahora veamos la seguridad en las redes, que en efecto este tema no está estrictamente ligado a "internet", puesto que aunque no se esté conectado a Internet, una red está expuesta a distintos tipos de ataques electrónicos, incluidos los virus.

Miremos a manera de ejemplo como se le puede asignar valores a los delitos electrónicos, el caso de la agencia norteamericana Defense Information Systems Agency titulado "Defending the Defense Information Infrastructure- Defense Information Systems Agency", del 9 de julio de 1996. En dicho informe las corporaciones más grandes de los Estados Unidos reportan haber experimentado pérdidas estimadas en U$S 800 millones dólares en 1996 debido a ataques a la red. Asimismo el informe de marzo de 1997 de The Computer Security Institute (CSI) indica que el crimen de cómputo continúa en alza y se reportan pérdidas superiores a los U$S 100 millones de dólares y esto es tan solo durante el primer cuarto del año 1997. Si, además, tenemos en cuenta que según las estadísticas de estas agencias norteamericanas sólo 1 de cada 500 ataques son detectados y reportados, ya es posible hacerse una idea de los valores involucrados en este tipo de delito.

Este es uno de los ejemplos que nos sirve para entender la necesidad que tiene cualquier organización que trabaje con equipos de cómputo, y más aún, con redes, se le hace totalmente necesario implantar las normas para hacer buen uso de los recursos y de la información misma.

ALGUNAS DEFINICIONES

Es preciso acotar ciertas definiciones que pueden tener muchos y diferentes significados, por eso las listamos a continuación:

- Seguridad: es calidad de seguro
- Seguro: libre de riesgo
- Información: acción y efecto de informar
- Informar: dar noticia de una cosa
- Redes: el conjunto sistemático de caños o de hilos conductores o de vías
- de comunicación o de agencias y servicios o recursos para determinado fin
- Seguridad en Redes:

- Es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin.
- Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Ejercicio del -Tema 1
Defina en cuatro (4) líneas lo que entendió del concepto de seguridad en redes. Use como mínimo 5 conceptos básicos estudiados en el tema 1 y subráyelos a manera de hacer hincapié.

_____
_____
_____
_____
_____

2.2. Impacto en las Organizaciones

EL IMPACTO EN LAS ORGANIZACIONES

La creación de políticas de seguridad, viene de la mano de varios tipos de problemas que pueden afectar el funcionamiento de la organización.

¿Cómo puede la seguridad en las redes impactar a la organización si se implementan para hacer más seguro el sistema?

La verdad de esto consiste en que la implementación de un sistema de seguridad lleva a incrementar la complejidad en las operaciones de la organización, tanto en lo técnico como en lo administrativo.

Por ejemplo, antes de la implementación del sistema de seguridad, cualquier usuario, para acceder a un recurso, debía entrar con un solo usuario (login). Ahora, con la implementación del nuevo esquema de seguridad, debe ingresar haciendo uso de dos usuarios (logines): uno para ingresar al sistema y otro para acceder al recurso.

El usuario entiende esto como un impedimento en su trabajo, en lugar de verlo como una razón de seguridad para él, pues de esta manera, se puede controlar más el uso del recurso y, ante algún problema, será mucho más fácil establecer responsabilidades.

Ahora, al poner en funcionamiento cualquiera norma nueva de seguridad, ésta traerá una nueva tarea para la parte técnica (por ejemplo, cambiar los derechos o privilegios de algunos usuarios) y administrativamente, se les deberá avisar por medio de una nota de los cambios realizados y en qué les afectará.

¿CÓMO SE VISUALIZA EL PROCESO?

En un estudio de "Datapro Research Corp. se resumía que los problemas de seguridad en sistemas basados en redes responde a la siguiente distribución:

- Errores de los empleados 50%
- Empleados deshonestos 15%
- Empleados descuidados 15%
- Otros 20% (Intrusos ajenos a la Empresa 10%; Integridad física de instalaciones
- 10%)
- Se puede notar que el 80% de los problemas, son generados por los empleados
- de la organización, y, éstos se podrían tipificar en tres grandes grupos:

1. Problemas por ignorancia
2. Problemas por Pereza
3. Problemas por malicia".

De todas estas razones que vimos, la ignorancia es la más fácil de direccionar, todo esto a través del desarrollo de tácticas de entrenamiento y procedimientos formales e informales son fácilmente neutralizadas. Los usuarios, además, necesitan de tiempo en tiempo, que se les recuerden cosas que ellos deberían conocer.

La Pereza será siempre un gran problema –tanto para los administradores de sistemas como para los usuarios – pero, se encuentra que éste es un problema menor cuando los usuarios ven las metas de los sistemas de seguridad.

Esto requiere soporte de la Administración, y de la organización como un todo formado por usuarios particulares. Además de esto, un ambiente laboral que se focalice en las soluciones, en vez de la censura, es generalmente más eficiente que aquel que tiende a la coerción o la intimidación.

La malicia, se debe combatir creando una cultura en la organización que aliente la lealtad de los empleados.

La visibilidad consiste en el aporte de las personas de la organización y, dar a conocer las acciones tomadas. Es decir que, cuando se deben producir cambios en las políticas no es necesario que se decidan unilateralmente.

Es muy productivo y aconsejable que se integren grupos de trabajo para discutir y/o conocer el alcance y el tipo de medidas a llevar a cabo. Esto, además de llevar algunas veces a obtener soluciones que son más efectivas que las que se pensaban tomar, hace que aquellos que sean sensibles a los cambios no se sientan recelosos de los cambios realizados y se comprometan con el cambio.

Luego, una vez tomada la decisión, se debe comunicar directamente a todas las personas involucradas en los cambios realizados por medio de cartas, notas o boletines informativos. De esta manera, aseguramos que los hechos son visibles al resto de la organización. Como consecuencia, las personas no sienten resquemores o recelos de las nuevas medidas implementadas y se unen rápidamente a ellas.

Ahora es muy buena y permitente una recomendación, tener en cuenta cuando deban realizarse modificaciones, hacerlas contando con la asesoría de la parte legal. Así, se pueden llegar a establecer los alcances de las penalidades en caso de infringir las normas dictadas.

Así mismo, con respecto a este punto en particular, es muy recordable que las modificaciones o nuevas normativas, así mismo como sus respectivas penalizaciones, estén bien expuestas, ya sea por medio de boletines organizaciones (medios de comunicación internos), o cualquiera otro medio de comunicación organizacional que permita llevar a cabo estas acciones con razonable éxito.

IMPLEMENTACIÓN DE LAS MEDIDAS DE SEGURIDAD

La implementación de medidas de seguridad en la organización, es un proceso que involucra tanto al departamento técnico como al administrativo. Como este proceso debe involucrar a toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la validez que se necesita.

Hay que mirar con lupa el impacto en la organización luego de la implementación de las políticas de seguridad que se hace necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

También, como hemos mencionado anteriormente, es fundamental no dejar de lado la notificación a todos los miembros involucrados en las nuevas normativas y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Pero de todo lo que se ha hablado hay algo que resulta muy claro y es que proponer o identificar una política de seguridad requiere de un alto compromiso con la organización, precisión técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del ambiente que rodea las organizaciones modernas.

POLÍTICAS GENERALES DE SEGURIDAD

DEFINICIÓN:

Una política de Seguridad Informática (PSI) se encarga de establecer un canal formal de la forma de actuar del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

Esto no quiere decir que sea una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a las diferentes conductas erróneas de los empleados. Es más bien una descripción para quienes desean proteger y la razón para ello.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

ELEMENTOS

Las Políticas de Seguridad deben considerar entre muchos otros elementos, los que describimos a continuación:

Alcance de las políticas:

Esto incluye las facilidades, sistemas y el personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios.

Objetivos de la política:

Que consiste en la descripción clara de los elementos involucrados en la definición de las mismas.

Responsabilidades:

Que se definen para cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

Requerimientos mínimos:
Estos son necesarios para la configuración de la seguridad de los sistemas que cubren el alcance de la política.

Definición de violaciones y de las consecuencias:
Esto para los casos del no cumplimiento de la política.

Responsabilidades de los usuarios:
Esta información y definición de responsabilidades con respecto a la información a la que ella tiene acceso. Las PSI deben ofrecer explicaciones bastante claras acerca de por qué deben tomarse ciertas decisiones, es decir, por qué son importantes estos u otros recursos o servicios.

Seguridad en Redes:
Las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje muy claro en el que no se haga uso de tecnicismos ni términos legales que impidan una comprensión clara de esta políticas, esto obviamente sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad encargada en hacer que las cosas ocurran, el rango para los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se pudieran imponer.

Para terminar, las PSI como documentos de la organización, deben seguir un proceso donde haya una permanente actualización y que esté sujeta a los cambios organizacionales relevantes tales como: crecimiento del personal, cambios en infraestructura física o computacional, alta rotación del personal, cambio de negocios, entre otros.

ALGUNOS PARÁMETROS

Ya hemos venido analizando una pequeña perspectiva de las implicaciones que tiene la formulación de las políticas de seguridad, es bueno también que miremos algunas recomendaciones a la hora de documentar y formular estas políticas.

1. Trate de hacer un ejercicio donde haga un análisis de riesgos informáticos, a través del cual valore los activos, y así poder reafirmar las PSI de su organización.

2. Involucre a las áreas propietarias de los recursos o servicios, ya que estos poseen la experiencia y son una fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.

3. Haga una comunicación explícita a todo el personal que esté involucrado en el desarrollo de las PSI, así con los beneficios y riesgos relacionados con los recursos y bienes, y los elementos de seguridad.

4. Es necesario identificar quién tiene la autoridad para tomar ciertas decisiones, pues son ellos los responsables de cuidar los activos de la funcionalidad de su área u organización.

5. Haga un proceso de monitoreo constante de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

6. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI establecidas. No de nada por obvio.

ANÁLISIS PARA LLEVAR A CABO UN SISTEMA DE SEGURIDAD INFORMÁTICA

En el siguiente gráfico veremos los elementos que están involucrados en la asignación de una política de seguridad.

