Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

COMPARACIÓN DE LAS TECNOLOGÍAS DE CONTROL DE ACCESO A LAS INSTALACIONES EN UNA ORGANIZACIÓN

SUAN KATHLEEN JUI BAECHLI

Asesorado por: Ing. Christian Alberto Barneónd León

Guatemala, noviembre de 2005

UNIVERSIDAD SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

COMPARACIÓN DE LAS TECNOLOGÍAS DE CONTROL DE ACCESO A LAS INSTALACIONES EN UNA ORGANIZACIÓN

TRABAJO DE GRADUACIÓN
PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

SUAN KATHLEEN JUI BAECHLI
Asesorado por: Ing. Christian Alberto Barneónd León

AL CONFERÍRSELE EL TÍTULO DE
INGENIERA EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2005

UNIVERSIDAD SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADOR	Inga. Floriza Felipa Avila de Medinilla
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

COMPARACIÓN DE LAS TECNOLOGÍAS DE CONTROL DE ACCESO A LAS INSTALACIONES EN UNA ORGANIZACIÓN,

tema que me fuera asignado por la Coordinación de la Carrera de Ciencias y Sistemas en enero de 2004.

Suan Kathleen Jui Baechli

AGRADECIMIENTOS A:

Dios Por brindarme la oportunidad de obtener este triunfo y por guiar mi camino en todo momento.

Mis padres Mario Jui, por enseñarme a ser una persona de bien y porque siempre ha sido un gran ejemplo a seguir. Sandra Baechli, por luchar junto a mí y por todos los consejos brindados. A ambos les agradezco por todas las enseñanzas que me brindaron y por el esfuerzo que realizaron para que hoy obtenga este triunfo. Gracias padres, por darme este gran regalo: mi carrera universitaria.

Mis hermanos Glen, Jim y Hans, por trazarme y enseñarme el camino a seguir. Por ser excelentes hermanos al apoyarme en todo momento y porque juntos hemos salido adelante.

Mi tía Rosa María Por ser como mi segunda madre, gracias tía por todos los sabios consejos.

Mi prima Hendy Por estar a mi lado y ser como mi gran hermana.

Mi asesor Ing. Christian Barneónd, por apoyarme con la realización de este trabajo de graduación.

Mis amigos Porque el apoyo que me brindaron en los buenos y malos momentos me ha servido para alcanzar este triunfo. Muy especialmente a Julio por su ayuda incondicional.

ACTO QUE DEDICO A:

Mis padres	Mario Jui Rivera y Sandra Baechli de Jui
Mis hermanos	Glen Robert, Jim Byron y Hans Gary.
Mi familia	Tía Rosa María, Hendy, cuñadas, sobrinos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ADN	Àcido DesoxirriboNucleico. Material genético de todos los organismos celulares y casi todos los virus.
AUTENTICACIÒN	Proceso que identifica a la persona.
AUTORIZACIÓN	Proceso que indica si se concede o deniega el acceso a la persona que se ha autenticado con anterioridad.
BIOMETRÍA	Disciplina que permite identificar y/o obtener rasgos de la persona basándose en sus características físicas y/o en sus pautas de comportamiento.
BIT	Acrónimo de *Binary Digit*. Dígito binario, es la unidad mínima de información empleada en informática.
BYTE	Unidad básica de almacenamiento de información, es equivalente a ocho bits.
CALÍGRAFO	Persona que se dedica a estudiar los rasgos de la escritura que son propios de cada persona.

CCD *Coupled Charging Device*. Dispositivo de Carga Acoplada, mediante un arreglo de fotodiodos toma una foto del símbolo de código de barras y la traduce a una señal.

CIRCUITO INTEGRADO Pastilla o chip en la que se encuentran todos o casi todos los componentes electrónicos necesarios para realizar alguna función.

CÓDIGO BIOLÓGICO Código único formado por patrones biológicos que reconoce las características individuales de la persona.

CÓDIGO DE BARRAS Arreglo en paralelo de barras y espacios que contienen información codificada.

COERCITIVIDAD Fuerza del campo magnético requerido para borrar una cinta codificada.

CRESTAS PAPILARES Relieves epidérmicos situados en la palma de las manos y en la planta de los pies.

DEMODULACIÒN Proceso que crea un código para la secuencia de textura en el iris.

DSV *Dinamic Signature Verification*. Es una verificación de las características dinámicas de la firma.

FAR	*False Acceptance Rate*. Tasa de falsa aceptación, es la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo.
FRR	*False Rejection Rate*. Tasa de falso rechazo, es la probabilidad de que el sistema de autenticación rechace a un usuario legítimo
HHLC	*Hand Held Laser Compatible*. Señal que genera un láser de pistola al leer un código de barras.
HUELLAS LATENTES	Huellas que permanecen en el sensor una vez utilizadas.
IRISCODE	Secuencia de descripción de los patrones del iris del ojo.
LECTOR	Dispositivo que identifica a la persona en el sistema por medio de la lectura de su identificación.
MINUCIAS	Ciertos arcos, bucles o remolinos de la huella digital.
NIP	Número de identificación personal. Sirven como identificadores únicos cuando las personas desean tener acceso a un área determinada.
OERSTED	Tipo de medida para la coercitividad de una cinta magnética.

PIXEL	Es la menor unidad en la que se descompone una imagen digital. Cada imagen es formada como una matriz rectangular de píxeles.
PLANTILLA	Información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación.
RFID	*Radio Frequency Identification*. Identificación por radio frecuencia, es la tecnología de proximidad que es un método de identificación automática sin contacto.
SCA	Sistema de Control de Acceso. Consiste en automatizar el control para limitar el acceso a las instalaciones de la organización.
SENSOR	Dispositivo que detecta, o sensa manifestaciones de cualidades o fenómenos físicos, como la energía, velocidad, aceleración, tamaño, cantidad, etc.
SURCO INTRAPAPILAR	Utilizado para la determinación de la huella digital, son los que se determinan por las depresiones que separan los relieves o crestas.
TÉCNICA MULTIMODAL	Combinación de diferentes métodos biométricos para aumentar el nivel de seguridad.

WNR *Wide to Narrow Ratio*. Utilizada en código de barras, es la razón del grosor del elemento más angosto contra el más ancho.

RESUMEN

La seguridad de control de accesos es de vital importancia para una organización, con el objetivo de restringir áreas, establecer un control y limitar el acceso a las instalaciones de la organización, lo que repercute en un entorno más seguro, al prevenir fraudes, daños y pérdidas.

Este trabajo consta de tres capítulos, los cuales se describen a continuación:

En el capítulo 1 se explica el tipo de seguridad que una organización puede lograr al disponer de un SCA, para ello, se plantean las necesidades de implantar un SCA, se describen las características, objetivos y auditorías que se pueden obtener al contar con un SCA. Además, se detallan las etapas a seguir para diseñar un plan de seguridad, de acuerdo a la cantidad de seguridad que se desee, tomando en cuenta los recursos de la organización.

