UNIVERSIDAD TECNOLÓGICA NACIONAL

FACULTAD REGIONAL TUCUMÁN

SEGURIDAD INFORMÁTICA

2022

Comisión: 3k1

TRABAJO FINAL INTEGRADOR

Temas:

- **Sistemas Biométricos**
- **Auditoría Informática**

Docente:

Ing. José Daniel Zakhour

Integrantes:

[46406] Zurita, José Matías

[44528] Madozzo Romay, Bruno

Sistemas biométricos

TEMA: SISTEMAS BIOMÉTRICOS

¿Qué es la biometría?

La biometría (del griego bios vida y metron medida) es la toma de medidas estandarizadas de los seres vivos (personas) o de procesos biológicos (interacciones). Se llama también biometría al estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos.

En las tecnologías de la información (TI), la «autentificación biométrica» o «biometría informática» es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autentificación, es decir, «verificar» su identidad.

Las huellas dactilares, la retina, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). Algunos rasgos biométricos, como la voz, comparten aspectos físicos y del comportamiento.

¿Cómo funciona?

En un sistema de Biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de acierto que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 99,9%).

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (False Acceptance Rate o FAR), la tasa de falso negativo (False NonMatch Rate o FNMR, también False Rejection Rate o FRR), y la tasa de fallo de alistamiento (Failure-to-enroll Rate, FTE o FER).

En los sistemas biométricos reales el FAR y el FRR puede transformarse en los demás cambiando cierto parámetro. Una de las medidas más comunes de los sistemas biométricos reales es la tasa en la que el ajuste en el cual acepta y rechaza los errores es igual: la tasa de error igual (Equal Error Rate o EER), también conocida como la tasa de error de cruce (Cross-over Error Rate o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto.

Las tasas de error anunciadas implican a veces elementos idiosincrásicos o subjetivos. Por ejemplo, un fabricante de sistemas biométricos fijó el umbral de aceptación alto, para reducir al mínimo las falsas aceptaciones; en la práctica, se permitían tres intentos, por lo que un falso rechazo se contaba sólo si los tres intentos resultaban fallidos (por ejemplo: escritura, habla, etc.), las opiniones pueden variar sobre qué constituye un falso rechazo. Si entró a un sistema de verificación de firmas usando mi inicial y apellido, ¿puedo decir legítimamente que se trata de un falso rechazo cuando rechace mi nombre y apellido?

A pesar de estas dudas, los sistemas biométricos tienen un potencial para identificar a individuos con un grado de certeza muy alto. La prueba forense del ADN goza de un grado particularmente alto de confianza pública actualmente (ca. 2004) y la tecnología está orientándose al reconocimiento del iris, que tiene la capacidad de diferenciar entre dos individuos con un ADN idéntico.

¿Qué beneficios tiene?

Uno de los beneficios que otorga la tecnología biométrica es que hace que no sea necesario llevar una tarjeta o llave para acceder a un edificio. Las infraestructuras de grandes redes empresariales, las identificaciones en el gobierno, las transacciones bancarias seguras, y los servicios sociales y de salud, entre otros ámbitos, ya se benefician del uso de este tipo de verificaciones.

Asociada a otras tecnologías de restricción de accesos, la biometría garantiza uno de los niveles de autenticación menos franqueables en la actualidad. Además, los inconvenientes de tener que recordar una password o un número de PIN de acceso serán pronto superados gracias al uso de los métodos biométricos, debido a que estos últimos presentan notables ventajas: están relacionados de forma directa con el usuario, son exactos y permiten hacer un rastreo de auditorías.

La utilización de un dispositivo biométrico permite que los costos de administración sean más pequeños, ya que sólo se debe realizar el mantenimiento del lector, y que una persona se encargue de mantener la base de datos actualizada. Otro beneficio: las características biométricas de una persona son intransferibles a otra.

Tablas comparativas y de participantes

Lo que sigue a continuación es una tabla en la que recogen las diferentes características de los sistemas biométricos:

	Iris	Huella	Venas	Mano	Facial (2D/3D)
Fiabilidad	Muy alta	Muy alta	Muy alta	Alta	Media/Alta
Facilidad de uso	Media	Alta	Muy alta	Alta	Alta
Prevención de ataques	Muy alta	Alta	Muy alta	Alta	Media/Alta
Aceptación	Media	Alta	Alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Media/Alta

La industria de biométrica ofrece varias tecnologías. Cada tecnología es considerada como un segmento de mercado diferente. Las más conocidas son las huellas dactilares, reconocimiento de cara y reconocimiento de iris (ojos). El cuadro abajo contiene las diferentes tecnologías, aplicaciones horizontales y los principales mercados verticales (en el sector privado y público) que ofrece la industria biométrica:

Tecnología	Aplicación horizontal	Principales mercados verticales
AFIS/Lifescan	Controles de vigilancia	Servicios policiales y militares
Reconocimiento de cara	Identificación sin contacto	Farmacéuticas, hospitales, industria pesada y obras
Geometría de mano	Identificación criminal	Hospitales y sector salud
Reconocimiento de iris (ojo)	Acceso a sistemas	Industria manufacturera
Reconocimiento de voz	Acceso a instalaciones	Viajes y turismo
Escritura y firma	Vigilancia	