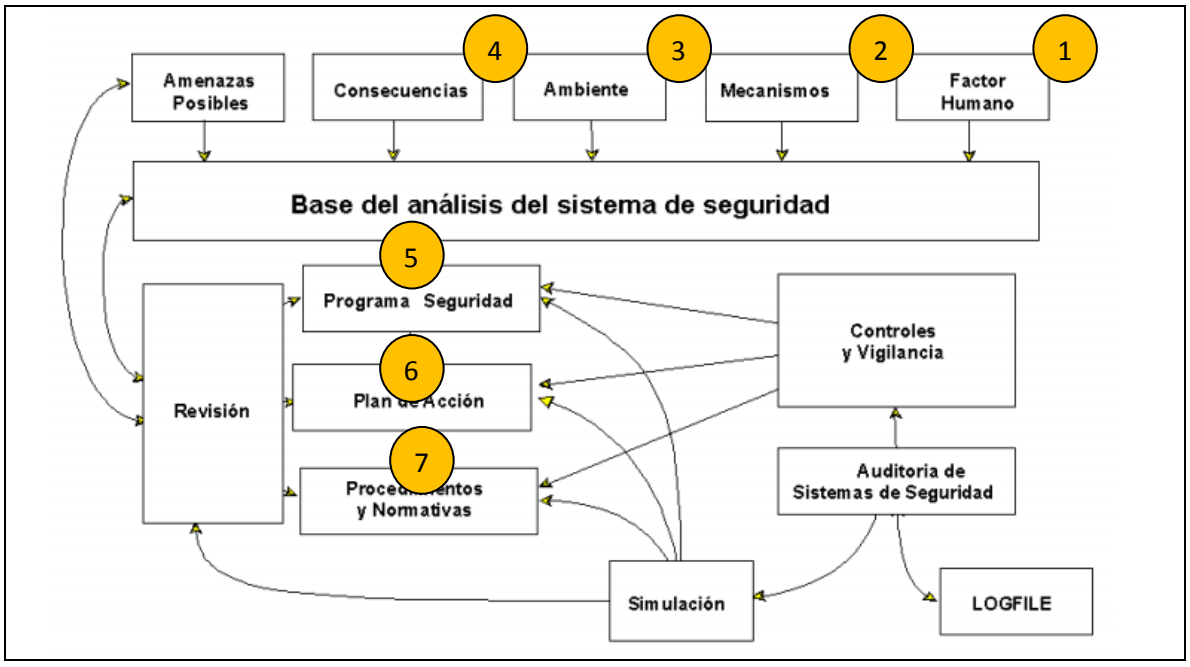


Gráfico: Política de seguridad-elementos-

Analicemos paso a paso en qué consiste este esquema:

1. Se realiza una evaluación del factor humano involucrado, no olvidando que este es el factor más crítico en todo el sistema de seguridad.
2. Se mira el medio ambiente en que se desempeña el sistema.
3. Las consecuencias que puede traer si este trae consigo defectos en la seguridad, tales como: pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.
4. Ahora veamos cuáles son las amenazas posibles.

5. Cuando ya se tiene una evaluación de los cuatro aspectos anteriormente mencionados, se pasa al punto 6.

6. Hacer un programa de seguridad, que involucra los pasos a tomar para poder asegurar el horizonte de seguridad que se desea.

7. Luego, nos vamos al plan de acción, que es en sí la forma de la aplicación del programa de seguridad.

8. Para terminar se procede a la redacción y establecimiento de los procedimientos y normas que permiten llegar al objetivo final.

RIESGOS

Los usuarios suelen autenticarse haciendo uso de una contraseña o password. Pero la idea es buscar alternativas más seguras a través de otros medios como: la firma con reconocimiento automático a través del computador, o el análisis del fondo de ojo, la huella digital entre otras.

Limitándonos a la seguridad propiamente dicha, los riesgos pueden ser múltiples, ahora lo primero que debemos hacer para atacar estos riesgos es conocerlos y así seguidamente poder tomar decisiones al respecto; pues el identificarlos y no hacer nada frente a ellos no tendría lógica, y podríamos estarnos enfrascando en un problema de seguridad que puede acrecentarse cada vez más.

Sabemos además que las acciones que se deben atender tiene un costo y en muchos casos este es alto, y por ende esto conlleva a que los dirigentes de la organización se pregunten cuál sería el riesgo máximo que ellos pudieran hacerle frente.

Una respuesta a este interrogante no es nada fácil, pues esto depende de lo crítico del problema y de la organización en sí. Es tener que analizar el impacto que este le causaría a la organización.

Algunos ejemplos de daños de menor riesgo podrían ser:

- Acceso indebido a los datos
- Ingreso a sesiones no autorizada de soportes magnéticos con información crítica
- Daños por fuego, por agua
- Variación no autorizada de programas, su copia indebida
- Hackers: quienes intentan acceder a los sistemas sobre todo para demostrar la capacidad de superar las barreras de protección que se hayan establecido en cierta organización.

Ahora, los virus también son una gran amenaza que se convierte en un riesgo constante porque de forma continua aparecen nuevas modalidades, que no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan.

Además es necesario entender que los virus pueden llegar a afectar a los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil, ya que por las características y la complejidad de los grandes equipos y debido a las características de diseño de los sistemas operativos.

Luego, podríamos pensar entonces qué sería lo más importante de proteger y podemos decir que los datos son más críticos si pensamos en lo que esto implica para la continuidad de la organización.

Sabemos también que muchos de las pérdidas son asumidas por los seguros de la compañía, pero y qué pasa con las deudas que se generan al no poder recuperar las pérdidas ocasionadas por la pérdida de datos, o por no poder tomar decisiones a tiempo por la misma carencia de esta información desaparecida.

NIVELES DE TRABAJO

Veamos el siguiente listado de niveles de trabajo:

1. Confidencialidad: Esto es la protección de la información contra la lectura no autorizada.
2. Integridad: La información que se vaya a proteger incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos. Esto comprende cualquier tipo de modificaciones:

Causadas por errores de hardware y/o software.
Causadas de forma intencional.
Ausadas de forma accidental. Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

1. Autenticidad: la autenticidad garantiza que quien dice ser "X" es realmente "X".

2. Disponibilidad de los recursos y de la información: La información no sirve de nada si se encuentra en el sistema pero los usuarios no pueden acceder a ella. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

3. Consistencia: Consiste en asegurar que el sistema siempre se comporte de la forma esperada.

4. Control de Acceso: Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que ofrece además de controlar cómo lo hacen.

5. Auditoría: Esto es tener los mecanismos necesarios para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno de los usuarios y los tiempos y fechas de dichas en que estos hacen cualquier operación.

CÓMO ESTABLECER LOS NIVELES DE RIESGO

Veamos a continuación un ejemplo que nos presenta la Coordinación de Emergencia en Redes Teleinformáticas, en su manual de seguridad en las páginas 31 a 36:

“Al crear una política de seguridad de red, es importante entender que la razón para crear tal política es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son costeables. Esto significa que se debe entender cuáles recursos de la red vale la pena proteger y que algunos recursos son más importantes que otros. También se deberá identificar la fuente de amenaza de la que se protege a los recursos. A pesar de la cantidad de publicidad sobre intrusos en una red, varias encuestas indican que para la mayoría de las organizaciones, la pérdida real que proviene de los “miembros internos” es mucho mayor (tal cual se ha explicado anteriormente).

El análisis de riesgos implica determinar lo siguiente:

Qué se necesita proteger
De quién protegerlo
Cómo protegerlo

Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

En el análisis de los riesgos, es necesario determinar los siguientes factores:

Estimación del riesgo de pérdida del recurso (lo llamaremos Ri)
Estimación de la importancia del recurso (lo llamaremos Wi)

Como un paso hacia la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico. Por ejemplo, al riesgo (Ri) de perder un recurso, se le asigna un valor de cero a diez, donde cero, significa que no hay riesgo y diez es el riesgo más alto. De manera similar, a la importancia de un recurso (Wi) también se le puede asignar un valor de cero a diez, donde cero significa que no tiene importancia y diez es la importancia más alta. La evaluación general del riesgo será entonces el producto del valor del riesgo y su importancia (también llamado el peso). Esto puede escribirse como:

WRi
= Ri *Wi
Dónde:
WRi : es el peso del riesgo del recurso "i" (también lo podemos llamar ponderación)
Ri: es el riesgo del recurso "i"
Wi: es la importancia del recurso "i" Seguridad en Redes

Ejemplo práctico
Supongamos una red simplificada con un router, un servidor y un bridge.

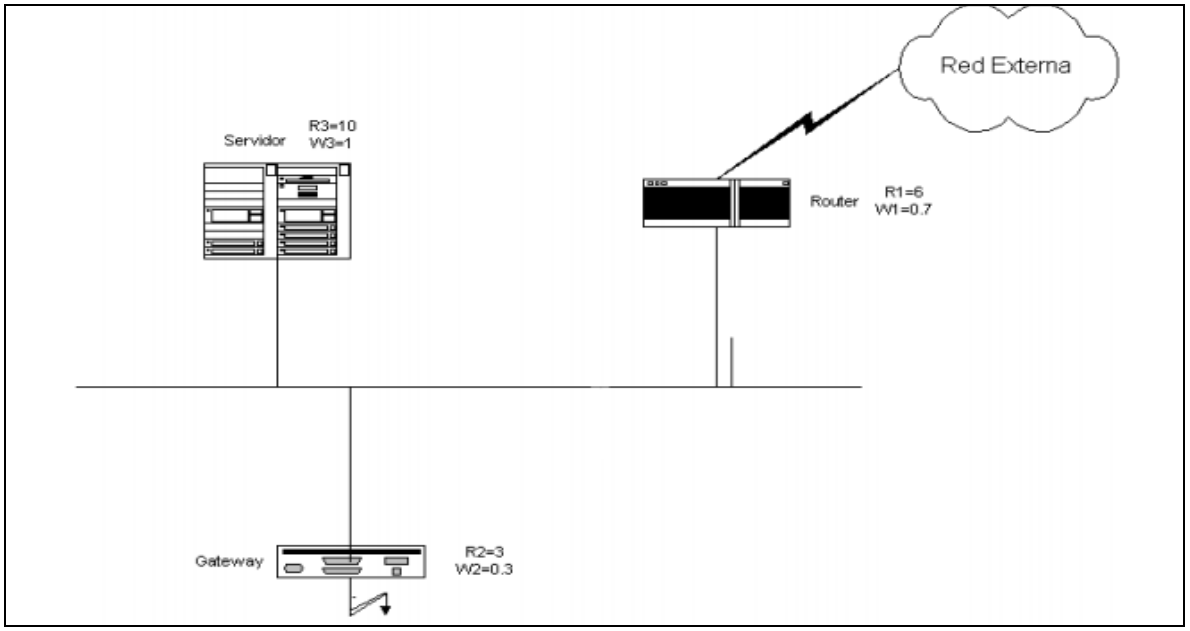


Gráfico: Ejemplo práctico de una Red

Los administradores de la red y de sistemas han producido las estimaciones siguientes para el riesgo y la importancia de cada uno de los dispositivos que forman nuestra red:

Como se ve, a cada uno de los componentes del sistema, se le ha asignado un cierto riesgo y una cierta importancia. Hay que destacar que estos valores son totalmente subjetivos, dependen exclusivamente de quien ó quienes están realizando la evaluación.