En el capítulo 2 se identifican las diferentes tecnologías de SCA, las cuales son los sistemas basados en conocimiento, en posesión y biométricos. Para cada uno de ellos, se describe el proceso que siguen, abarcando desde la captura de datos hasta la concesión o denegación del acceso.

Un factor primordial para la implantación del SCA, es la elección del tipo de tecnología a utilizar.

En el capítulo 3, se analizan los factores que se deben de tomar en cuenta al momento de realizar la elección y se realizan cuadros comparativos de los diferentes tipos de SCA con el objetivo de que una organización pueda realizar su selección en base a sus necesidades.

OBJETIVOS

- **General**

Efectuar una comparación entre las diferentes tecnologías de control de acceso, estableciendo factores para identificar la tecnología que represente la mejor opción para las organizaciones.

- **Específicos**

1. Describir los conceptos importantes de un sistema de control de accesos, identificando las características, los objetivos y las auditorías que presenta el SCA.

2. Detallar las etapas para diseñar un plan de seguridad de control de acceso.

3. Dar a conocer los diferentes medios de identificación de personas.

4. Definir los factores para evaluar las diferentes tecnologías de control de acceso.

INTRODUCCIÓN

En la actualidad, para una organización es una necesidad y es de vital importancia tener un control de seguridad respecto a las personas que ingresan a sus instalaciones, es por ello que, los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados. Cada organización debe analizar sus necesidades específicas y determinar el nivel de seguridad que desean, es por ello que, es necesario crear un plan de seguridad, el cual debe ser cuidadosamente diseñado, revisado y actualizado constantemente.

Para seguridad de una organización, es importante que las instalaciones sean accedidas únicamente por personas autorizadas, adquiriendo un Sistema de Control de Accesos (SCA) en el cual se tiene un control de accesos de personal y de visitas a las instalaciones, con el objetivo de mantener una serie de auditorías de los accesos efectuados por las distintas personas en las diferentes instalaciones, utilizando esta información para obtener estadísticas para la organización. Con dichas estadísticas se pueden obtener muchos beneficios para una organización, ya que, esta información se puede obtener al instante con el objetivo de realizar análisis de diferentes tipos.

Para un SCA, es necesario contar con un proceso de identificación de las personas, el cual sea único y seguro.

Existen diferentes medios de identificación, los cuales funcionan de manera diferente y poseen ventajas y desventajas, sin embargo, dependiendo del tipo de organización, del nivel de seguridad que se requiera y de los recursos económicos con los que se cuenten, la organización debe decidirse por el medio de identificación que le satisfaga sus expectativas.

1. SEGURIDAD DE SISTEMAS DE CONTROL DE ACCESO

1.1. Seguridad Integral en una organización

La seguridad integral consiste en garantizar que únicamente tengan acceso a las áreas de una empresa, las personas que se ha planificado que puedan tener dicho acceso, con el objetivo del aseguramiento de los recursos de una organización. Esto conlleva la implementación de un sistema de control de seguridad, así como los recursos y las estrategias para conseguirla.

Dentro de una organización, es de vital importancia mantener la filosofía de seguridad integral, para minimizar los actos criminales y accidentales.

1.1.1. Objetivos de la seguridad integral

Con respecto a la seguridad integral, existen cuatro principales objetivos:

- Control de accesos: Consiste en canalizar, controlar o limitar el acceso a las instalaciones de la organización.

- Visibilidad reforzada: Es necesario realizar los cambios necesarios para garantizar que desde el puesto de control se tenga la máxima visibilidad posible sobre los accesos, empleados y áreas sujetas y susceptibles de control. Las oportunidades para la comisión de delitos o actos criminales se reducen considerablemente si los empleados y visitantes están siempre bajo observación.

Zonas acristaladas como división y/o cerramientos de las oficinas de los supervisores y las áreas de trabajo u oficinas de los subordinados evita, limita o coapta la realización de fraude, malversación o abuso de confianza.

La meta del diseño de la visibilidad reforzada tiene que ser poder observar los movimientos de las personas y los medios en todas las direcciones.

- Reforzamiento estructural: Reforzar aquellas zonas de máximo riesgo o de mayor interés. Debe el diseño del sistema crear las barreras necesarias para detener, detectar o aprender la comisión de algún acto criminal o accidental. El objetivo del reforzamiento estructural es dificultar y retardar la comisión de potenciales actos delictivos e ilegales y disuadir su realización.

  El reforzamiento estructural debe estar sistemáticamente integrado con los sistemas de alarma y detección. Este tipo de reforzamiento es apropiado en aquellas áreas o zonas en las que haya material susceptible o atractivo para el delincuente.

- Impacto Psicológico: Este cuarto objetivo nos lleva al mensaje psicológico o impacto que debe estar presente. Los usuarios del edificio e instalaciones conocen que las medidas de control y seguridad instaladas constituyen un impacto psicológico que favorece a la seguridad general.

1.2. Sistemas de Control de Acceso

Realizar control de acceso significa seleccionar o filtrar a las personas que pueden acceder a determinadas áreas, permitiendo de manera dinámica y efectiva controlar al personal y activos con el propósito de minimizar las pérdidas, aclarar fraudes, prevenir la fuga de información en las empresas, hacer eficiente el desempeño del personal y brindar un entorno más seguro.

1.2.1. Necesidad de implantar un SCA

Debido a que es necesario poseer un alto nivel de seguridad, en muchas organizaciones, las cerraduras y llaves han quedado anticuadas, implantando en su lugar un sistema de control de acceso. La necesidad de implantar un control de accesos electrónico, es debido a:

- Las llaves estándar son muy fáciles de copiar.
- Cada persona puede necesitar varias llaves.
- Se necesita que solamente ciertas personas puedan tener acceso a determinadas áreas de la empresa.
- La pérdida o robos representan un mayor riesgo de seguridad y requiere de mucho tiempo y dinero para solventarlo.
- No se posee un control estricto de las personas que accedan a determinado sector.

Al tener un SCA, se proporciona seguridad añadida imponiendo reglas de horarios, activando una alarma en caso de intento de acceso no autorizado y almacenando todos los movimientos de acceso, entradas y salidas, con el objetivo de analizar los eventos más adelante, en caso de haber detectado una fractura en la seguridad.

Es importante que los SCA, sean de fácil uso para las personas, ya que si el sistema es complejo de utilizar, complica el trabajo de las personas, lo cual puede tener una relevancia significativa.