Los estándares asociados a tecnologías biométricas

En los últimos años se ha notado una preocupación creciente por las organizaciones regulatorias respecto a elaborar estándares relativos al uso de técnicas biométricas en el ambiente informático. Esta preocupación es reflejo del creciente interés industrial por este ámbito tecnológico, y a los múltiples beneficios que su uso aporta. No obstante, la estandarización continua aún sigue siendo deficiente y como resultado de ello, los proveedores de soluciones biométricas continúan suministrando interfaces de software propietario para sus productos, lo que dificulta a las empresas el cambio de producto o vendedor.

A nivel mundial el principal organismo que coordina las actividades de estandarización biométrica es el Sub-Comité 17 (SC17) del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC).

En Estados Unidos desempeñan un papel similar el Comité Técnico M1 del INCITS (InterNational Committee for Information Technology Standards), el National Institute of Standards and Technology (NIST) y el American National Standards Institute (ANSI).

Existen además otros organismos no gubernamentales impulsando iniciativas en materias biométricas tales como: Biometrics Consortium, International Biometrics Groups y BioAPI. Este último se estableció en Estados Unidos en 1998 compuesto por las empresas Bioscrypt, Compaq, Iridiam, Infineon, NIST, Saflink y Unisis. El Consorcio BioAPI desarrolló conjuntamente con otros consorcios y asociaciones, un estándar que promoviera la conexión entre los dispositivos biométricos y los diferentes tipos de programas de aplicación, además de promover el crecimiento de los mercados biométricos.

Algunos de los estándares más importantes son:

- *Estándar ANSI X.9.84:* creado en 2001, por la ANSI (American National Standards Institute) y actualizado en 2003, define las condiciones de los sistemas biométricos para la industria de servicios financieros haciendo referencia a la transmisión y almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.
- *Estándar ANSI / INCITS 358:* creado en 2002 por ANSI y BioApi Consortium, presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.
- *Estándar NISTIR 6529:* también conocido como CBEFF (Common Biometric Exchange File Format) es un estándar creado en 1999 por NIST y Biometrics Consortium que propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica.
- *Estándar ANSI 378:* creado en 2004 por la ANSI, establece criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de

identidad e identificación, empleando información biométrica proveniente de otros sistemas.

- *Estándar ISO 19794-2:* creado en 2005 por la ISO/IEC con propósitos similares a la norma ANSI 378, respecto a la que guarda mucha similitud.
- *Estándar PIV-071006:* creado en 2006 por el NIST y el FBI en el contexto de la norma FIPS 201 del gobierno de EE. UU, establece los criterios de calidad de imagen que deben cumplir los lectores de huellas dactilares para poder ser usados en procesos de verificación de identidad en agencias federales.

Los procesos de autentificación e identificación biométrica

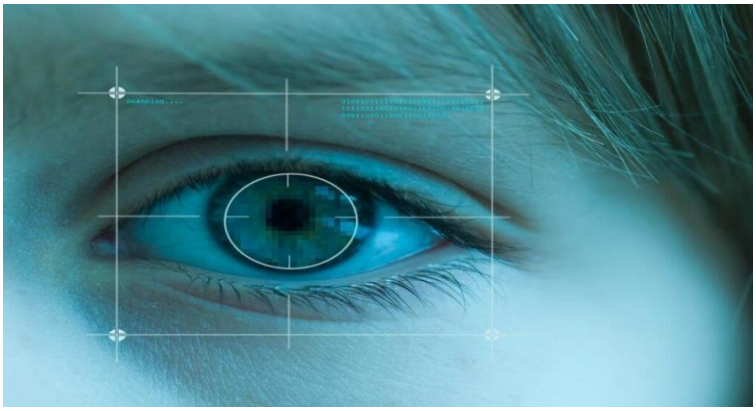
En el proceso de autentificación (o verificación) los rasgos biométricos se comparan solamente con los de un patrón ya guardado, este proceso se conoce también como uno-para-uno (1:1). Este proceso implica conocer presuntamente la identidad del individuo a autentificar, por lo tanto, dicho individuo ha presentado algún tipo de credencial, que después del proceso de autentificación biométrica será validada o no.

En el proceso de identificación los rasgos biométricos se comparan con los de un conjunto de patrones ya guardados, este proceso se conoce también como uno-para-muchos (1:N). Este proceso implica no conocer la identidad presunta del individuo, la nueva muestra de datos biométricos es tomada del usuario y comparada una a una con los patrones ya existentes en el banco de datos registrados. El resultado de este proceso es la identidad del individuo, mientras que en el proceso de autentificación es un valor verdadero o falso.