Tenemos, entonces:
Router:
R1 = 6
W1 = 7
Bridge:
R2 = 6
W2 = 3
Servidor:
R3 = 10
W3 = 10
El cálculo de los riesgos evaluados, será, para cada dispositivo:
Router:
WR1 = R1 * W1 = 6 * 7 = 42
Bridge:
WR2 = R2 * W2 = 6 * 3 = 1.8
Servidor:

WR3 = R3 * W3 = 10 * 10 = 100
La tabla que sigue a continuación, nos muestra cómo podríamos llevar a cabo esta tarea de una manera ordenada y los valores que contiene son los que hemos tratado:

Recurso del sistema		Riesgo (R_i)	Importancia (W_i)	Riesgo Evaluado (R_i * W_i)
Número	Nombre			
1	Router	6	7	42
2	Bridge	6	3	18
3	Servidor	10	10	100

Tabla de Red

Vemos que, en este caso, el recurso que debemos proteger más es el Servidor ya que su riesgo ponderado es muy alto. Por tanto, comenzaremos por buscar las probables causas que pueden provocar problemas con los servicios brindados por él.

Hay que tener muy en cuenta que, al realizar el análisis de riesgo,se deben identificar todos los recursos (por más triviales que parezcan) cuya seguridad está en riesgo de ser quebrantada.

Ahora bien, ¿cuáles son los recursos?

Los recursos que deben ser considerados al estimar las amenazas a la seguridad son solamente seis:

Hardware: procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.

Software: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Datos: durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, en tránsito sobre medios de comunicación.

Gente: usuarios, personas para operar los sistemas.

Documentación: sobre programas, hardware, sistemas, procedimientos administrativos locales.

Accesorios: papel, formularios, cintas, información grabada.

La pregunta que cabe formular, luego de haber hecho el trabajo anterior, es cómo protegemos ahora nuestros recursos. Tal vez, ésta sea la pregunta más difícil de responder, pues, según el recurso del que se trate, será el modo de protegerlo.

Primero, deberemos tener en cuenta qué es lo queremos proteger. Si se trata de los problemas ocasionados por el personal propio o de intromisiones clandestinas que puedan afectar la operatoria de la organización.

1. Hay que tener en cuenta, que todos los estudios realizados demuestran que el 80% de los problemas proceden de los llamados “clientes internos” de la organización (los empleados o elementos que se desempeñan en la organización), y sólo el 20 % restante, proviene de elementos externos a la organización.

Una aproximación acerca de cómo proteger los recursos de los problemas originados por el cliente interno consiste en la identificación del uso correcto de los mismos por parte de éstos.

Pero primero, deberemos saber quiénes son los que van a hacer uso de los recursos. Es decir se debe contar, previamente, con un conocimiento cabal de todos los usuarios que tenemos en el sistema. Esta lista no es obligatoriamente individual, sino que puede ser, en efecto, una lista por grupos de usuarios y sus necesidades en el sistema. Esta es, con seguridad, la práctica más extendida pues, definida la necesidad de un grupo de usuarios, lo más efectivo es englobarlos a todos en un mismo grupo.

Una vez identificados los usuarios (o grupos de usuarios), se puede realizar la determinación de los recursos de que harán uso y de los permisos que tendrán. Esto es sencillo de realizar con una tabla como la siguiente:

Recurso del sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	Nombre			
1	Base Datos Cuentas Corrientes	Grupo de auditores	Local	Lectura
2	Router 2500	Grupo de mantenimiento de comunicaciones	Local y remoto	Lectura y escritura

Tabla determinación de Recursos

Este modelo, nos permitirá disponer para cada usuario (o grupos de usuarios), la información de qué se les está permitido hacer y qué no.

El otro problema que nos presentamos, es el de las intromisiones clandestinas.
Aquí, es preciso tener en cuenta el tipo de recurso a proteger. En base a ello, estará dada la política de seguridad.

Daremos, a continuación, algunos ejemplos acerca de a qué nos estamos enfrentando:
¿Cómo aseguramos que no están ingresando a nuestro sistema por un puerto desprotegido o mal configurado?

¿Cómo nos aseguramos de que no se estén usando programas propios del sistema operativo o aplicaciones para ingresar al sistema en forma clandestina?

¿Cómo aseguramos de que, ante un corte de energía eléctrica, el sistema seguirá funcionando?

¿Cómo nos aseguramos de que los medios de transmisión de información no son susceptibles de ser monitoreados?

¿Cómo actúa la organización frente al alejamiento de uno de sus integrantes?

La respuesta a estos interrogantes reside en la posibilidad de conseguir dicha seguridad por medio de herramientas de control y seguimiento de accesos, utilizando check-lists para comprobar puntos importantes en la configuración y/o funcionamiento de los sistemas y por medio de procedimientos que hacen frente a las distintas situaciones.

Es muy aconsejable que se disponga de una agenda con las tareas que se deben llevar a cabo regularmente, a fin de que el seguimiento de los datos obtenidos sea efectivo y se puedan realizar comparaciones válidas al contar con datos secuenciales.

Esta agenda, podría ser en sí misma un procedimiento.
Damos, a continuación, un ejemplo de procedimiento de chequeo de eventos en el sistema:

Diariamente:
Extraer un logístico sobre el volumen de correo transportado. Extraer un logístico sobre las conexiones de red levantadas en las últimas 24 horas.

Semanalmente:
Extraer un logístico sobre los ingresos desde el exterior a la red interna.
Extraer un logístico con las conexiones externas realizadas desde nuestra red.

Obtener un logístico sobre los downloads de archivos realizados y quién los realizó.
Obtener gráficos sobre tráfico en la red.

Obtener logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino).

Mensualmente:
Realizar un seguimiento de todos los archivos logísticos a fin de detectar cambios (realizados con los archivos de back-up del mes anterior).

Cabría resaltar que, en gran parte, este procedimiento puede ser automatizado por medio de programas que realicen las tareas y sólo informen de las desviaciones con respecto a las reglas dadas".

Ejercicio del Tema 2-

Haciendo uso del gráfico de "política de seguridad- elementos-", escoja uno de los elementos y créele una política de seguridad, y explique como la implementaría y a qué nivel.

3. SISTEMAS DISTRIBUIDOS

OBJETIVO GENERAL

Describir panorámicamente los aspectos relevantes que están involucrados en los Sistemas Distribuidos.

OBJETIVOS ESPECÍFICOS

- Introducir a los estudiantes a los conceptos generales de los sistemas distribuidos.
- Brindar una panorámica de lo que son las aplicaciones distribuidas y sus usos.

Prueba Inicial

Ejercicio Inicial:

Trate de hacer una lista de tres (3) ejemplos de sistemas distribuidos y explique cada uno de ellos.

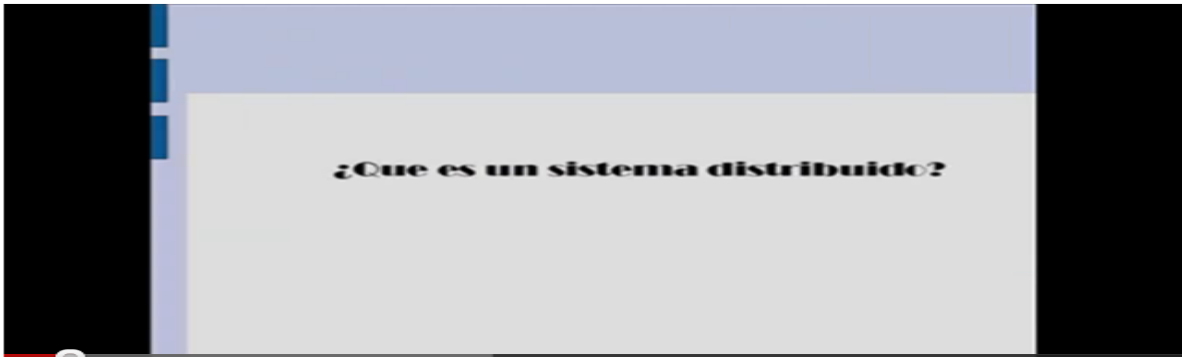
1._____
_____

2._____
_____

3._____
_____

3.1. Conceptos Generales

Antes de comenzar, veamos el siguiente video introductorio a los Sistemas Distribuido:



http://www.youtube.com/watch?v=J1Wupea9mP8

SISTEMAS DISTRIBUIDOS

Definición de sistema distribuido: Podríamos decir que un sistema distribuido es un conjunto de computadores interconectados entre sí y que comparten un estado y ofrecen una visión de un sistema único.

Como los componentes de un SD pueden no ser homogéneos, se necesita contar entonces con una capa de Software que es conocida como un “middleware”, para que esta haga como si fuera un sistema único.

Una evolución en los años 90´s que fue la que introdujo los equipos portátiles, dio paso a lo que se denomina tecnología móvil. Estos equipos móviles salen de la red local (LAN) con el propósito de descubrir nuevos recursos. Esto implica una adaptación a los cambios de red y a veces a trabajar en modo offline o desconectado. Pueden constituirse redes “ad-hoc” las cuales requieren protocolos específicos como MOBILE IP, y así se hacen muy claras las ventajas de las comunicaciones inalámbricas.

El rápido cambio de la tecnología está involucrándonos cada vez más con dispositivos miniatura. Desde ese punto de vista, cualquier dispositivo adquiere la capacidad de cómputo y comunicaciones de un computador.

Algunos ejemplos de esto son: Los celulares, GPS, tarjetas inteligentes, entre otros muchos que han ido apareciendo en el mercado y seguirán sorprendiéndonos.

PROPIEDADES DE LOS SISTEMAS DISTRIBUIDOS

Si un sistema Distribuido quiere ofrecer una visión de sistema único deberá cumplir con algunas propiedades como:

1. **Transparencia**

El principal objetivo de un SD es proporcionar al usuario y a las aplicaciones una visión de los recursos del sistema como si fueran gestionados por una máquina virtual.

La distribución física de los recursos es totalmente transparente, y por esto podemos describir aspectos de esta transparencia, como:

- Identificación: Los espacios de los nombres de los recursos son independientes de la topología de red y de la propia distribución de los recursos, es decir, una aplicación cualquiera puede referirse a un recurso con un nombre totalmente independiente del nodo en que esta se ejecuta.