1.2.2. Características de los SCA

Una tecnología de control de accesos, brinda las siguientes características:

- Autenticación (¿Quién soy?): La autenticación es un proceso que identifica a la persona. Cada persona posee un único medio de identificación, que será el que se usa para acceder a todos los lugares que este habilitado. Al pasarlo por la unidad lectora correspondiente y/o digitar su clave de identificación, se verifica que dicha persona esté habilitada para el ingreso y permite el acceso, registrando a la vez en su memoria interna la fecha y hora del evento.

- Autorización (¿Qué puedo hacer?): La autorización indica a qué lugares o instalaciones puede acceder la persona. La habilitación o no de cada una de las personas, se realiza por el supervisor, pudiendo realizar altas y/o bajas en forma independiente para cada una de ellas, aún sin disponer de su medio de Identificación.

- Registro de auditoría (¿Qué he hecho?): Con el SCA, se lleva un registro de auditoría de los accesos que ha efectuado cada persona, llevando control de tiempos de entrada y de salida. Además, un buen sistema de control de acceso debe registrar los intentos fallidos de autenticación que se han realizado.

1.2.3. Objetivos de los SCA

Dentro de los objetivos que tiene un sistema de control de acceso, podemos mencionar:

- Generación de identificación única para cada empleado: Es importante encontrar una forma de identificar a cada empleado para permitir o negar el acceso a las áreas de una organización.

- Control del ingreso y egreso a las áreas restringidas o de riesgo en forma segura y efectiva: Con este control, la organización logra mantener aisladas las diferentes áreas de la empresa, llevando un registro de todos los movimientos de ingresos y egresos realizados a cada uno de los sectores controlados.

- Control de Personal: Lleva un registro actual de los accesos que realizan todos los empleados. El control de personal tiene la capacidad de especificar las áreas a las que tienen acceso y el horario en las que acceden.

- Creación de permisos de acceso temporales: Estos permisos pueden ser para visitantes o para empleados que requieren acceder de forma extraordinaria a un área a la cual normalmente no tienen acceso.

- Generación de auditorías de entrada y salida a las instalaciones: Con los SCA, se llevan estadísticas de los accesos, obteniendo un procedimiento de vigilancia de entrada y salida a las instalaciones, teniendo información sobre la persona que intenta acceder a la instalación, la notificación de rechazo o aceptación de acceso, la hora de entrada y la hora de salida. Esta información es de enorme ayuda ya que permite administrar eficientemente al personal y diagnosticar problemas fácilmente.

- Localización de las personas de la organización: Con un SCA se puede fácilmente conocer el lugar en donde se encuentran las personas en cualquier momento.

- Integración con otros sistemas de seguridad: Con los SCA, se disminuye la necesidad de tener servicio de vigilancia. Sin embargo, si la organización desea aumentar la seguridad del lugar y tener un mayor control, se puede integrar cualquier sistema de seguridad con un SCA, por ejemplo: activar una sirena o alarma externa, que indique si existiera violación de puerta o vandalismo.

1.2.4. Auditorías que presenta un SCA

El SCA es de gran utilidad para controlar la seguridad de las diferentes áreas en una organización, debido a que el sistema es capaz de manejar automática y eficientemente las entradas y salidas que las personas de las organizaciones realizan. Un SCA presenta las siguientes auditorías:

- Horarios de entradas y salidas a la planta.

- Permanencia en áreas permitidas: Una vez accedida una "puerta" se lleva control del horario de entrada y salida a esa área, el cual permite conocer quiénes y a qué hora estuvieron en una área determinada, y en el caso del acceso(s) principal(es), a qué hora cada empleado ingresa y sale de la empresa.

- Intentos de ingreso a áreas restringidas: Si un empleado intenta acceder a una de estas "áreas restringidas" no sólo le es negado el acceso, sino que también se guarda un registro de quién y a qué hora intentó acceder una puerta a la que no tenía permiso entrar. Lo que permite tomar las precauciones necesarias para prevenir situaciones no deseadas que pone en peligro la integridad de los empleados y/o de la empresa.

- Permisos temporales y/o especiales para acceder a áreas restringidas: Con esto se pueden obtener auditorías sobre las personas que visitan a la organización. Además, se pueden evaluar los permisos especiales que se dieron a cada empleado.

- Generación de registros históricos de entradas y salidas para agilizar el procesamiento de una nómina: Con el SCA, el cálculo de la nómina es más ágil y toma un carácter más real ya que cuenta con un registro exacto y en línea de la hora en que cada empleado accede a la planta, además, genera un registro diario que el sistema de nómina de una empresa utiliza como parte del procesamiento de su cálculo.

Con las auditorías, se mejora notablemente el trabajo del departamento de Recursos Humanos al brindar información sumamente detallada acerca del desempeño de los empleados; por ejemplo, estadísticas de ausentismo, de llegadas tarde, de salidas tempranas, comparativos de horas reales vrs horas esperadas, etc.

Es importante notar que las auditorías, ayudan a determinar quién esta en un lugar donde haya ocurrido alguna anomalía, logrando de esta manera diagnosticar problemas de robos, faltantes de mercadería, roturas, movimiento de personal, etc.

1.2.5. Diseño de un plan de seguridad para un SCA

Normalmente el acceso al edificio o instalaciones, está restringido a personas y medios propios del lugar o vinculados al mismo. El diseño de un SCA es complicado pues los empleados y visitantes se sienten con el legítimo derecho de entrar o acceder a todas las áreas, en especial en las horas de trabajo o producción. El control de acceso en esas horas (las de trabajo o producción) es complicado además por la gran diversidad de visitantes, transportistas, empresas de suministros y empleados que están interactuando y que hay que controlar.

Cuando una persona desea acceder a determinada instalación, y esta cuenta con un control de accesos, se puede producir una autorización positiva o negativa. La existencia de una autorización positiva indica que se puede realizar el acceso, mientras que la existencia de una autorización negativa indica que el acceso ha sido denegado. El proceso de diseño consta de las siguientes etapas:

- Reconocimiento de áreas: consiste en identificar las diferentes áreas en las que se debe tener seguridad.

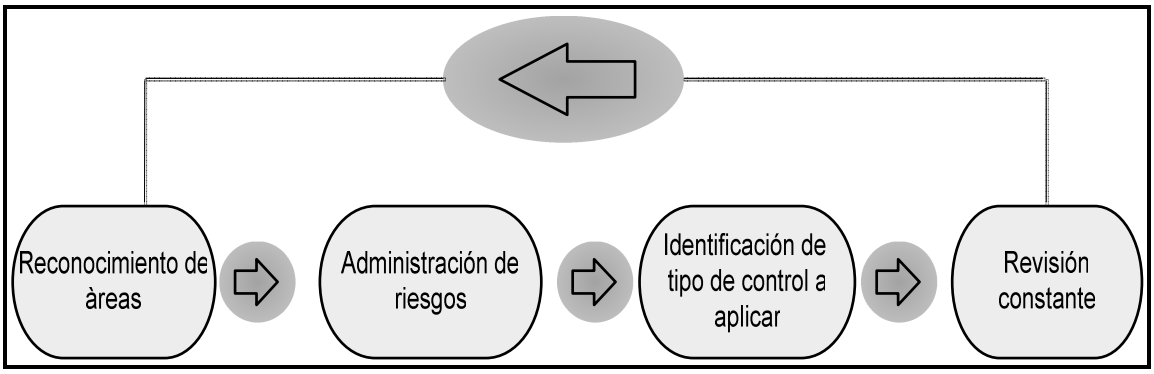
- Administración de riesgos: Consiste en anticipar los riesgos que podrían afectar la seguridad de la organización.