El proceso de autentificación o verificación biométrica es más rápido que el de identificación biométrica, sobre todo cuando el número de usuarios (N) es elevado. Esto es debido a que la necesidad de procesamiento y comparaciones es más reducido en el proceso de autentificación. Por esta razón, es habitual usar autentificación cuando se quiere validar la identidad de un individuo desde un sistema con capacidad de procesamiento limitada o se quiere un proceso muy rápido.

Un ejemplo de esto es la aplicación móvil OneID, diseñada para sistemas Single Sign-On, que utiliza la dactiloscopía.1 Una coalición de empresas de hardware y software denominada Alianza Fido, se dedica al estudio de sistemas biométricos para reemplazar el uso de contraseñas, ya sea con lectores de huellas dactilares, faciales o identificadores de voz. Un ejemplo de su producción es YubiKey, producto de la empresa Yubico.1

Reconocimiento de iris

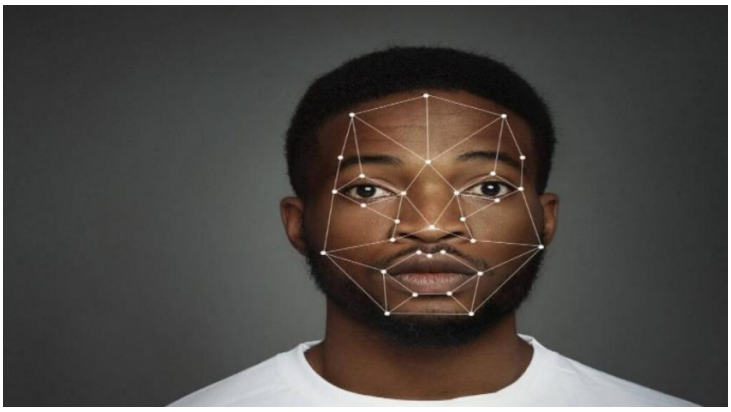


El iris es una membrana pigmentada suspendida en el interior del ojo, entre la córnea y el cristalino. Regula el tamaño de la pupila para controlar la cantidad de luz que ingresa al ojo. Adquiere su pigmentación de la melanina.

Antes de que ocurra el reconocimiento de iris, se localiza el iris usando características del punto de referencia. Estas características del punto de referencia y la forma distinta del iris permiten digitalización de la imagen, el aislamiento de la característica, y la extracción. La localización del iris es un paso importante en el reconocimiento del iris porque, si está hecho incorrectamente, el ruido resultante (e.g., pestañas, reflexiones, pupilas, y párpados) en la imagen puede conducir al bajo rendimiento.

Debido a que el infrarrojo tiene energía insuficiente para causar efectos fotoquímicos, la modalidad potencial principal de daños es termal. Cuando se produce NIR usando los diodos electroluminosos, la luz que resulta es incoherente. Cualquier riesgo para la seguridad del ojo es remoto con una sola fuente de led usando tecnología de led de hoy. Los iluminadores múltiples de led pueden, sin embargo, producir daño en el ojo si no es diseñado y usado cuidadosamente.

Reconocimiento facial 2D y 3D



El rostro de la persona es una característica física que permite la identificación de la persona de manera única y estable. Existen equipos que capturan el patrón 2D (proyección en el plano) y equipos que capturan el patrón 3D (descripción volumétrica del rostro).

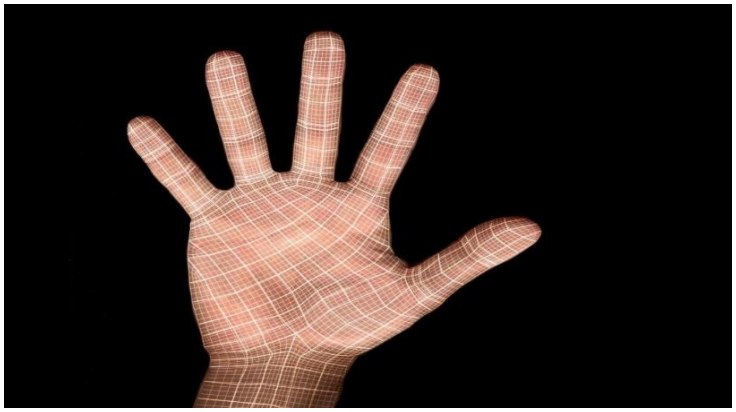
La desventaja de los equipos 2D es que el sistema no distingue si lo que está capturando es realmente un rostro o una fotografía de un rostro, por lo que no ofrecen un nivel de seguridad suficiente en la mayoría de aplicaciones de control de acceso.

Los equipos con tecnología biométrica facial 3D incluyen la tecnología infrarroja combinada con la 3D, con lo que inhabilitan el uso de caretas o fotografías para falsificar el rostro. Gracias a esto, la biometría facial 3D permite la identificación sin contacto de forma muy rápida y segura, debido a que se consigue construir un patrón 3D del rostro de la persona identificada.

Por lo tanto, los equipos 3D ofrecen una seguridad mucho más elevada ya que necesitan un rostro real (no una fotografía) para identificar el usuario. Por esta razón en aplicaciones de control de acceso y control de presencia es aconsejable usar equipos de reconocimiento facial 3D.