Veamos la siguiente figura:

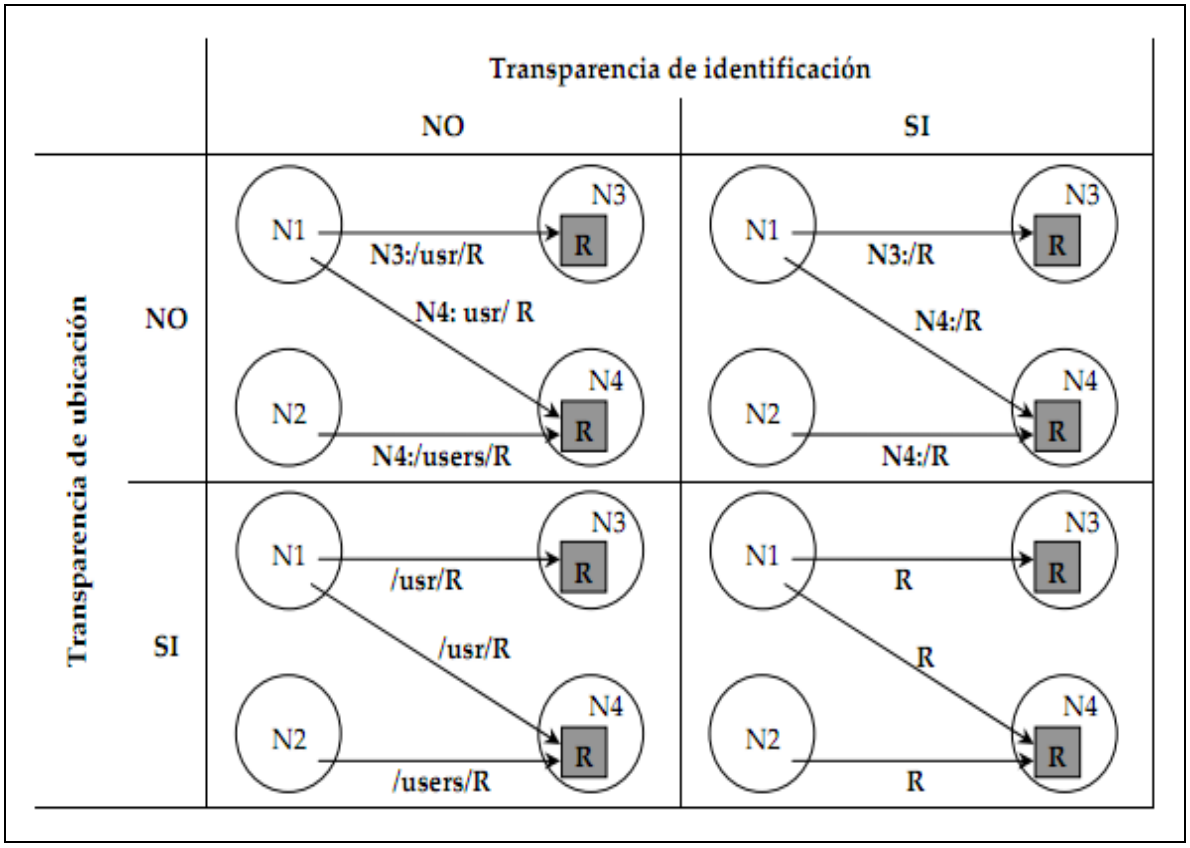


Gráfico: Propiedad de la Transparencia

- Ubicación Física de los Recursos: Ni los recursos ni tampoco las aplicaciones conocen el nodo en el que reside el recurso, y tampoco si este es remoto o local. Por esta razón, esto implica que los mismos recursos pueden migrar entre nodos sin que las aplicaciones se vean afectadas.

- Replicación: Ni los usuarios ni tampoco las aplicaciones tienen conocimiento de cuantas unidades hay de cada recurso, ni tampoco si hay adición o eliminación de las copias de los recursos.

- Paralelismo: Una aplicación cualquiera podría ejecutarse en paralelo sin que la aplicación tenga que especificarlo, y además sin tener ninguna consecuencia sobre la ejecución, excepto por medidas de rendimiento.
- Esta propiedad si afecta a los procesos que permiten la distribución de procesos y memoria.

- Compartición: Esta consiste en que un recurso compartido intente ser accedido de manera simultánea desde varias aplicaciones y no esto no tenga efecto sobre la ejecución de esta aplicación.

- Rendimiento: la implementación de los SD implica que hay un costo, y en este caso hablamos que ese costo será el rendimiento.

CARACTERÍSTICAS DE LOS SISTEMAS DISTRIBUIDOS

ESCALABILIDAD

Una de las características de los SD es su modularidad, y esta por ende le permite ser flexible y escalable.

La escalabilidad se entiende entonces como esa capacidad de crecer sin aumentar su complejidad ni mucho menos disminuir su rendimiento.

La escalabilidad presenta dos aspectos básicos que son:

2. El SD debe proporcionar espacios de nombres lo suficientemente amplios, de manera que no dé pie a una limitación inherente.

   “Los espacios de nombres, al igual que en los sistemas centralizados, pueden identificar objetos de diferente naturaleza, como ficheros, procesos, variables, o incluso direcciones de memoria (en los sistemas de memoria compartida distribuida, DSM). En el caso de los espacios lineales, como la memoria, existe una limitación inherente asociada al tamaño

del nombre, de forma que hoy en día es razonable plantear la insuficiencia de los espacios de direcciones de 32 bits. En otros casos, los espacios de nombres son jerárquicos y por lo tanto escalables por naturaleza"[1].

3. El SD debe mantener un buen nivel de rendimiento en el acceso a los recursos cuando el sistema crece.
   "El crecimiento de un sistema distribuido puede introducir cuellos de botella y latencias que degradan su rendimiento. Además del incremento de los costes de comunicación por el aumento de la distancia física entre los componentes del sistema, la complejidad estructural de los algoritmos distribuidos es a menudo más que lineal con respecto al tamaño del sistema, como iremos comprobando a lo largo del curso. Es necesario, por tanto, establecer compromisos entre tamaño del sistema, rendimiento y complejidad"[2].

FIABILIDAD

La fiabilidad de un sistema puede definirse como esa capacidad para realizar correctamente y en todo momento las funciones para las que se ha diseñado el mismo.
La fiabilidad se contempla dos aspectos que son:

4. Disponibilidad:
   Entendida como la fracción de tiempo que el sistema está en operación. El principal parámetro para medir la disponibilidad es el tiempo medio entre fallos (MTBF), pero hay que considerar también el tiempo de reparación.

5. Tolerancia a Fallos: un fallo en un momento específico podría tener consecuencias fatales para el sistema. Pensemos por ejemplo en un sistema de tiempo real, que controlan dispositivos vitales (pensemos en el campo de la medicina por ejemplo), y aunque la replicación aumenta la disponibilidad, esto no es garantía absoluta de la continuidad del servicio.

La tolerancia a fallos contempla entonces la capacidad del sistema para seguir operando correctamente ante el fallo de alguno de sus componentes.

CONSISTENCIA

Los SD traen consigo importantes beneficios como como el incremento del rendimiento a través del paralelismo y así permitiendo el acceso a copias locales del recurso.

[1] Introducción a los Sistemas Distribuidos. En: http://www.sc.ehu.es/acwlaroa/SDI/Apuntes/Cap1.pdf
[2] Introducción a los Sistemas Distribuidos. En: http://www.sc.ehu.es/acwlaroa/SDI/Apuntes/Cap1.pdf

Ahora, de otro modo la replicación aumenta la disponibilidad, que es la base para mejorar la tolerancia a fallos.

Así mismo, la distribución de recursos trae consigo algunos problemas. Algunos de estos son:

- La red de interconexión es una nueva fuente de fallos.
- La seguridad del sistema es vulnerable a accesos no permitidos.
- Dificultada para evitar situaciones de inconsistencia entre los componentes del sistema.

Ejercicio del Tema 1

Liste tres de las propiedades de los Sistemas Distribuidos y de un ejemplo de la vida real donde se pueda apreciar esta propiedad.

Propiedad 1: _____
Ejemplo1:_____
_____

Propiedad 2: _____
Ejemplo2:_____
_____

Propiedad 3: _____
Ejemplo3:_____
_____

3.2. Aplicaciones Distribuidas

APLICACIONES DISTRIBUIDAS

Diferenciemos entonces en primer lugar entre aplicaciones distribuidas (AD) y aplicaciones paralelas (AP).

Una AP es la que tiene la capacidad de dividirse en tareas que se ejecutan de manera concurrente en diferentes elementos del proceso. La razón de esto es la disminución del tiempo de finalización.

La mayoría de las aplicaciones pueden ejecutarse en paralelo, siguiendo sí a determinados esquemas de cómputo, que dependen del tipo de la aplicación y del hardware sobre el que se va a ejecutar.

Las tareas de estas aplicaciones se distribuyen entre los elementos del proceso, teniendo en cuenta la carga de cada uno de ellos y los costos de comunicación.

El objetivo principal de una AP, es la ejecución simultánea de las tareas.

Ahora, el objetivo de una AD puede estar sometido a la influencia de varios factores como:

- Alto rendimiento:

Una aplicación paralela puede ser también distribuida. Por ejemplo, puede utilizarse una red local para distribuir los procesos de la tarea entre los nodos de la red con el fin de aprovechar los recursos de cómputo disponibles para reducir el tiempo de finalización.

Este tipo de esquema de cómputo, conocido como computación en cluster, ofrece una excelente relación rendimiento/costo.

- Tolerancia a fallos:

En otras aplicaciones la distribución viene dictada por criterios como la integridad de la información. Así, en un sistema bancario es preciso mantener replicada la información acerca del estado de las cuentas de los clientes en diferentes servidores, pues el riesgo de perder información por el fallo de una máquina resulta inaceptable por las consecuencias que traería.

- Alta disponibilidad:

Hay aplicaciones donde la distribución se realiza para acercar la información al usuario y disminuir los tiempos de respuesta. La consistencia en la actualización no suele ser un aspecto crítico; en cambio importa mucho la escalabilidad. Hoy en día están muy extendidos los sistemas peer-to-peer, caracterizados por su gran escalabilidad al evitar los cuellos de botella de los servidores, ofreciendo disponibilidad de recursos de manera prácticamente indiscriminada. Un ejemplo son las redes de distribución de contenidos, como BitTorrent.

- Movilidad:

La cantidad de dispositivos móviles como portátiles, tablets, celulares y otros, introducen una dificultad más para el acceso a la información del usuario, de forma que este no tenga que gestionar la actualización de la información en cada dispositivo.