- Identificación del tipo de control a aplicar: Consiste en definir el tipo de seguridad que se va a colocar en cada área reconocida.

- Revisión constante: Consiste en verificar si el sistema de seguridad cumple con las expectativas de la organización.

- cumple con las expectativas de la organización.

Figura 1. Etapas del proceso de diseño



1.2.5.1. Reconocimiento de áreas

Una organización, se compone de varias instalaciones y es importante que el acceso a ellas sea limitado al menor número de personas posible. Sin embargo, es necesario proporcionar a las personas los accesos a las instalaciones necesarias, para que puedan cumplir eficientemente con su trabajo.

Los procedimientos de acceso lógico y físico son suficientes, incluyendo perfiles de seguridad de acceso para empleados, proveedores, equipo y personal de mantenimiento de las instalaciones.

Es necesario que la empresa, tenga un inventario de las instalaciones y que se definan los accesos de cada empleado a cada instalación, así como de las visitas. Para ello se deben tener mecanismos de entrada y de salida y establecer procedimientos de vigilancia.

Las políticas de acceso y autorización de entrada/salida, escolta, registro, pases temporales requeridos, cámaras de vigilancia son apropiadas para todas las áreas y especialmente para las áreas más sensibles.

1.2.5.2. Administración de los riesgos

La seguridad total es algo a lo que las organizaciones aspiran. Para ello, es necesario evaluar si la seguridad es apropiada a los riesgos, lo cual involucra a situarse sobre el límite del presupuesto. Los mejores sistemas son aquellos que reducen el riesgo inmediatamente después de su implantación, además de que permiten ampliaciones no redundantes cuando se necesite crecer.

El crecimiento se puede dar de varias formas: Las instalaciones físicas se vuelven más grandes, se tiene la necesidad de colocar más puertas, se incrementa el personal de una organización o simplemente para la empresa es indispensable poseer una mayor seguridad.

De esta manera valorar riesgos para cada área reconocida, involucra evaluar los riesgos, identificando donde están los riegos más altos y establecer como los riesgos pueden ser reducidos en cada área. El riesgo más alto es donde hay una combinación de los siguientes factores: Una puerta abierta, y acerca de las personas que no pueden pasar por ambos lados de la puerta que conduce hacia un área con algunas cosas de valor.

El proceso de administración de riesgos comprende varias etapas:

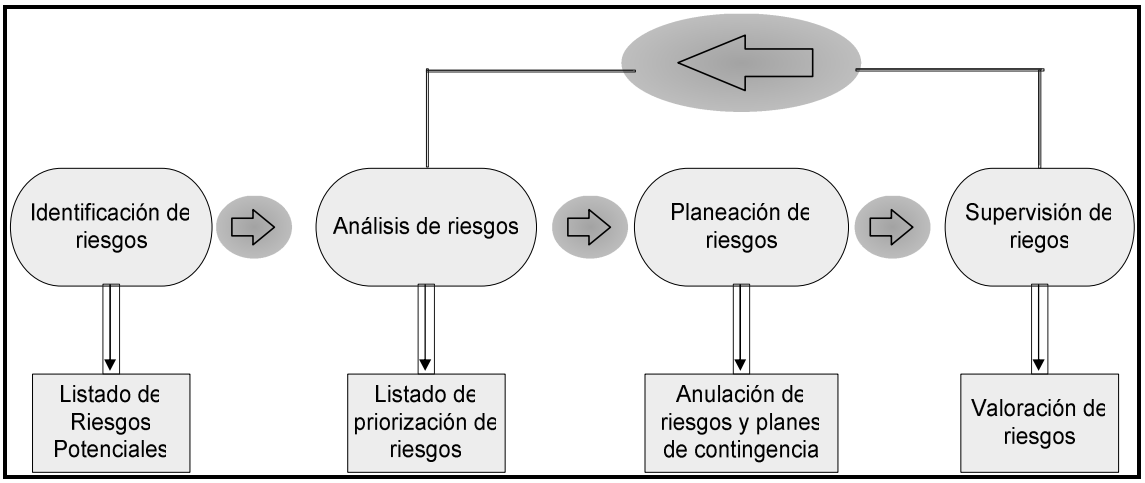
- Identificación de riesgos: consiste en identificar los posibles riesgos de seguridad que existen para cada área reconocida.

- Análisis de riesgos: Valorar las probabilidades y consecuencias de los riesgos identificados.

- Planeación de riesgos: Crear planes para abordar los riesgos, ya sea para evitarlos o minimizar los efectos.

- Supervisión de riesgos: Valorar los riesgos de forma constante y revisar los planes para la mitigación de riesgos tan pronto como la información de los riesgos esté disponible.

Figura 2. Etapas de la administración de riesgos



1.2.5.2.1. Identificación de los riesgos

Esta es la primera etapa de la administración de los riesgos. Comprende en el descubrimiento de los posibles riesgos del proyecto. Es necesario que en esta etapa no valoren o prioricen los riesgos identificados.

Para llevar a cabo la identificación de los riesgos se puede realizar un proceso de grupo utilizando un enfoque de lluvia de ideas o simplemente se pueden basar en la experiencia del administrador de la seguridad.

1.2.5.2.2. Análisis de riesgos

Durante este proceso, se considera por separado cada riesgo identificado y se decide acerca de la probabilidad y la seriedad del mismo.

La valoración de los riesgos puede realizarse en intervalos. La probabilidad de que el riesgo se valore como muy bajo (<10%), bajo (10-25%), moderado (50-75%) o muy alto (>75%).

Los efectos del riesgo pueden ser valorados como: catastrófico, serio, tolerable o insignificante.

El resultado de este proceso de análisis se debe de colocar en una tabla, la cual debe de ordenarse de acuerdo a la seriedad del riesgo. Una vez que los riesgos se hayan analizado y clasificado, se deben discernir cuáles son los más importantes que se deben de considerar. Este discernimiento depende de una combinación de la probabilidad del riesgo en cuestión y los efectos del mismo.