Otra característica importante de los sistemas de reconocimiento facial es la capacidad de identificar a la persona sin contacto (normalmente del orden de decenas de centímetros), por lo que estos sistemas son mucho menos intrusivos que los basados en biometría dactilar, de iris o vascular. Aparte de ser menos intrusivos, esta capacidad de identificación a distancia, hace que tengan muy buena aceptación para aplicaciones de control de acceso o control de presencia en entornos en que el contacto directo del usuario con el terminal pueda representar problemas (ya sea por cuestiones de higiene o bien por qué los usuarios llevan guantes).

Reconocimiento vascular



En la biometría vascular se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo. A diferencia de la huella dactilar el patrón biométrico es interno, por esta razón no deja rastro y solo se puede conseguir en presencia de la persona. Es por tanto muy difícil el robo de identidad.

Debido a estas características es especialmente indicado para entornos de alta seguridad, así como en entornos duros, en que la superficie del dedo (y por consiguiente la huella superficial) pueden estar en mal estado, erosionados o poco limpios.

Las aplicaciones de la biometría

Las aplicaciones de la tecnología biométrica son muchas y están relacionadas con la identificación de la persona. Entre las principales aplicaciones están las aplicaciones de control de acceso físico, control de presencia (o fichaje laboral), control de acceso a información y recursos o control de firma biométrica.

Para las aplicaciones de control de acceso y control de presencia es habitual el uso de la tecnología biométrica en combinación con otras tecnologías de identificación por tarjeta, como por ejemplo las tarjetas RFID. Esta combinación permite que el patrón biométrico se guarda en la tarjeta, por lo que es el usuario quién custodia esta información y no se guarda en el dispositivo de control.

El avance de la tecnología y la miniaturización de los dispositivos ha permitido recientemente el uso de escáneres de huella dactilar en dispositivos electrónicos de consumo, como ordenadores portátiles y móviles.

Suelen incorporarse sistemas biométricos para el control de asistencia, el sistema reconoce la entrada y salida del individuo, lo que facilita un control de las horas trabajadas, además de evitar falsedades en el registro de asistencia.

Cuestiones y preocupaciones

Como con otros procesos tecnológicos y de gran alcance, las excesivas dudas en lo referente a la biometría pueden eclipsar una crítica más general. La biometría puede llegar a asociarse con fallos severos de la justicia en aquellos casos en los que la tecnología ha desviado la atención del verdadero foco, así, un individuo podría:

- introducir deliberadamente ADN en la escena de un crimen
- relacionar sus propios parámetros biométricos con la identidad de otra persona

Robo de identidad

Las preocupaciones acerca del robo de identidad por el uso de la Biometria aún no han sido resueltas. Si el número de tarjeta de crédito de una persona es robado, por ejemplo, puede causarle a esa persona grandes dificultades. Si sus patrones de escaneado de iris son robados, sin embargo, y eso permite a otra persona acceder a información personal o a cuentas financieras, el daño podría ser irreversible ya que a diferencia del uso de claves o frases clave, los datos biométricos de un individuo no pueden cambiarse y una vez comprometidos no se podría volver a tener seguridad en su uso.

Frecuentemente, las tecnologías biométricas han sido puestas en uso sin medidas adecuadas de seguridad para la información personal que es resguardada a través de las mismas.

Privacidad

Aunque la biometría es frecuentemente utilizada como un medio para combatir la criminalidad, existe la preocupación de que la biometría pueda ser utilizada para disminuir las libertades personales de los ciudadanos.

Los desarrollos en tecnología video digital, infrarrojos, rayos X, inalámbricas, sistemas de posicionamiento global, biometría, escaneado de imágenes, reconocimiento de voz, ADN, e identificación de ondas cerebrales le proveen al gobierno con nuevos métodos para «buscar e investigar» vastas bases de datos individuales y colectivas de información sobre la población en general.

Casos de uso

Consumidor

La autenticación biométrica mediante dispositivos móviles se usa principalmente para banca móvil y comercio electrónico. Por ejemplo, los clientes pueden autenticar transacciones que se originan desde sus aplicaciones minoristas o de banca móvil mediante datos biométricos de reconocimiento facial o voz.

Las empresas Fintech que se integran con cuentas bancarias de clientes también aprovechan los datos biométricos de los dispositivos móviles para autenticar las transacciones. Este puede ser en un punto de venta físico (p. ej., realizar el reconocimiento facial al usar Apple Pay o Samsung Pay en una ubicación física tradicional) o para autenticar transferencias electrónicas de fondos a través de una aplicación fintech móvil (p. ej., Venmo o PayPal).

Empresa

Las empresas pueden usar datos biométricos mediante dispositivos móviles como una forma de autenticación externa. En este proceso, un empleado puede intentar acceder a una aplicación corporativa a través de un navegador web lanzado en un equipo portátil o tableta. Al navegar por el portal de inicio de sesión, el empleado ingresa su nombre de usuario. Se enviará una notificación al dispositivo móvil registrado del usuario autorizado. Este es el factor de autenticación de “posesión”. Solo el usuario que posee el dispositivo registrado puede autorizar el intento de inicio de sesión. Recibir una notificación de autenticación sin haber intentado un inicio de sesión podría indicar un inicio de sesión fraudulento.