Por ejemplo, un mensaje de correo borrado desde el teléfono móvil debería aparecer como borrado cuando posteriormente el usuario acceda a su correo desde un ordenador personal. Se

hace imprescindible desligar la información de su soporte, gestionando convenientemente las actualizaciones.

Cada vez más se trabaja sobre espacios virtuales de información en vez de sobre dispositivos físicos concretos, que se convierten en simples "caches" del ciberespacio de información del usuario. Así, el usuario se mueve desde un dispositivo a otro y y accede al espacio de su información de forma actualizada y consistente.

Ejemplos de productos actuales son Gmail de Google para el correo electrónico y Dropbox para documentos.

- Ubicuidad:

Algunas veces los recursos de las aplicaciones están distribuidos de manera inherente. El usuario se mueve en un entorno con recursos (ubicuos) no previstos de manera apresurada, y la aplicación trata de ofrecer un comportamiento inteligente en función de las necesidades del usuario y la disponibilidad de los recursos.

ENTORNOS DE LAS APLICACIONES DISTRIBUIDAS

Las Aplicaciones Distribuidas pueden verse en diferentes escenarios. Hoy por hoy el entorno más amplio y general es el Internet, pero también hay otros entornos más específicos.
Veamos a continuación algunos entornos para estas Aplicaciones Distribuidas:

INTERNET:
La WEB es la aplicación base del Internet, y así mismo es la puerta de acceso a otras aplicaciones de Internet como son el correo electrónico o e-mail, y la transferencia de datos.

Esta se basa en una estructura de comunicaciones que maneja una infraestructura de enlaces troncales de gran capacidad conocidos como los backbones (o columna), donde están conectadas las sub-redes y los proveedores de servicios de Internet (ISP), y que le proporcionan la infraestructura a los usuarios a través del uso de diferentes medios tales como el cableado telefónico tradicional. Con esto la WEB ha implementado el HTTP como el protocolo de acceso común.

Las aplicaciones distribuidas que se pueden desplegar en Internet son muy variadas, pero así mismo también son muy limitadas por cuestiones de seguridad y del mismo rendimiento.

Las conocidas aplicaciones PeerToPeer son un ejemplo de las aplicaciones de alta disponibilidad que salen de Internet.

Otro ejemplo que está tomando bastante fuerza son los servicios “Cloud computing”, que son conocidos como la “nube en internet” que permiten soportar aplicaciones que hasta hace poco se entendían que sólo estaban ligados a sistemas locales, y esta nubes hacen este trabajo de manera transparente. El objetivo de estos servicios es la virtualización de los espacios de información y la movilidad de los usuarios de una manera independiente a los dispositivos.

- **INTRANET:**

Empecemos por decir que Intranet es un entorno de Internet, pero de forma restringida. En ésta se utilizan los mismos protocolos y medios de acceso que en el internet, pero el acceso se inscribe en un dominio administrativo que bien puede ser el de una empresa en particular, o un negocio.

Una intranet puede estar compuesta por varias subredes y estas a su vez pueden estar integradas en Internet.

- **ENTORNOS UBICUOS**

En estos entornos las aplicaciones no están sujetas a ámbitos administrativos o de red en específicos así como las intranets, pero tampoco trabajan de manera ilimitada en el ámbito de Internet.

Así el dispositivo de un usuarios, el celular por ejemplo, trabaja en un entorno físico concreto, por ejemplo la casa del usuario o su trabajo, y de acuerdo a los servicios que descubre en ese entorno, se adapta a la infraestructura disponible de la forma más eficiente posible, es decir, imaginémonos una llamada telefónica de un usuario que la hace desde su casa hacia su empresa, ésta podría utilizar diferentes infraestructuras como una línea ADSL en el domicilio a la que se conecta el teléfono mediante un punto de acceso al que accede por bluetooth.

Los medios de comunicación conmutarían de una forma dinámica, de manera que se optimice la calidad y el coste de la comunicación.

Ejercicio del tema 2:

Haga una lista de 5 aplicaciones distribuidas que usted conozca y diga en que entorno se mueven y si es posible que estén en otro entorno.

App 1: _____
Entorno: _____
Entorno 2: _____

App 2: _____
Entorno: _____

Entorno 2: _____

App 3: _____
Entorno: _____
Entorno 2: _____

App 4: _____
Entorno: _____
Entorno 2: _____

App 5: _____
Entorno: _____
Entorno 2: _____

4. COMUNICACIONES INALÁMBRICAS Y SERVICIOS EN LA RED

OBJETIVO GENERAL

Estructurar el modelo, el diseño y la evaluación de los sistemas de comunicaciones inalámbricos tanto con características de usuario estático como de usuario móvil.

OBJETIVOS ESPECÍFICOS

Dar a conocer el proceso evolutivo de los sistemas de comunicación

Mostrar de una manera amplia las diferentes aplicaciones y servicios que ofrece Internet y sus usos.

Prueba Inicial

Ejercicio Inicial:

Haga una lista de las diferentes tecnologías inalámbricas que conozca y explique al menos un uso de ésta.

4.1. Sistemas de Comunicación Inalámbrica

Veamos el siguiente video que nos introducirá al tema:

http://www.youtube.com/watch?v=qD-9jr3VrYI

COMUNICACIONES INALÁMBRICAS

Cuando hablamos de WIFI nos referimos a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día.

WIFI, también conocida como WLAN, Wireless Lan o Red inalámbrica. WIFI no es una abreviatura de Wireless Fidelity, éste es simplemente es un nombre comercial.

Hoy podemos hablar de dos tipos de comunicación WIFI, éstos son:

- 802.11b, que emite a 11 Mb/seg, y
- 802.11g, más rápida, a 54 MB/seg.

De hecho, son su velocidad y alcance (unos 100-150 metros en hardware asequible) y esto lo convierten en una fórmula perfecta para el acceso a internet sin cables.

Para tener una red inalámbrica en casa sólo necesitaremos un punto de acceso, que se conectaría al módem, y un dispositivo WIFI que se conectaría en nuestro dispositivo.

Existen terminales WIFI que se conectan al PC a través del puerto USB, pero son las tarjetas PCI, las recomendables, pues nos permite ahorrar espacio físico de trabajo y nos ofrecen mayor

rapidez. Para portátiles podemos encontrar tarjetas PCMI externas, aunque muchos de los dispositivos ya se venden con tarjeta integrada.

En cualquiera de los casos se recomienda mantener el punto de acceso en un lugar alto para que la recepción/emisión sea más fluida. Incluso si encontramos que nuestra velocidad no es tan alta como debería, esto podría ser debido a que los dispositivos no se encuentren adecuadamente situados o puedan existir barreras entre ellos (como paredes, metal o puertas).

El funcionamiento de la red es bastante sencillo, normalmente sólo se tiene que conectar los dispositivos e instalar el correspondiente software. Muchos de los routers WIFI incorporan herramientas de configuración para controlar el acceso a la información que se transmite por el aire.

Pero al tratarse de conexiones inalámbricas, no es difícil que alguien interceptara nuestra comunicación y tuviera acceso a nuestro flujo de información. Por esto, es recomendable la encriptación de la transmisión para emitir en un entorno seguro.

En WIFI esto es posible gracias al WPA, mucho más seguro que su predecesor WEP y con nuevas características de seguridad, como la generación dinámica de las claves de acceso.

SISTEMAS DE COMUNICACIÓN INALÁMBRICA

Algunos de los sistemas de comunicación inalámbrica que existen son los siguientes:

Ventana óptica
Infrarrojo
Luz visible
Radiofrecuencia

También hay algunas limitaciones para algunos tipos de medios ya que estos pueden estar sujetos a interferencia electromagnética, atenuación, entre otros factores:
Bandas reguladas
Telefonía celular
GSM
CDPD
CDMA
Microondas
Satélites de comunicaciones
Geosíncronos
De órbita baja

Bandas no reguladas
Ethernet inalámbrico (IEEE 802.11)
Bluetooth

Telefonía Celular
Existen diferentes sistemas de telefonía celular en el mundo. Los sistemas difieren en tecnologías y bandas de frecuencia. Además, como resultado de su evolución, estos sistemas se clasifican en varias generaciones.

La característica común a los sistemas celulares es la división de un área geográfica en celdas o células y la reutilización de frecuencias en celdas no adyacentes. Esto permite dar servicio a una mayor cantidad de clientes y un mayor número de llamadas simultáneas sin requerir una mayor porción del espectro electromagnético.

En cada una de las celdas se dispone de cierta cantidad de canales bidireccionales, lo cual limita el número de llamadas simultáneas que pueden ocurrirse. Cuando la demanda de clientes en una celda crece hasta saturar la capacidad del sistema, la celda debe dividirse en celdas de menor área a fin de mantener la calidad del servicio.

Para establecer una comunicación bidireccional entre el celular y el operador base, se usan un par de frecuencias, una para transmisión en cada dirección. Al iniciarse una llamada, el celular negocia la selección de estas frecuencias con el operador base más cercana, aquella cuya señal detecta con mayor intensidad. Cuando el celular se acerca a la frontera entre dos celdas ocurre un proceso llamado handoff en el cual se negocia un nuevo par de frecuencias, se establece una conexión con el nuevo operador base y por último se libera la conexión con el operador anterior.

Evolución de la telefonía celular

La evolución de la telefonía celular es complicada ya que distintos países establecieron esquemas de transmisión y bandas de frecuencia diferente e incompatible entre sí. Veamos la siguiente figura comparativa.