1.2.5.2.3. Planeación de riesgos

En esta etapa se consideran cada uno de los riesgos identificados y las estrategias para administrarlos. Estas estrategias se encuentran dentro de tres categorías:

- Estrategias de anulación: Estas estrategias consisten en reducir la probabilidad de que el riesgo surja.

- Estrategias de disminución: Estas estrategias consisten en reducir el impacto del riesgo.

- Planes de contingencia: Estas estrategias significa que, si sucede lo peor, se está preparado para ello y se cuenta con una estrategia para abordarlo.

1.2.5.2.4. Supervisión de riesgos

En esta etapa se valora cada uno de los riesgos identificados para decidir si éste es más o menos probable y cuando los efectos del mismo han cambiado.

La supervisión de riesgos es un proceso continuo y, en cada revisión, se debe de considerar cada uno de los riesgos por separado.

1.2.5.3. Identificación del tipo de control a aplicar

Luego de reconocer las áreas y de realizar todo el proceso de administración de riesgos, se debe establecer la cantidad de control que se debe de aplicar, para dos tipos de grupos:

- Proveedores, personal de mantenimiento, visitas: La organización debe de tener cuidado con las personas que no pertenecen a la organización, que intencionada o no intencionadamente pueden acceder a las instalaciones con algún objetivo en específico. Para ello, es importante establecer la cantidad de control a aplicar en cada área definida, identificando las áreas en donde las visitas puedan tener acceso sin ocasionar daño alguno, o definir áreas, en donde es necesario que las visitas tengan acceso pero con supervisión, disminuyendo la posibilidad que obtengan información confidencial de la organización.

- Personal: Se debe establecer la cantidad de control que se le va a proporcionar al personal, dependiendo del puesto organizacional del empleado. En el caso de que un empleado ya no pertenezca a la organización, es necesario quitarle los derechos de acceso que poseía.

La siguiente tabla presenta las características de los controles, las funciones y los lugares en los que benefician.

Tabla I. Tipos de Control

Tipo de Control	Como Funciona	Donde le Beneficia
Niveles de Acceso	Cada persona puede solamente pasar por ciertas puertas.	Cuando algunas áreas de la organización deben tener una mayor protección que otras.
Zonas Horarias	Cada persona puede solamente pasar por ciertas puertas a ciertas horas.	Cuando existen horas del día o días de la semana, en las que se les restringen el acceso a determinadas personas.
Medio de Identificación + NIP	Después de que una persona utilice su medio de identificación deberá introducir su NIP para que la puerta se abra.	Se debe utilizar, cuando existen riesgos de pérdidas o robos de los medios de identificación.
Anti pass-back	Después que se ha accedido a un área, no se puede volver a utilizar la misma identificación hasta pasado un tiempo ("anti pass-back por tiempo") o hasta que esa identificación sea utilizada para salir del área.	Cuando hay riesgo que una persona que entre en un área, ceda su medio de identificación a otra persona que esté fuera.
Esclusa	Una puerta no se puede abrir hasta que la otra puerta esté cerrada.	Cuando se quiera limitar, que únicamente pueda acceder una persona a la vez a un determinado pasillo.
Alarmas	Se notifica al supervisor, cualquier evento que sea "inesperado" o que tenga "comportamiento anormal".	Puede beneficiar en diferentes casos, por ejemplo, si una puerta es dejada abierta demasiado tiempo, o una persona intenta acceder cuando no está autorizado.
Monitorización-Puntos	Existen entradas "Libres" en los sistemas de control de accesos que se pueden visualizar.	En las salidas de emergencias, se puede autorizar a las personas a no utilizar el sistema de control de accesos.

Debido a que el plan de seguridad contempla áreas de seguridad, las cuales representan los diferentes niveles y variaciones de restricción y control de acceso, desde las zonas de acceso no restringido hasta las zonas de acceso prohibido. La precisión y determinación del nivel de control requerido es labor conjunta con el equipo de diseño y los futuros/actuales usuarios y gestores del edificio e instalaciones.

Las áreas deben agruparse por el nivel de control exigido, mediante la creación de secciones dentro del edificio o instalaciones o bien separando físicamente, de ser posible, las sección o áreas en función de su nivel de control exigible. Por ejemplo, es común colocar aquellas dependencias o áreas no restringidas o de libre acceso - que no demanda control de acceso o requieren un mínimo de control - y de gran volumen de visitantes lo más cerca de la entrada o lobby del edificio. El acceso a estas áreas no puede implicar el paso por zonas de mayor nivel o exigencia de seguridad.

Diseñando en base a zonas, se aumenta la efectividad y reduce los costes de sistemas de control de acceso y de detección. Las áreas de producción deben estar debidamente sectorizadas, pues los empleados deben ser sometidos a pocas interrupciones y distracciones durante sus movimientos en el trabajo.

1.2.5.4. Revisión constante

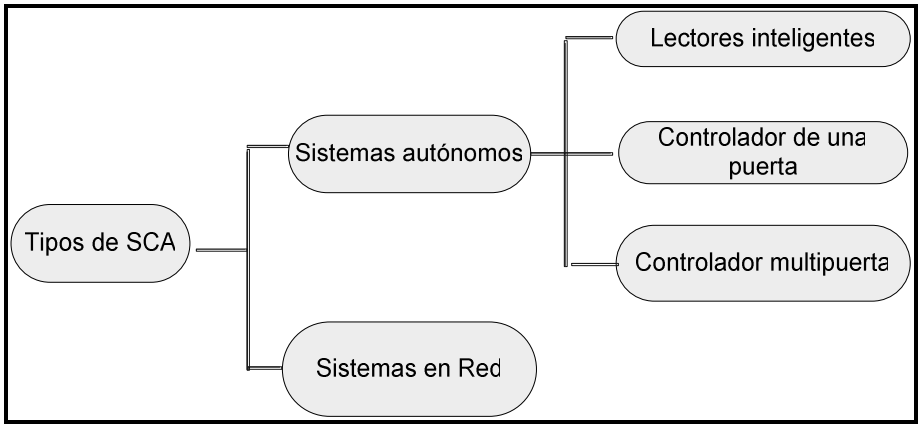
Las actividades del plan de seguridad requieren revisiones y actualizaciones periódicas. Estos cambios se realizan cuando las configuraciones y otras condiciones y circunstancias cambian considerablemente o cuando hay que modificar las leyes y normas organizativas. Éste es un proceso iterativo, nunca termina y debe revisarse y probarse con periodicidad.

Para efectuar las revisiones constantes, es necesario que la organización efectúe un desarrollo, mantenimiento y revisiones continuas de políticas y procedimientos de seguridad, efectuando revisiones de los perfiles de acceso. Además, se deben establecer medidas a aplicar, en caso de violaciones a la seguridad.