Una verificación biométrica en el dispositivo es el segundo factor de autenticación. El uso de reconocimiento facial, por ejemplo, verifica que el individuo que posee el dispositivo en el momento de la solicitud de inicio de sesión es, de hecho, el usuario autorizado. Esto impide el acceso ilícito a los datos empresariales si un dispositivo se pierde o es robado.

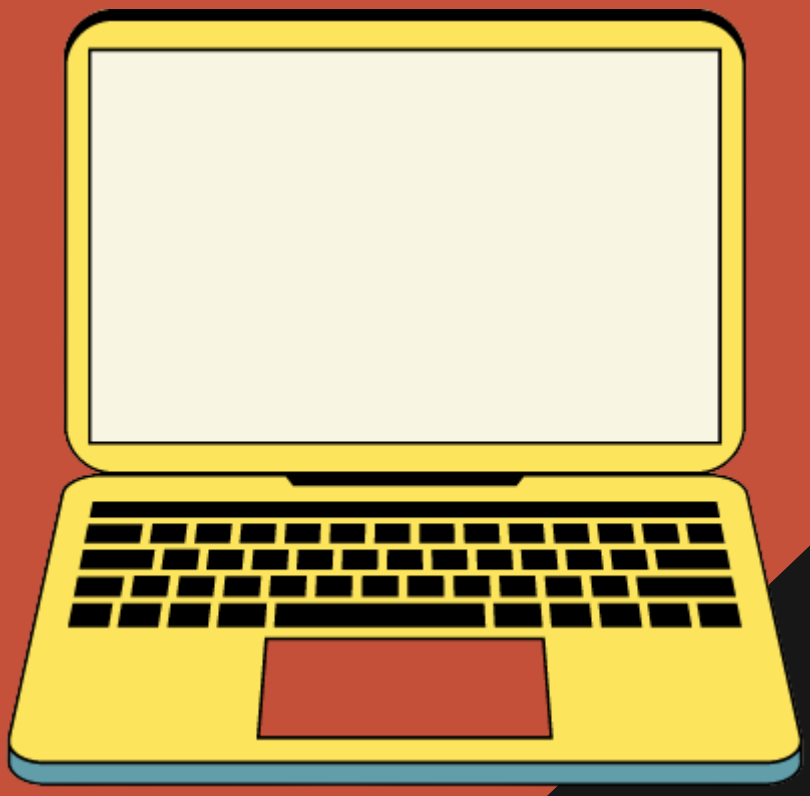
Los casos de uso empresariales y comerciales como estos están estimulando el crecimiento significativo en el mercado de autenticación biométrica mediante dispositivos móviles, que se espera que alcance un valor neto de casi $50 mil millones en 2022.

Conclusion

La biometría es usada en muchas aplicaciones fuera del área de la seguridad informática. Lugares como los aeropuertos frecuentemente utilizan sistemas de reconocimiento de rostros para buscar criminales, la policía usa sistemas de reconocimiento de huellas digitales para rastrear sospechosos, la termografía infrarroja puede identificar personas que se encuentran bajo la influencia de varios tipos de drogas. Los sistemas biométricos que trabajan en aplicaciones distintas a la autenticación podrían no ser exitosos si se usan en aplicaciones de autenticación.
La biometría es una de las mejores formas de autenticar usuarios, debido a que valida características inherentes al usuario y que teóricamente el único que puede tener tales características es el verdadero usuario.

Auditoria Informatica

{ }



TEMA: AUDITORÍA INFORMÁTICA

¿Qué es la Auditoría?

Es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados. El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso.