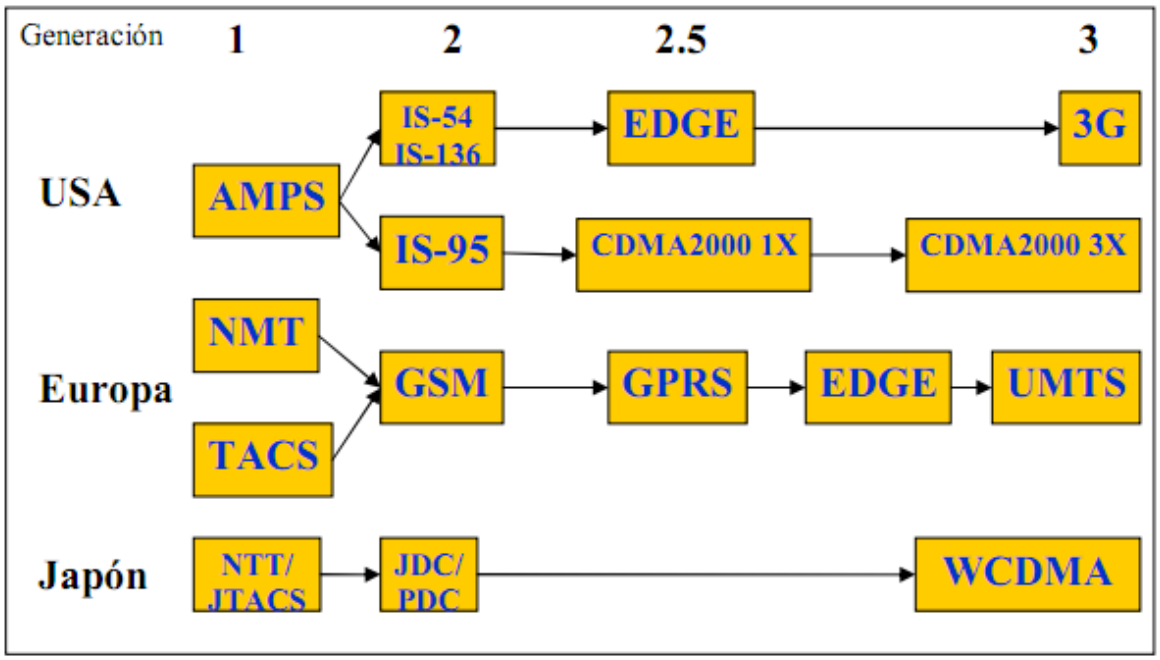


Gráfico: Comparación redes de celulares

"La primera generación de telefonía celular utiliza transmisión analógica y modulación de frecuencia. El ancho de banda disponible se divide mediante FDMA dando origen a unos 400 canales bidireccionales, de los cuales cerca de 50 se usan en cada celda. La transmisión de datos requiere de un MODEM similar a los que se usan en líneas telefónicas convencionales, es decir, se debe hacer una llamada y los datos deben ser convertidos a formato analógico para su transmisión y de nuevo a digital para ser aceptados en el destino. Las velocidades típicas son del orden de 9600 bps o menos.

El sistema Norteamericano de primera generaciones conoce como AMPS (Advanced Mobile Phone System). En Europa se utilizan múltiples sistemas en los diversos países. Entre estos tenemos NMT (Nordic Mobile Telephone) en los países escandinavos y TACS (Total Access Communications System) entre otros. Los sistemas de primera generación en Japón son NTT (Nippon Telephone and Telegraph) y JTACS (Japanese TACS).

La segunda generación de telefonía celular utiliza transmisión digital y técnicas de modulación más avanzadas por lo que se aprovecha mejor el ancho de banda disponible por canal. El número de canales también es mayor ya que pueden emplearse TDMA y CDMA. Al ser digitales las transmisiones, se facilita la transmisión de datos.

Sin embargo, las velocidades de transmisión son relativamente bajas, típicamente menos de 19.200 bps.

El sistema europeo de segunda generación se conoce por la sigla GSM (Group Special Mobile que luego se convirtió en Global System for Mobile communications). En Norteamérica se establecieron dos sistemas de segunda generación el IS-54 (Interim System 54) luego actualizado a IS-136 y el IS-95. El sistema de segunda generación en Japón se conoce como PDC o JDC (Personal Digital Cellular o Japanese Digital Cellular). IS-95 usa CDMA mientras que los demás usan TDMA.

Además de voz, los sistemas celulares se utilizan para transmitir datos. El protocolo CDPD (Cellular Digital Packet Data) permite transmitir datos sin necesidad de realizar una llamada telefónica celular, es decir sin necesidad de establecer un circuito.

CDPD solo usa un canal de transmisión cuando está enviando o recibiendo información. Cuando se necesita enviar un paquete de datos CDPD comienza a escuchar los canales del sistema celular hasta encontrar uno que este libre. Al obtener un canal CDPD envía el paquete de datos y libera el canal hasta la próxima transmisión.

Como CDPD solo usa la capacidad ociosa del sistema, resulta muy económico y las compañías proveedoras de servicios celulares pueden ofrecerlo a bajo precio. Por otra parte, en un sistema congestionado puede ser difícil encontrar un canal libre lo que va en detrimento de la calidad de servicio. El proveedor puede aliviar esta situación asignando algunos canales para uso exclusivo de CDPD, pero estos se restarían del servicio de voz, representando un costo mayor. La principal desventaja de CDPD es su relativamente baja velocidad de transmisión de 19.200 bps (19,2 Kbps).

La creciente demanda en el sector de transmisión de datos motiva el siguiente paso en la evolución de los servicios celulares. El objetivo final de la tercera generación es el del servicio universal. Es decir, un sistema que funcione de igual manera en todos los países, que pueda transmitir tanto voz como datos, que reemplace tanto los servicios celulares de segunda generación como servicios similares como PCS (Personal Communications Systems) y los servicios móviles de datos. Así mismo, se espera que la tercera generación mejore la calidad de los servicios de voz, incremente la capacidad de las redes y logre mayores tasas de transferencia de datos. Para lograr todo esto, la tercera generación empleará transmisión por paquetes en vez de transmisión por circuitos.

Debido a las diferencias entre los diversos sistemas celulares, no es fácil lograr los objetivos propuestos por la tercera generación. De hecho los sistemas propuestos como “de tercera generación”, aunque tienen similitudes, aun son incompatibles entre si. Mientras tanto, la demanda de acceso a datos digitales, entre ellos a Internet, ha obligado a las operadoras a ofrecer sistemas de transición y que se han denominado generación 2.5.

En Europa, el primer paso intermedio se denomina GPRS (General Packet Radio Services) que superpone un servicio de transmisión por paquetes sobre GSM. El siguiente paso se conoce como EDGE (Enhanced Data rates for Global Evolution) que es un nuevo esquema de modulación que triplica la velocidad de GPRS. El estándar europeo de tercera generación es UMTS (Universal Mobile Telecommunications System). UMTS usa una frecuencia de 2000 Mhz distinta de la de los sistemas de primera y segunda generación. A diferencia de GSM que usa TDMA, UMTS usa una variante de CDMA conocida como WCDMA (Wideband CDMA) que usa un ancho de banda de 5 Mhz en vez de 1.25 Mhz.

En Norteamérica los sistemas TDMA evolucionarán hacia EDGE similar al estándar europeo aunque a frecuencias ligeramente diferentes. Sin embargo la tercera generación no utilizará UTMS. Por otra parte los sistemas CDMA evolucionarán hacia CDMA2000 1x y luego a CDMA2000 3x. Cada paso representa una mejora en procesamiento, ancho de banda y/o modulación. Lamentablemente estas versiones de CDMA no son compatibles con WCDMA.

En Japón no se consideró necesaria una generación intermedia por lo que es el primer país en implementar facilidades de tercera generación. Su sistema está basado en WCDMA y es similar al sistema UMTS europeo.

La siguiente tabla resume algunas características de los sistemas de la diversas generaciones”3.

	Generación 1	Generación 2	Generación 2.5	Generación 3
Tipo de señal	Analógica	Digital	Digital	Digital
Transmisión	Por circuitos	Por circuitos	Por paquetes	Por paquetes
Servicio de datos	Modem	Mensajes/WAP	Internet	Multimedia
Velocidad	9.6 Kbps	19.2 Kbps	144 Kbps	384-2048 Kbps

Tabla generaciones

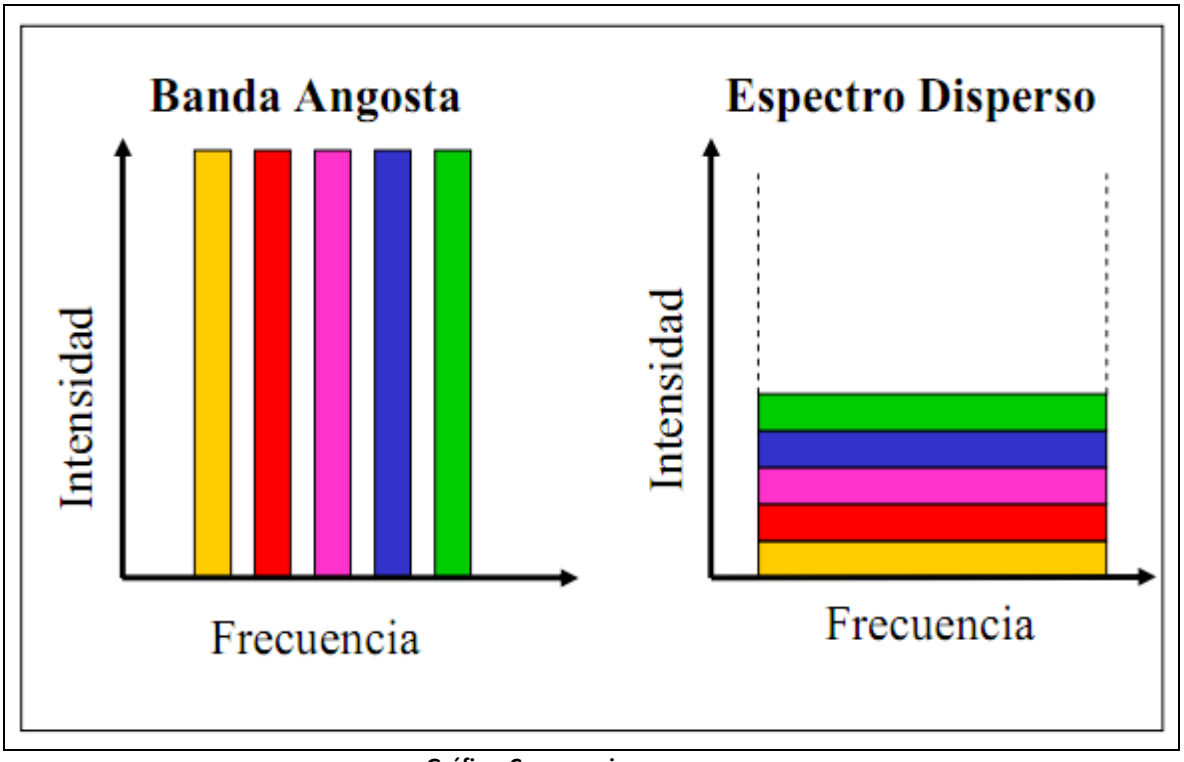
Ejercicio de Aprendizaje:
Realice una tabla de comparaciones Generacional para Colombia. Use como ayuda la tabla que se muestra previamente a este ejercicio.