1.2.6. Tipos de SCA.

Los tipos de SCA se pueden observar en la siguiente figura.

Figura 3. Tipos de SCA



1.2.6.1. Sistemas autónomos

Son aquellos sistemas que no necesitan de ordenador y software, dentro de esta categoría se encuentran los lectores inteligentes, los controladores de una puerta y los controladores multipuerta.

1.2.6.1.1. Lectores inteligentes

Es el nivel más simple, los lectores inteligentes son una combinación de lector/ controlador que facilita un apropiado paquete todo en uno, que puede ser instalado rápidamente para un sistema de control de accesos para una puerta. Puede instalar más de uno si tiene más de una puerta, pero cada vez que se necesite añadir o eliminar tarjetas de usuarios, se tendrá que desplazarse a cada una de sus ubicaciones.

Hay un riesgo de seguridad con estos productos, este riesgo es que la electrónica controladora está sobre el lado más inseguro de la puerta, y por lo tanto puede ser saboteado. Es necesario que se consideren las necesidades de la organización, y si es muy alta la probabilidad de sabotaje, entonces se debe de utilizar un tipo diferente de sistema.

1.2.6.1.2. Controlador de una puerta

Estos controladores consiste en que cuando se proteja una puerta, se debe instalar el controlador en la parte segura de la puerta para asegurarse de las situaciones de alto riesgo. No importa que el lector sea saboteado, la puerta no se abrirá.

1.2.6.1.3. Controlador multipuerta

Para situaciones de múltiples puertas, hay controladores que pueden controlar varias puertas cada uno. Esto puede representar un ahorro, puesto que hay un solo controlador y también puede ser más conveniente porque puede programar las tarjetas en las múltiples puertas con una simple acción. Sin embargo, dependiendo de la distancia de los cableados, la viabilidad y los costos de los cables entre las puertas pueden ser mayores a los beneficios esperados.

1.2.6.2. Sistemas en red

Las empresas pueden requerir controlar el acceso en más de una puerta. Si bien esto se puede solucionar con múltiples unidades aisladas, un sistema en red tiene muchas ventajas, siendo la más obvia la supervisión centralizada. Las actividades de rutina y las condiciones de alarma se reportan a la PC central, donde se pueden organizar y presentar en manera de reportes.

Los sistemas en red son aquellos que están enlazados con un ordenador y un software. Estos sistemas proporcionan lo último en comodidad y flexibilidad y son altamente competitivos, tanto en funcionamiento como en precios. Los sistemas modernos son intuitivos y amigables y requieren un mínimo entrenamiento para los administradores.

Los sistemas en red también permiten el "manejo de plantillas", donde todos los usuarios se enrolan en un mismo lector, el cual automáticamente transfiere todas las plantillas a las otras unidades en la red. Luego las plantillas se pueden eliminar o editar en la PC central.

Algunos de estos sistemas almacenan toda la información en la PC, que es también donde se realiza la comparación. Otros sistemas operan sin una PC central, distribuyendo todos los datos de las plantillas a cada lector. En ambos casos el efecto del manejo de plantillas es el mismo.

Las razones por las que los sistemas en red son utilizados se describen a continuación:

- Al utilizar sistemas autónomos, es necesario instalar más de uno para asegurar el número de puertas necesarias, además de efectuar operaciones de programación en múltiples ubicaciones.

- Existe más de una simple combinación de derechos de acceso, por ejemplo, la complejidad es elevada al programar 16 puertas en un sistema autónomo, donde cada persona tiene diferentes permisos por cada puerta.

- Es más fácil y conveniente utilizar múltiples estaciones de trabajo para administrar diferentes aspectos del sistema.

- Con los sistemas en red se puede controlar y monitorizar un área remota.

1.2.6.3. Ventajas y desventajas de los tipos de SCA.

En la siguiente tabla se muestran las ventajas y desventajas.

Tabla II. Ventajas y desventajas de los tipos de SCA

Tipo de sistema	Ventajas	Desventajas
Lectores Inteligentes	Bajo costo. Fácil Instalación.	Sistema sobre el lado inseguro de la puerta y puede ser saboteado para un acceso no autorizado.
Controlador de una puerta	Mayor seguridad que los lectores inteligentes en ubicaciones vulnerables.	Si el control es a más de una puerta, las tarjetas tienen que ser programadas en cada lector.
Controlador Multi Puerta	Con un simple punto de programación tiene capacidad de controlarlo (2-16 puertas).	Sofisticadas características pueden completar la configuración.
Sistemas Red	Programación y monitorización central independiente al número de puertas. Interfase de usuario mucho más intuitivo y flexible. Múltiples estaciones de trabajo pueden ser administradas por el sistema. Sofisticados filtros de listados, administración de alarmas e interfases con otros sistemas.	El precio es mayor que los demás sistemas. Una falla en el ordenador ocasiona fallas en el sistema.

1.2.7. Funcionamiento del SCA

Una vez que se instala el SCA, es necesario dar de alta a todos los empleados de la empresa, se especifican las puertas de las áreas a las que tienen permiso de acceder así como el horario y las fechas de acceso. Conforme se dan de alta los empleados, se genera el medio de identificación para el empleado.

Cada empleado intenta acceder a las puertas de la empresa, utilizando el medio de identificación, para que el sistema permita o no el acceso por dicha puerta. Una vez que el permiso es negado o concedido se guarda un registro de la hora en la que se intenta acceder dicha puerta y si se logro o no accederla.

El supervisor del SCA, puede efectuar las siguientes acciones en cualquier momento:

- Dar de alta nuevos empleados con sus respectivos permisos y derechos: El SCA es una herramienta que registra nuevos empleados, genera los accesos que tienen y realiza las especificaciones del momento en que dichos accesos tienen vigencia (especificación de horario).

- Dar de baja empleados: Cuando un empleado se va a ausentar temporal o permanentemente, es necesarios darlos de baja.

- Modificar los permisos y derechos que un empleado tiene.

- Cancelar permisos: Quitar permisos a los empleados a áreas a las cuales tenía acceso.

- Conceder nuevos permisos: Asignar permisos a los empleados a áreas que eran restringidas para él.

- Conceder permisos temporales: El SCA es un sistema es capaz de limitar el horario de estancia en algunas áreas especiales de la empresa, y crea permisos de accesos temporales a dichas áreas para empleados que sea necesario que las accedan de manera extraordinaria.

1.2.8. Componentes de un SCA.

- **Medio de identificación:** Es lo que una persona sabe o tiene con el propósito de identificarse.

- **Lectores:** Esto es lo que identifica a la persona en el sistema por medio de la lectura de su identificación y enviándola al concentrado. Algunos lectores están más protegidos que otros contra el vandalismo, se debe evaluar las necesidades para asegurarse estos riesgos. Si un lector es transgredido, puede resultar un acceso no autorizado.