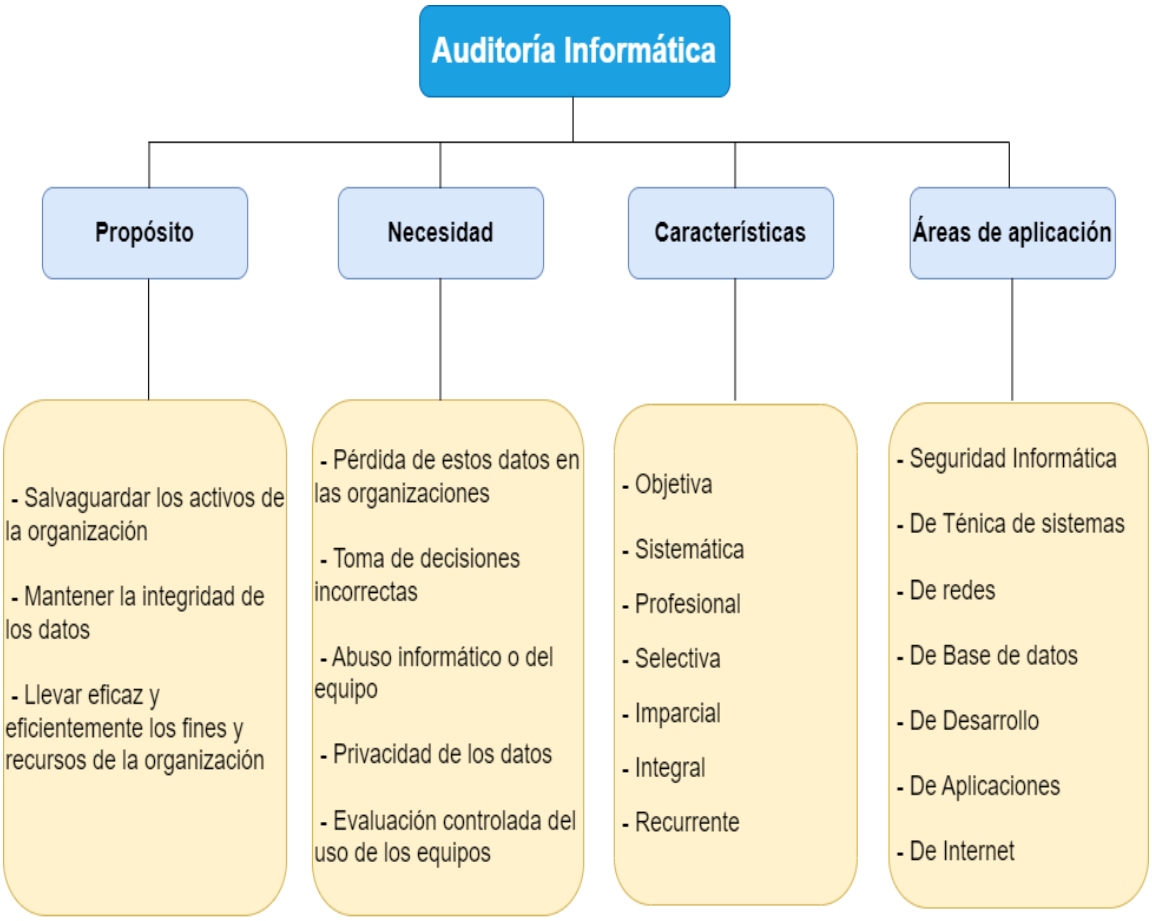
¿Qué es la Auditoría Informática?

La **Auditoría informática** es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Así mismo permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

- Desempeño
- Fiabilidad
- Eficacia
- Rentabilidad
- Seguridad
- Privacidad



Otra definición

La **auditoría informática** es el conjunto de procedimientos y técnicas que nos sirven para evaluar un sistema informático en base a unas reglas establecidas de antemano. Este sistema puede ser tanto hardware (máquinas) como software (aplicaciones informáticas).
Las auditorías pueden tener diferentes objetivos:

- Analizar la eficiencia de un sistema informático
- Verificar el cumplimiento de una normativa
- Revisar la gestión adecuada de los recursos existentes

Tipos de Auditoría Informática

Auditoría interna: es aquella que se hace adentro de la empresa; sin contratar a personas de afuera.

Auditoría externa: como su nombre lo dice es aquella en la cual la empresa contrata a personas de afuera para que haga la auditoria en su empresa. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Objetivos de la Auditoría Informática

La **auditoría informática** deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría informática es de **vital importancia para el buen desempeño de los sistemas de información,** ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

Los aspectos relativos al control de la seguridad de la Información tienen tres líneas básicas en la auditoria del sistema de información:

- La **seguridad operativa** de los programas, seguridad en suministros y funciones auxiliares, seguridad contra radiaciones, atmósferas agresivas, agresiones y posibles sabotajes, seguridad físicos de las instalaciones, del personal informático, etc.
- La **confidencialidad y la seguridad informática** hace referencia no sólo a la protección del material, el logicial, los soportes de la información, sino también al control de acceso a la propia información.
- En relación a los aspectos jurídicos y económicos relativos a la seguridad de la información hace referencia a **analizar la adecuada aplicación del sistema de información en la empresa** en cuanto al derecho a la intimidad y el derecho a la información, y controlar los cada vez más frecuentes delitos informáticos que se cometen en la empresa.

Además, debe evaluar todo lo relacionado a la informática, organización de centros de información, hardware y software.