[3] Comunicaciones Inalámbricas. En: http://www.ica.luz.ve/cstufano/CursoDeRedes/Wirelessdoc.pdf

CDMA

CDMA es una tecnología de espectro disperso. Esto significa que para efectuar una transmisión, en vez de una señal de alta intensidad y ancho de banda no muy amplio, se utiliza una señal de baja intensidad y ancho de banda muy amplio.

Cuando una señal se dispersa en un mayor rango de frecuencias, su intensidad disminuye, ya que la energía total se mantiene. Esto permite que las señales de distintas conversaciones puedan sumarse, siempre que sea posible etiquetar a cada señal de alguna forma, y así permita después identificarla y recuperarla. También se requiere que todas la señales se reciban en la base con aproximadamente la misma intensidad. Para lograrlo las base indica a los celulares a cual nivel de potencia deben transmitir. La siguiente figura ilustra lo anterior:



Gráfica: Comparaciones

"Para identificar cada señal, CDMA realiza una operación binaria, llamada NXOR (Not eXclusive OR), entre la secuencia binaria a transmitir y una secuencia, llamada chip, que se repite periódicamente a una tasa (bits por segundo) mucho mayor. La operación NXOR produce un bit uno si las dos señales son uno o las dos son cero y cero sin son diferentes. Esta operación es simétrica, lo que significa que la señal original puede recuperarse (convertirla en banda angosta

nuevamente) aplicando a la señal dispersa usando el mismo chip. Para que la tecnología funcione los chips aplicados a las diversas señales deben ser ortogonales entre si.

Cuando a la suma de un conjunto de señales dispersas se aplica NXOR con un chip, solamente la señal correspondiente a ese chip será transformada a banda angosta y por tanto aparecerá con una alta intensidad. Las demás serán re-dispersadas y por tanto serán de baja intensidad y podrán ser filtradas. Por otra parte, cualquier señal de banda estrecha que invada la banda de frecuencias utilizada también será dispersada y filtrada por el equipo receptor.

En la práctica, los chips se escogen de manera tal que todos puedan ser colocados en una larga secuencia binaria en la cual, comenzando en cada bit de la secuencia se obtiene un nuevo chip. De forma, la secuencia de bits es la misma para todas las estaciones y el emisor y receptor solo deben ponerse de acuerdo sobre cual es el bit en el que se inicia su chip. Esto requiere que todos los equipos estén sincronizados por un reloj maestro.
La siguiente figura ilustra el proceso de dispersión y recuperación de una señal.

En la figura la señal 101101 es parte de una conversación y se uso para fines ilustrativos una frecuencia solo seis veces mayor para el chip”4.

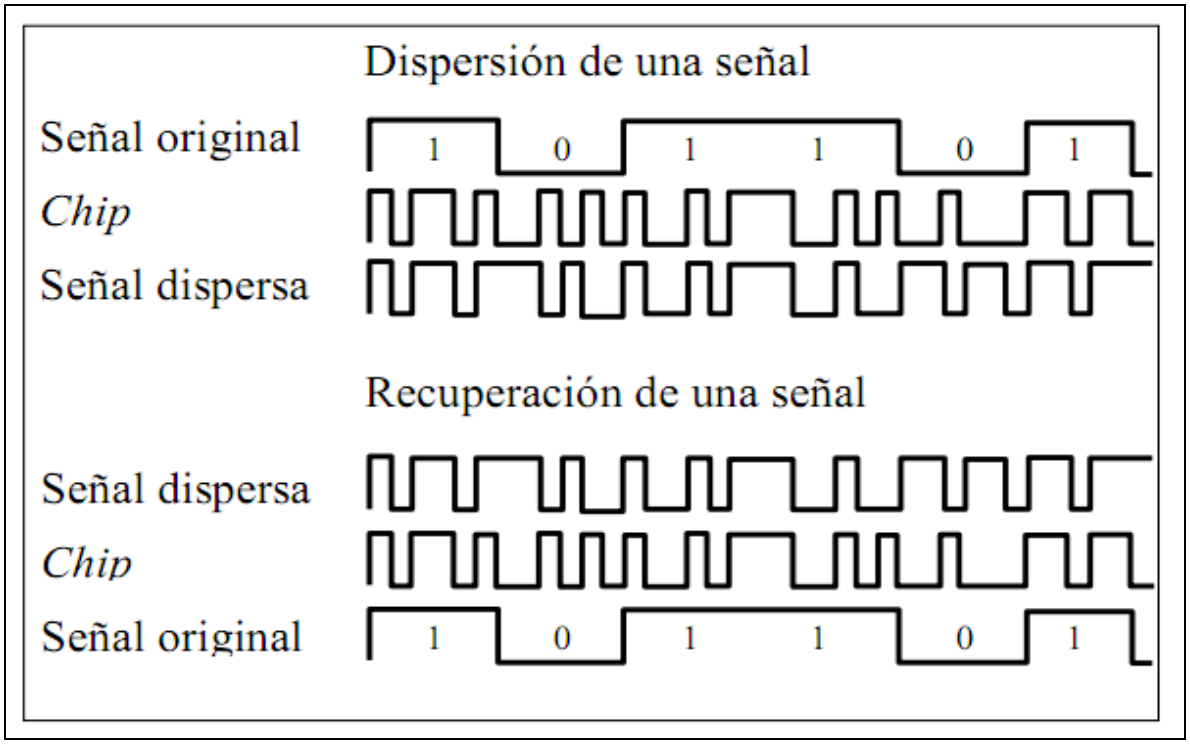


Gráfico: Dispersión de una señal

[4] Comunicaciones Inalámbricas. En: http://www.ica.luz.ve/cstufano/CursoDeRedes/Wirelessdoc.pdf

Ethernet inalámbrico

"Los estándares de la serie 802 del IEEE (Institute of Electrical and Electronics Engineers) son fundamentales en el área de redes locales o LANs (Local Area Networks) en particular 802.2 define la interfaz entre la capa de enlace de datos y la capa de red, mientras que 802.3 es básicamente equivalente a Ethernet y 802.11 aplica a redes locales inalámbricas o WLANs (Wireless LANs)"5.

Las redes WLANs transmiten los datos a altas velocidades, pero únicamente en distancias cortas con el fin de proveer acceso LANs convencionales.

Las bandas de frecuencia que usa la IEEE 802.11 no están reguladas, y por ello no requieren licencias para su operación lo que facilita la instalación de servicios de este tipo.

Otras aplicaciones podrían desear utilizar las mismas bandas en interferir con la transmisión de datos. La tabla que se muestra a continuación, nos muestra algunas características de estos estándares.

Parámetro	802.11	802.11a	802.11b
Estado	Aprobado, productos	Aprobado, productos en desarrollo	Aprobado, productos
Banda de frecuencias	2.4 GHz	5 GHz	2.4 GHz
Modulación	DSSS	DSSS	OFDM
Velocidad de transmisión	1, 2 Mbps	6, 9, 12, 18, 24, 36, 54 Mbps	1, 2, 5.5, 11 Mbps

Tabla de estándares Ethernet

La 802.11b también conocida Wi-Fi es la tecnología más popular en los momentos y para la que se dispone de la mayor cantidad de productos comerciales.

Bluetooth

El término Bluetooth se refiere a una especificación abierta para una tecnología que permita comunicación inalámbrica de corto alcance para voz y datos en cualquier parte del mundo.

Esta tecnología tiene varios aspectos que hay que analizar, y estos son:
Especificación abierta: La especificación fue desarrollada por un grupo de interés especial (SIG) y está disponible a todo el público de manera gratuita.

[5] Comunicaciones Inalámbricas. En: http://www.ica.luz.ve/cstufano/CursoDeRedes/Wirelessdoc.pdf

Comunicación inalámbrica de corto alcance: El Bluetooth pretende reemplazar una variedad de cables de interconexión por ondas de radio con un protocolo común. La tecnología ha sido diseñada específicamente para un corto alcance (hablamos de 10 metros aproximadamente) lo que requiere bajos niveles de potencia y es por tanto adecuado para dispositivos pequeños.
Voz y datos: hoy en día, las comunicaciones de voz frecuentemente se transmiten en formatos digitales, el Bluetooth tiene facilidades tanto para comunicaciones de voz como de datos y por tanto permite que todo tipo de dispositivos se comuniquen usando alguno o ambos de estos medios.

En cualquier parte del mundo: El Bluetooth usa la banda de 2.4 GHz que es NO regulada en casi todos los países del mundo. La especificación Bluetooth consta de mas de 1500 páginas dividida en dos.

La arquitectura de protocolos de Bluetooth: esta incluye los protocolos básicos, el protocolo para reemplazo delos cables, el protocolo para control de telefonía y los protocolos adoptados.

Los protocolos básicos forman una pila de cinco capas que incluye:

Radio: Interfase, frecuencias, saltos de frecuencia, modulación y potencia.

Baseband: Establecimiento de conexión, direccionamiento, formato de los paquetes, señalización, control de potencia.

LMP (Link Manager Protocol): Autenticación de usuarios, encriptado, negociación del tamaño de los paquetes.

L2CAP (Logical Link Control and Adaptation Protocol): Interfaz única para capas superiores. Ofrece servicios orientados a conexión y no orientados a conexión.

SDP (Service Discovery Protocol): determinación de información, servicios y características de los servicios ofrecidos por un dispositivo.

El protocolo para reemplazo de cables es RFCOM que permite presentar a la aplicación un puerto serial virtual.

El protocolo de control de telefonía TCSBIN (Telephony Control Specification – BINary) define la señalización para el establecimiento de llamadas de voz y de datos entre dispositivos. También tiene procedimientos para manejar la movilidad de los dispositivos.

Entre los protocolos se tiene:

PPP (Point to Point Protocol)
TCP/UDP/IP

OBEX: desarrollado por IrDA (Infrared Data Association) para el intercambio de objetos. Provee una funcionalidad similar a HTTP.
WAE/WAP (Wireless Application Environment / Wireless ApplicationProtocol)

Ahora veamos algunos de los casos de uso de Bluetooth:
Transferencia de archivos.

Puente Internet: conexión inalámbrica de un PC a un teléfono móvil o MODEM inalámbrico para proveer acceso discado a Internet y servicios de fax.

Acceso a redes locales.

Sincronización: dispositivos de información personal.

Teléfono multiuso: Inalámbrico, intercomunicador, celular.

En una red Bluetooth hasta ocho(8) dispositivos se interconectan para formar una “piconet”.