- **Cerraduras:** La elección de la cerradura depende primero de la puerta (cerradura eléctricas, cerraduras magnéticas, torniquetes o barreras), para ello es necesario evaluar la arquitectura y la necesidad de robustez a los posibles ataques. Todos los tipos de cerradura tienen sus ventajas y las desventajas y están disponibles en una variedad de gamas y diseños.

- **Sensores de Puerta:** Proporciona un nivel extra de seguridad ya que si un sensor de puerta está instalado, entonces, tan pronto como la puerta abre, la cerradura es bloqueada y la puerta quedará cerrada de nuevo, evitando de esta manera que la puerta esté abierta después de que la persona acceso.

- **Pulsador:** Un pulsador de apertura permite a las personas pasar por una puerta, desde el área segura a una menos segura, sin el uso de un medio de identificación. Pulsar el botón ocasiona que la cerradura sea liberada, así como si un medio de identificación hubiera sido validado. Este componente es importante ya que en numerosas ocasiones es necesario que las personas salgan de un área sin depender de cualquier forma de sistemas eléctricos.

- **Sensores de puerta abierta:** Son sensores que se colocan en las puertas (uno en la puerta y otro en el marco) y detectan si la misma se encuentra abierta o cerrada. La señal de salida se conecta a cualquiera de los controladores que permanentemente están monitoreando esta entrada. Si detectan la apertura anormal o violación de una puerta, disparan una señal de alarma.

- **Controlador**: Los controladores, registran quién (nombre y datos vinculados), dónde (puerta), dirección (entrada o salida) y cuando se accedió (día y hora), cada controlador memoriza los eventos en forma independiente de la computadora. Los lectores pueden ir incorporados en el controlador o estar separados. Los lectores inteligentes son una combinación de lector/ controlador que puede ser instalado para un sistema de control de accesos para una puerta, y son muy inseguros. Los controladores separados proporcionan mayor seguridad y pueden gestionar una o varias puertas.

- **Cables:** Los cables son muy importantes para la conexión del SCA, ya que si la instalación no se realiza correctamente, se necesitará cablear nuevamente, lo cual repercute en un costo de hora-hombres. Las consideraciones con respecto a los cables son:

    - Los cables de lector tienen limitaciones debido a la degradación de señal sobre la distancia. Típicamente, 100 metros es el límite – pero puede ser menor dependiendo de la tecnología de lector, la especificación del controlador y también la cantidad de ruido eléctrico en la cercanía.

    - Para cables de comunicaciones y lector se requiere baja capacitancia.

    - Los cables de la cerradura tienen limitaciones debido a la reducción de voltaje.

    - Todos los cables deberían estar apantallados, todas las señales deben de llevar cables separados e independientes. Los requerimientos típicos por puerta son:

Tabla III. Requerimientos típicos de cable por puerta

Componente	No de Hilos
Lector	6 Hilos
Sensor	2 Hilos
Cerradura	2 Hilos
Pulsador	2 Hilos
Alarma Puerta abierta	2 Hilos

- **Programa:** El software proporciona un medio de programar y configurar las reglas para el sistema, normalmente esta información se envía a los controladores para que estos tomen las decisiones. Estas configuraciones se almacenan también en una base de datos sobre el ordenador para que se pueda ver lo que se ha programado y si un controlador se ha averiado o falla y tiene que ser reemplazado entonces podrá ser recargado con la información necesaria. El software registra todos los accesos y proporciona un sistema de auditoría, normalmente también monitorea el sistema, grabando los eventos y salvando la información al disco para que los informes puedan imprimirse.

2. IDENTIFICACIÓN PERSONAL

2.1. Modelo del proceso de identificación personal

Una parte importante de la seguridad concierne al asunto de la identificación personal en el acceso a los servicios, es decir: que en base a una total seguridad en la identificación del operador, pueda garantizarse que a la organización solo pueden acceder determinadas personas a determinadas áreas.

Todos los SCA trabajan con la base de la identificación de las personas, antes de decidir si permitir el acceso o denegarlo. Cualquier proceso de identificación personal debe tener un medio de identificar a la persona que desea obtener el acceso. Existen tres indicadores de identidad que definen el proceso de identificación:

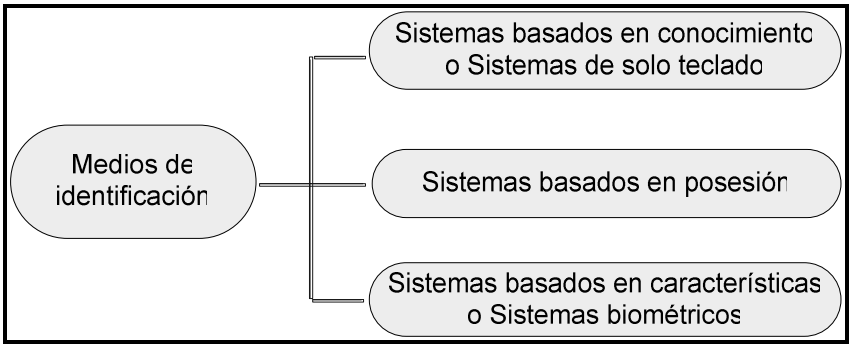
- Conocimiento: Es la identificación por medio de algo que se sabe, es decir, es por el conocimiento que tiene la persona, por ejemplo: una clave de acceso, un NIP.

- Posesión: Es la identificación por medio de algo que se tiene, es decir, la persona posee un objeto, por ejemplo: una tarjeta, una llave, etc.

- Característica: Es la identificación de una característica que tiene la persona, la cual puede ser verificada, estos sistemas son los biométricos, por ejemplo: una de sus huellas dactilares.

La siguiente figura muestra los medios de identificación:

Figura 4. División de los medios de identificación



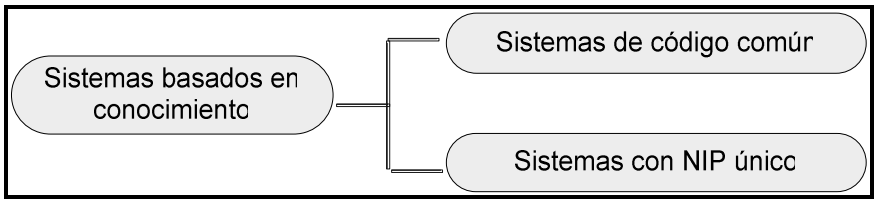
Cada uno de los indicadores anteriores genera una estrategia básica para el proceso de identificación personal. Además pueden ser combinados con el objeto de alcanzar grados de seguridad más elevados y brindar, de esta forma, diferentes niveles de protección. Distintas situaciones requerirán diferentes soluciones para la labor de identificación personal. Por ejemplo, con relación al grado de seguridad, se debe considerar el valor que está siendo protegido así como los diversos tipos de amenazas. También es importante considerar la reacción de los usuarios y el costo del proceso.