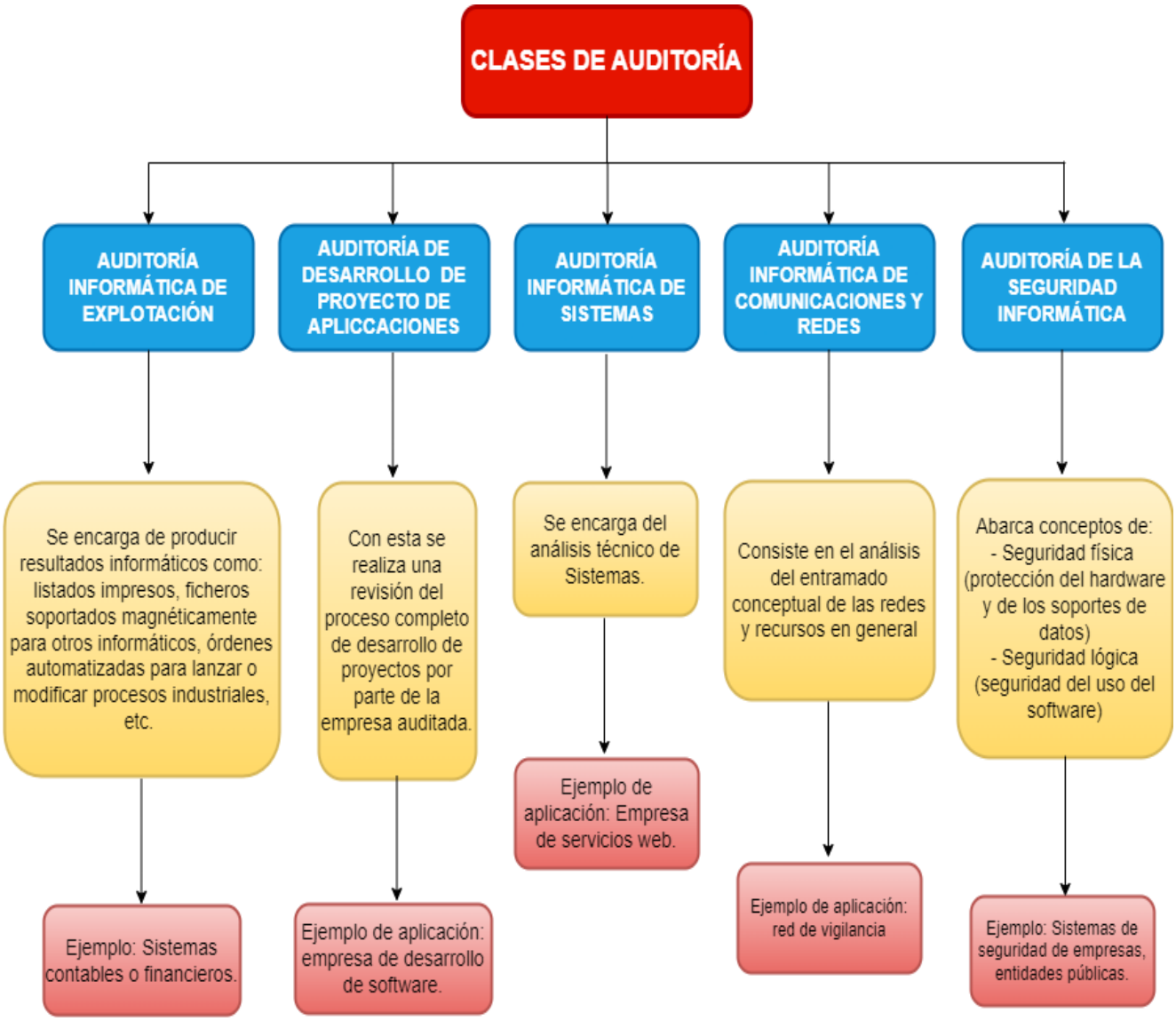
Importancia de la Auditoría Informática

La **auditoría informática** permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización.

Se hace énfasis en la revisión independiente, debido a que el auditor debe mantener independencia mental, profesional y laboral para evitar cualquier tipo de influencia en los resultados de la misma.

La **técnica de la auditoría**, siendo por tanto aceptables equipos multidisciplinarios formados por titulados en Ingeniería Informática e Ingeniería Técnica en Informática y licenciados en derecho especializados en el mundo de la auditoría.

Clases de Auditoría: Características y ejemplos



Auditoría Informática de explotación

Es el control que se realiza sobre las funciones del sistema de información para asegurar que las mismas se efectúen de forma regular, ordenada y que satisfagan los requisitos empresariales. La Explotación Informática se ocupa de producir resultados informáticos de todo tipo. Para realizar la Explotación Informática se dispone de una materia prima, los Datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. Explotación debe recepcionar sólo programas fuentes, los cuales hayan sido aprobados por Desarrollo.
La Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico.

Auditoria Informática De Desarrollo De Proyectos O Aplicaciones

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizados tiene la empresa. Una Aplicación recorre las siguientes fases:

- Prerrequisitos del Usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Reprogramación y Programación)
- Pruebas
- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoria deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Auditoría Informática de Sistemas

Es aquella que contempla el estudio, revisión y valoración de Todos los elementos (o parte de ellos) de los sistemas automáticos de procesamiento de la información, incluyendo operaciones no automáticas relacionadas con ellos y su interfaz correspondiente.
Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones, líneas y redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas. La propia existencia de aplicativos para la obtención de estadísticas desarrollados por los técnicos de Sistemas de la empresa auditada, y su calidad, proporcionan al auditor experto una visión bastante exacta de la eficiencia y estado de desarrollo de los Sistemas.

Auditoría de comunicaciones y redes

Se aplica en empresas que poseen tecnologías de comunicaciones y/o sistemas de información que están conectados ya sea mediante intranet o internet. La auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales.
El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre cuántas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo,

las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas.