Uno de estos dispositivos es el maestro y los otros son esclavos. Los dispositivos en una piconet, comparten un canal de 1 MHZ y se comunican a velocidades de hasta 720 Kbps. El dispositivo maestro determina las características del canal. Los esclavos sólo pueden comunicarse con el maestro y sólo con su permiso.

Un dispositivo puede pertenecer a más de una piconet y hacer de maestro o esclavo en cada una de ellas. Un conjunto de piconets forma una scatternet. Este esquema permite que muchos dispositivos compartan la misma área física y hagan un uso eficiente del ancho de banda.

Bluetooth usa hasta 80 frecuencias con un ancho de banda total de 80MHz. El sistema Bluetooth usa un esquema de salto de frecuencias. Cada piconet usa una secuencia de salto de frecuencias diferente, de modo que múltiples canales lógicos pueden compartir el mismo ancho de banda de 80 MHz. Cuando dispositivos en piconets diferentes, en canales lógicos diferentes usan la misma frecuencia ocurre una colisión.

Cuando la cantidad de piconets en un área aumenta, se incrementan las colisiones y se degrada el rendimiento. Las scatternets comparten el ancho de banda. Las piconets comparten el canal lógico.

Veamos una imagen que nos muestre lo explicado anteriormente:

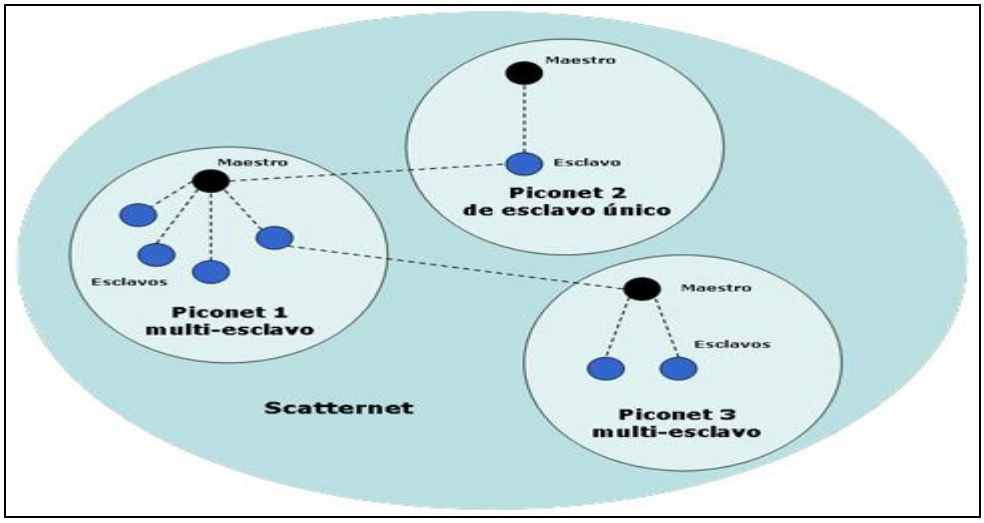


Imagen: Red Bluetooth

4.2. Aplicaciones en Internet

El internet nos brinda múltiples y amplios servicios, que en este caso sólo hablaremos de algunos para darles una idea de lo que se puede hacer con sólo contar con una conexión a Internet.

Comencemos con **World Wide Web**
Este servicio es uno de los más nuevos en Internet, pero eso sí es el más usado por todos los usuarios.

Este fue concebido al finalizar los años 80´s por un laboratorio europeo conocido como “CERN”, con el objetivo de que los científicos del laboratorio pudieran compartir la información que trabajaban a través de documentos científicos que estuvieran escritos en hipertexto.

WWW son las siglas con las que se designa World Wide Web, y es en ella donde se encuentran millones de páginas que son de propiedad de diferentes tipos de organización

Dentro de esta se puede encontrar información de cualquier tipo de tipo de tema, además puedes hacer uso del comercio electrónico, o estar en cualquier lugar del mundo en cualquier instante de tiempo.

Todo esto es posible gracias a los navegadores con los que cuenta, pues con los recursos multimediales que estos ofrecen, es que se hace posible.

El correo electrónico, es el otro servicio que veremos.

Este servicio nos permite enviar y recibir cartas de manera digital como simulación del uso de correo ordinario, o del servicio de fax, y todo es posible desde que ambos, emisor y destinatario cuenten con este recurso.

Si miramos, realmente el propósito de este servicio es el mismo que el del correo ordinario, pero la diferencia está en el costo, la disponibilidad del receptor y la saturación de las líneas telefónicas.

Actualmente el correo electrónico es la base de la comunicación entre las diferentes organizaciones y las personas naturales, pues de esta manera hay ahorro en costos y tiempo.

Sigamos con el **FTP**

Estas tres siglas se leen como “File Transfer protocol” que en nuestro español diríamos, Protocolo de transferencia de ficheros.

Este servicio permite la transferencia de ficheros o paquetes de un computador a otro a través de internet.

Pero quizá el servicio más novedoso de los FTP, es la posibilidad de descarga de libros haciendo uso del internet.

Ahora veamos los **Grupos de Noticias**
Estos se tratan de un grupo de servidores que están apoyados en programas de correo electrónico que se encargan de recoger la información que introducen los usuarios que están subscritos al grupo y que tienen interés en un tema en particular, y usando este como un foro de intercambio de información al igual que lo harían usando anuncios.

Para terminar, miremos las **Listas de Distribución:**

Estas son muy parecidas a los grupos de noticias, con la diferencia que no hay que al servidor a recoger las últimas noticias, es el servidor mismo el que envía todos los correos que recibe en el grupo, y los envía al correo del usuario.

Por ejemplo las IRC, que quiere decir Internet Relay Chat, o más conocidas como Grupos de Charlas en Internet, que es un servicio que permite intercambiar mensajes en tiempo real con otras personas.

En este servicio también es posible el intercambio de imágenes y sonidos al mismo tiempo que se encuentran en el chat o conferencia.

Ejercicio del Tema 2

Realice un ensayo que contenga:

a. La historia de la web.
b. Una descripción y aplicación amplia de cada uno delos siguientes elementos:

- El correo electrónico
- FTP
- Grupos de Noticias
- Listas de Distribución

4.3. Pistas de Aprendizaje

Tenga en cuenta que: a la hora de instalar un sistema Wi-Fi saber contratar un acceso dedicado a internet independiente al principal cuyo ancho de banda dependerá de la cantidad de usuarios que lo utilizarán.

Tenga en cuenta que: a la hora de instalar un sistema Wi-Fi saber que esta conexión a internet deberá estar protegida mediante contraseña ya que dependiendo de las instalaciones la señal puede ser captada por oficinas adyacentes o usuarios no autorizados que usen nuestro ancho de banda.

Tenga en cuenta que: a la hora de instalar un sistema Wi-Fi saber que la contraseña debe ser cambiada periódicamente por el administrador de la red avisando por mail a los usuarios autorizados.

No olvidar que: que un sistema distribuido es una colección de ordenadores autónomos enlazados por una red y soportados por aplicaciones que hacen que la colección actúe como un servicio integrado.

No olvidar que: los desafíos de un sistema distribuido son la escalabilidad, seguridad, extensibilidad, Heterogeneidad, Tolerancia a fallos, concurrencia y transparencia.

No olvidar que: Las comunicaciones basadas en el no uso de cables o wireless, son las conocidas como comunicaciones móviles.

4.4. Glosario

COMUNICACIÓN: proceso por el cual se puede transmitir información.

ESCALABILIDAD: capacidad de un sistema para mejorar sus recursos.

INALÁMBRICO: que no necesita el uso de cableado.

INTERNET: conjunto descentralizado de redes de comunicación interconectadas entre si.

INTRANET: Red de computadores privados.

LOGIN: inicio de sesión haciendo uso de un usuario y una contraseña.

RED: conjunto de computadores conectados entre sí por medio de dispositivos físicos.

ROUTER: dispositivo utilizado para la interconexión de equipos de informática.

SEGURIDAD: implementaciones para disminuir los riesgos de un sistema.

SISTEMA DISTRIBUIDO: grupo de computadores autónomos que se conectan a través de una red.

TRANSPARENCIA: propiedad de los sistemas distribuidos que consiste en hacer ver a los usuarios que es un sistema de tiempo compartido.

4.5. Bibliografía

Wheat, J. y otros. (2001). Designing a Wireless Network. Syngress Publishing, Inc.

Varela, C. Y Domínguez, L. (2002). Redes Inalámbricas. [En Línea]. Consultado:[Noviembre, 2011] Disponible en: http://blyx.com/public/wireless/redesInalambricas.pdf

Lafuente, A. Introducción a los Sistema Distribuidos.[En Línea]. Consultado: [Noviembre, 2011]. Disponible en: http://www.sc.ehu.es/acwlaroa/SDI/Apuntes/Cap1.pdf

Casas,C. Aplicaciones de la Red Internet. Editorial Vértice. [En Línea]. Disponible en: http://books.google.com.co/books?id=yE7kDQfA1t4C&pg=PA3&dq=servicios+y+aplicaciones+en+internet&hl=es&ei=MhvNTtywEITAgAf6z6HXDQ&sa=X&oi=book_result&ct=result&resnum=7&ved=0CFUQ6AEwBg#v=onepage&q=servicios%20y%20aplicaciones%20en%20internet&f=false

4.6. Tabla Referencia de Imágenes y Gráficos

Nombre imagen	Dirección	Autor
Gráfico: Política de seguridad-elementos-	http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf	Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina
Gráfico: Ejemplo práctico de una Red	http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf	Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina
Tabla de Red	http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf	Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina
Tabla determinación de Recursos	http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf	Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina
Gráfico: Propiedad de la Transparencia	http://www.sc.ehu.es/acwlaroa/SDI/Apuntes/Cap1.pdf	Lafuente, Alberto.

Gráfico: Comparación redes de celulares	http://www.ica.luz.ve/cstufano/CursoDeRedes/Wirelessdoc.pdf	N/A
Tabla generaciones	http://www.ica.luz.ve/cstufano/CursoDeRedes/Wirelessdoc.pdf	N/A
Gráfica: Comparaciones	http://www.ica.luz.ve/cstufano/CursoDeRedes/Wirelessdoc.pdf	N/A
Gráfico: Dispersión de una señal	http://www.ica.luz.ve/cstufano/CursoDeRedes/Wirelessdoc.pdf	N/A
Tabla de estándares Ethernet	http://www.ica.luz.ve/cstufano/CursoDeRedes/Wirelessdoc.pdf	N/A
Imagen: Red Bluetooth	http://www.seguridadmobile.com/bluetooth/especificacion-bluetooth/estandar-bluetooth/index.html	seguridadmobile