**Instituto Tecnológico de Culiacán**



## “AR – Tarea 2”

Instituto tecnológico de Culiacán

Materia: Administración de redes

Maestro: Lic. Carlos Sandoval Castellanos

Alumno: Güémez Sánchez Diego Arturo

Fecha: 06 de octubre del 2017.

Índice

[Introducción: 3](#_Toc495082028)

[Antecedentes: 3](#_Toc495082029)

[Tecnologías de comunicación 4](#_Toc495082030)

[Como elaborarlas e implementarlas 4](#_Toc495082031)

[Como sancionarlas 7](#_Toc495082032)

[Servicios de seguridad 8](#_Toc495082033)

[Confidencialidad 8](#_Toc495082034)

[Autenticación 8](#_Toc495082035)

[Integridad 9](#_Toc495082036)

[Control de acceso (Disponibilidad) 9](#_Toc495082037)

[No repudio 10](#_Toc495082038)

[Conclusión 11](#_Toc495082039)

# Introducción:

En este trabajo de investigación se habla acerca de las políticas de TI en organizaciones, el cómo elaborarlas, como implementarlas, como sancionarlas y como descartarlas, al igual que hablaremos de los siguientes servicios de seguridad en cuanto a TI corresponde:

* Confidencialidad
* Autenticación
* Integridad
* Control de acceso
* No repudio

# Antecedentes:

Los humanos han estado almacenando, recuperando, manipulando y comunicando información desde que los sumerios en Mesopotamia desarrollaran la escritura cerca del 3000 a. C., pero el término tecnología de la información en su significado moderno hizo su primera aparición en 1958 en un artículo publicado en la revista Harvard Business Review; sus autores Harold J. Leavitt y Thomas L. Whisler comentaron que “la nueva tecnología no tiene aún un nombre establecido. Deberíamos llamarla tecnología de la información (TI)”. Su definición consistía en tres categorías: técnicas de procesamiento, la aplicación de métodos estadísticos y matemáticos para la toma de decisión, y la simulación del pensamiento de orden superior a través de programas computacionales.

Basándose en la tecnología de almacenamiento y procesamiento empleada, es posible distinguir cuatro eras del desarrollo de TI: pre-mecánica (3000 a. C.-1450 d. C.), mecánica (1450-1840), electromecánica (1840-1940) y electrónica (1940-al presente). [1]

# Tecnologías de comunicación

Hoy en día, los negocios son más competitivos en varios aspectos, tales como el incremento de su eficiencia productiva, la mejora en la calidad de sus productos y servicios o alguna respuesta inmediata positiva que se tenga ante las necesidades del cliente. Con el propósito de lograr esos objetivos, los negocios y empresas han optado por el uso de tecnologías de información, las cuales han brindado un impacto positivo en el desempeño de las funciones de estas compañías.

****

# Como elaborarlas e implementarlas

La Administración de las Tecnologías de Información tiene como objetivo el desarrollo de sistemas de información que ayudan a resolver problemas de la administración.

Lo primero que se debe realizar en el rediseño de una organización con [sistemas de información](https://es.wikipedia.org/wiki/Sistemas_de_informaci%C3%B3n) es el análisis de las necesidades. Existen dos metodologías importantes para determinar las necesidades de información esenciales de la organización en su totalidad:

* El análisis de la empresa, el cual examina toda la organización en términos de sus unidades, funciones, procesos y elementos de información
* El análisis de los [factores críticos para el éxito](https://es.wikipedia.org/w/index.php?title=Factores_cr%C3%ADticos_para_el_%C3%A9xito&action=edit&redlink=1), el cual se basa en la premisa de que las necesidades de información de una organización están determinadas por un número reducido de factores críticos para el éxito (CSF, del inglés critical success factors).

Existen cuatro clases de cambio estructural en las organizaciones que se pueden presentar en el rediseño de una organización sobre la base de sistemas de información:

1. Automatización, la forma más común de cambio en la organización que la tecnología de información hace posible. Esta consiste en el uso de computadoras para acelerar el desempeño de tareas existentes.
2. Racionalización, consiste en la agilización de los procedimientos operativos estándar eliminando cuellos de botella obvios, de modo que la automatización haga más eficientes los procedimientos operativos.
3. Reingeniería, esta implica rediseñar radicalmente el flujo de trabajo y los procesos de negocios que se siguen para generar productos y servicios, con el objeto de reducir radicalmente los costos del negocio
4. Cambios de paradigma, esta es la forma más radical de cambio en los negocios e implica una reconceptualización de la naturaleza del negocio y de la organización misma.

Un sistema de información nuevo se construye como solución de algún tipo de problema o conjunto de ellos que la organización percibe ante sí. El término desarrollo de sistemas se refiere a todas las actividades implicadas en la producción de una solución de sistemas de información para un problema u oportunidad de la organización. El desarrollo de sistemas es un tipo de resolución de problemas estructurada con actividades bien definidas. Estas consisten en:

1. El análisis de sistemas. Análisis de un problema que la organización tratará de resolver con un sistema de información. Además de sugerir una solución el análisis de sistemas implica un estudio de factibilidad para determinar si la solución es factible, para ello es preciso analizar tres áreas de factibilidad:
   1. Factibilidad técnica
   2. Factibilidad económica.
   3. Factibilidad operativa.
2. Diseño de sistemas. Detalla cómo un sistema satisfará los requisitos de información determinados por el análisis de sistemas. El diseño puede ser lógico, el cual presenta los componentes del sistema de información; y físico, el cual es el proceso de traducción del modelo lógico al diseño técnico específico el sistema nuevo.
3. Programación. Proceso de traducir a código de programa las especificaciones del sistema preparadas durante la etapa de diseño.
4. Pruebas. Proceso exhaustivo y minucioso que determina si el sistema produce los resultados deseados en condiciones conocidas.
5. Conversión. Proceso de cambiar del sistema antiguo al nuevo. Existen cuatro estrategias de conversión principales:
   1. Estrategia paralela. Enfoque de conversión seguro y conservador en el que tanto sistema antiguo como posible sustituto operan juntos durante un tiempo hasta que todos quedan convencidos de que el sistema nuevo funciona correctamente.
   2. Estrategia de cambio directo. Enfoque de conversión riesgoso en el que el sistema nuevo sustituye totalmente al antiguo en un día designado.
   3. Estrategia de estudio piloto. Introduce el sistema nuevo en un área limitada de la organización hasta que demuestre ser plenamente funcional; sólo entonces podrá efectuarse la conversión al sistema nuevo en toda la organización.
   4. Estrategia del método de fases. Introduce el sistema nuevo en etapas, ya sea por funciones o por unidades de organización.
6. Producción y mantenimiento. Una vez que se ha instalado el sistema nuevo y se ha terminado de efectuar la conversión, se dice que el sistema está en producción. En esta etapa, tanto los usuarios como los especialistas técnicos revisan periódicamente el sistema para determinar qué tan bien está cumpliendo con sus objetivos originales y decidir si conviene efectuar alguna modificación. Los cambios con el fin de corregir errores, cumplir con requisitos nuevos o mejorar la eficiencia del procesamiento reciben el nombre de mantenimiento.

Los sistemas difieren en cuanto a su tamaño, complejidad tecnológica y los problemas de organización que se supone van a resolver. Puesto que hay diferentes tipos de sistemas y de situaciones en los que cada sistema se concibe o construye, se han desarrollado varios métodos de construcción de sistemas, los cuales deben cumplir con la metodología apropiada. [2]



# Como sancionarlas

**Artículo 6º** Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

**Artículo 7º** Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

**Artículo 8º** Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

**Artículo 9º** Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de uso restringido sobre personas o grupos de personas naturales o jurídicas.

**Artículo 10º** Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos o dispositivos; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

**Artículo 11º** Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

**Artículo 12º** Falsificación de documentos. El que, a través de cualquier medio, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro. [3]

# Servicios de seguridad

## Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad. [4]

## Autenticación

Es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.

Esta propiedad se puede considerar como un aspecto de la integridad -si está firmado por alguien, está realmente enviado por el mismo- y así figura en la literatura anglosajona. [4]



## Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

La integridad también es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada, para salvaguardar la precisión y completitud de los recursos.

La violación de integridad se presenta cuando un empleado, programa o proceso modifica o borra datos importantes que son parte de la información.

La integridad garantiza que los datos permanezcan inalterados excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital es uno de los pilares fundamentales de la seguridad de la información. [4]

## Control de acceso (Disponibilidad)

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

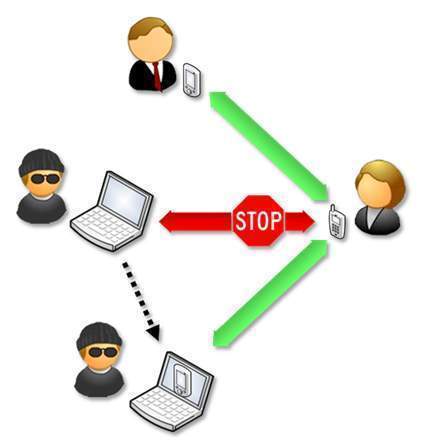
Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar. [4]

## No repudio

Es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.

Esta propiedad se puede considerar como un aspecto de la integridad -si está firmado por alguien, está realmente enviado por el mismo- y así figura en la literatura anglosajona. [4]



# Conclusión

Como conclusión podríamos decir que las nuevas Tecnologías de la Información y de la Comunicación han evolucionado espectacularmente en los últimos años, debido especialmente a su capacidad de interconexión a través de la Red. Esta nueva fase de desarrollo va a tener gran impacto en la organización de la enseñanza y el proceso de aprendizaje. La acomodación del entorno educativo a este nuevo potencial y la adecuada utilización didáctica del mismo supone un reto sin precedentes.

# Bibliografía

Venezuela, G. O. (s.f.). *Wipo.* Recuperado el 6 de octubre de 2017, de http://www.wipo.int/edocs/lexdocs/laws/es/ve/ve041es.pdf

*Wikipedia*. (24 de septiembre de 2017). Recuperado el 6 de octubre de 2017, de https://es.wikipedia.org/wiki/Tecnolog%C3%ADa\_de\_la\_informaci%C3%B3n

*Wikipedia*. (26 de agosto de 2017). Recuperado el 6 de octubre de 2017, de https://es.wikipedia.org/wiki/Administraci%C3%B3n\_de\_las\_tecnolog%C3%ADas\_de\_la\_informaci%C3%B3n

*Wikipedia*. (12 de septiembre de 2017). Recuperado el 6 de octubre de 2017, de https://es.wikipedia.org/wiki/Seguridad\_de\_la\_informaci%C3%B3n