Auditoría de la seguridad informática

Es la herramienta principal para poder conocer el estado de seguridad en que se encuentra una empresa en relación con sus sistemas informáticos, de comunicación y acceso a internet. Estas auditorías permiten mejorar los sistemas e incrementar la ciberseguridad, siendo fundamentales para poder garantizar el funcionamiento del negocio y proteger la integridad de la información que manejan.
Una auditoría de seguridad informática es un procedimiento que evalúa el nivel de seguridad de una empresa o entidad, analizando sus procesos y comprobando si sus políticas de seguridad se cumplen.
El principal objetivo de una auditoría de seguridad es detectar las vulnerabilidades y debilidades de seguridad que pueden ser utilizadas por terceros malintencionados para robar información, impedir el funcionamiento de sistemas, o en general, causar daños a la empresa.

Metodología de trabajo de la Auditoría Informática:

Etapas de la metodología:

1. **Alcance y objetivos de la auditoría informática**

   Los alcances expresan los límites de la auditoría entre autoridades y clientes sobre las funciones y materias auditadas. Así mismo fijan y dan a conocer los objetivos que se pretenden alcanzar.

2. **Estudio inicial del entorno auditable**

   Consiste en examinar las funciones y actividades siguientes:

   - Aplicaciones, base de datos y archivos:

     El entorno se aplica mediante las siguientes características:

- Volumen, antigüedad y complejidad de las aplicaciones.
- Metodología del diseño
- Documentación
- Cantidad y complejidad de base de datos y archivos

- Entorno operacional:

  Se determina los conocimientos de los siguientes factores:
  - *Situación geográfica de los sistemas:* ubicación de los Centros de Proceso de Datos, verificando la existencia de responsables por cada uno de ellos.
  - *Arquitectura y configuración de hardware y software:* configuración adecuada para cada uno de los equipos y sistemas para constituir un Sistema compatible e intercomunicado.
  - *Inventario de hardware y software:* recabar información en elementos físicos y lógicos como CPU´s, unidades de control local, programas de utilidad adquiridos o desarrollados, etc.
  - *Comunicaciones y redes de comunicaciones:* se debe tener acceso a la red pública de comunicaciones para obtener información de las Redes Locales de la empresa.

- Organización:

  El auditor deberá conocer el organigrama de la empresa para conocer la estructura oficial, así también los departamentos que lo componen determinando cuales son las funciones más importantes.
  Dentro de la organización se debe tener en cuenta:

  - *Relaciones jerárquicas y funcionales entre órganos de la organización:* verificación del cumplimiento de las relaciones funcionales y jerárquicas previstas.
  - *Flujos de información:* canales alternativos de información con los que la empresa cuente.
  - *Números de puestos de trabajo:* comprobar que los Nombres de los puestos de trabajo corresponden a funciones reales distintas.
  - *Número de personas por Puesto de Trabajo:* se deberá exponer el número de empleados reales de cada sección auditada.

3. Determinación de los recursos necesarios para realizar la auditoría

Los recursos se determinan en:

- *Recursos materiales:* los cuales se constituyen en materiales de hardware y software.

- *Recursos humanos:* las características y perfiles del personal seleccionado dependen de la materia auditable.

4. Elaboración del plan y de los programas de trabajo

El Plan de auditoría se desarrolla teniendo en cuenta lo siguiente:

- La revisión debe realizarse por áreas generales o áreas específicas.
- Si la auditoria es global o parcial el volumen determina el número de auditores necesarios.
- El Plan estructura las tareas a realizar por cada integrante del equipo.
- Establecer las prioridades de materias auditables, de acuerdo con las prioridades del cliente.
- Establecer la disponibilidad futura del personal y de los demás recursos.

5. Actividades propiamente dichas de la auditoría

Las técnicas y herramientas que se utilizan son:

Auditoría por temas generales o por áreas específicas:

- Por áreas generales, resulta evidente la calidad y el empleo de más tiempo total y mayores recursos.
- Por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a las mismas.

Técnicas de trabajo:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas
- Simulación
- muestreos

Herramientas:

- Cuestionario general inicial
- Cuestionario-Checklist
- Estándares
- Monitores
- Simuladores (Generadores de datos)
- Paquetes de auditoría (Generadores de programas)
- Matrices de riesgo

6. Confección y redacción del informe final

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

7. Redacción de la carta de Introducción o carta de presentación del informe final

La carta de introducción tiene especial importancia porque en la misma se resume la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargó o contrató la auditoría.

Conclusión

La auditoría informática consiste en verificar un sistema de información automatizado que nos permita obtener una deducción del funcionamiento de dicho sistema. Cabe aclarar que la informática no gestiona la empresa, solo ayuda a la toma de decisiones. La auditoría informática existe ya que juega un rol importante en el funcionamiento de una empresa. El auditor informático debe velar por el correcto uso de los recursos que la empresa provee para disponer de una eficiente y eficaz herramienta de colaboración en el sistema de información.