2.2. Sistema basados en Conocimiento

Estos sistemas también son conocidos como sistemas de solo teclado. Dentro de este tipo de sistemas, se encuentran dos categorías: los de código común y los que generan NIP únicos.

La siguiente figura muestra la división de los sistemas basados en conocimiento:

Figura 5. División de los sistemas basados en conocimiento



2.2.1. Sistema de código común

Los sistemas de código común son aquellos en que todas las personas tienen el mismo número. Obviamente esta opción es la más económica, pero la menos segura. Hace tiempo que han caído en desuso y no se han generado hasta el momento nuevas aplicaciones donde puedan resurgir como una opción válida.

2.2.2. Sistemas con NIP únicos

En los sistemas con NIP únicos, cada persona tiene un número diferente y estos al menos permiten borrarlos si estos llegan a ser comprometedores. Pero estos a pesar de todo, conllevan el riesgo de poder ser traspasados y poco a poco desconocer quien los está utilizando.

Los NIP sirven como identificadores únicos cuando las personas desean tener acceso a un área determinada. Para que este proceso sea efectivo, se debe tener cuidado en la forma en que se distribuyen y almacenan los NIP.

Los sistemas de distribución de NIP tienen que ser supervisados para asegurarse que sean distribuidos a las personas correctas. Distribuirlos por correo ordinario o electrónico plantea algunos riesgos, ya que puede ser difícil garantizar que la persona que lo recibe está facultada para hacerlo. Por otra parte puede ser difícil o poco práctico exigir que los NIP sean entregados de manera personal.

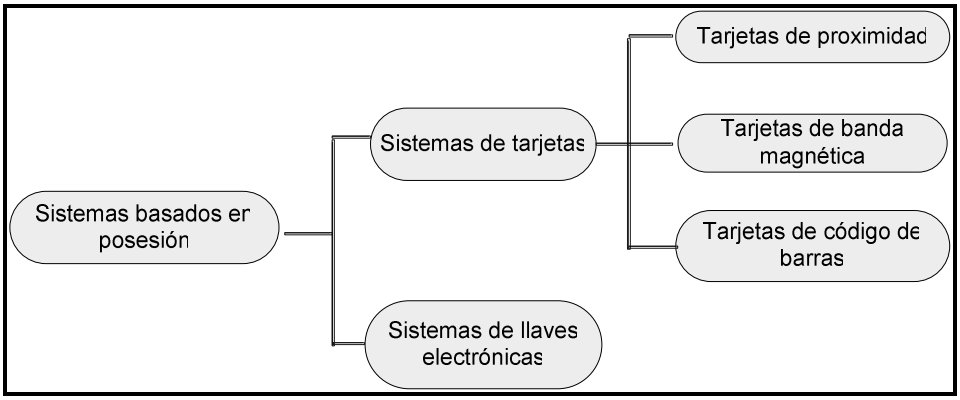
Un dispositivo que puede evitar el mal uso de los NIP es el de exigir una segunda identificación, como una tarjeta de identidad o una identificación biométrica, con esto nos percatamos de que cuando un NIP ha sido robado, no sea mal utilizado ya que el sistema al que está ligado va a exigir alguna otra prueba de identidad.

2.3. Sistemas basados en posesión

Dentro de este tipo de sistemas, se encuentran los sistemas de tarjetas y los sistemas de llaves electrónicas.

La siguiente figura muestra la división de los sistemas basados en posesión.

Figura 6. División de los sistemas basados en posesión



2.3.1. Sistemas de tarjetas

Estos sistemas son bastante populares, cada tarjeta es normalmente única y para evitar la preocupación acerca de las pérdidas de las tarjetas, se puede solicitar un número NIP de manera que la máquina lo haga efectivo.

Como las tarjetas son utilizadas para verificar la identidad de las personas durante eventos sensibles como las elecciones, la mayoría contienen rasgos orientados a minimizar la posibilidad de fraude. La inclusión de una fotografía, firma o huella digital sirve como un mecanismo visual de verificación de la identidad. Los dispositivos de seguridad impresos como los hologramas o diseños a color difíciles de reproducir pueden ser empleados para prevenir tarjetas falsificadas o alteradas.

La elección de la tecnología de tarjeta, puede parecer desconcertante al principio, pero cada tecnología tiene su configuración y características únicas y precios diferentes. Existen tarjetas que se deben insertar o deslizar o solamente presentar la tarjeta a distancia.

2.3.1.1. Cuidados de las tarjetas

Las tarjetas que tienen como limitación el contacto directo de un elemento lector, como lo es el cabezal de lectura magnética, hará que se genere desgaste en la tarjeta. Este se identifica con la aparición de rayas a lo largo de la banda magnética o el código de barras.

La duración de las tarjetas está relacionada con el uso que la persona pueda darle. Debe tenerse en cuenta las limitaciones propias de su tecnología, como:

- No doblar la tarjeta.
- No dejarla expuesta a los rayos ultravioleta o solares.
- No exponer a temperaturas por sobre los 35° C.
- No exponerla a elementos químicos como resinas y solventes.
- No aplastarla ni troquelarla.

Siguiendo las indicaciones antes mencionadas, la duración de la tarjeta sólo dependerá del cuidado del usuario y de la carga de trabajo que deba soportar diariamente.

2.3.1.2. Tecnologías de tarjetas

Cada tecnología tiene sus particularidades, lo cual hace que sea más adecuada para determinado ambiente o aplicación. Todos los productos para control de acceso y personal manejan cualquiera de las tecnologías que se describen a continuación para la identificación del individuo.

2.3.1.2.1. Tarjetas de proximidad

La tecnología de proximidad, llamada también identificación por radiofrecuencia (RFID) es un método de identificación automática sin contacto; es la tecnología más nueva y de más rápido crecimiento en el segmento de identificación automática en la industria. RFID permite identificación automática, localización y monitoreo de personas, objetos y animales en una infinidad de aplicaciones.

Estas tarjetas no tienen desgaste, ya que al ser una tecnología de identificación por radiofrecuencia (RFID), solamente hay que acercarla al lector y por lo tanto no existe el desgaste por rozamiento.

La tarjeta puede ser leída aún si la misma no es removida de la cartera ó billetera y a través de la mayoría de otros materiales no metálicos. La orientación de la tarjeta y del lector no es crítica y el contacto con monedas ó llaves no alterará su código, ni impedirá una lectura precisa y exacta.

Las tarjetas de proximidad no tienen partes móviles, ni contactos eléctricos que limpiar, ni uso ó desgaste mecánico, tampoco cabezas lectoras que mantener y es resistente a los actos de vandalismo, ya que desde el punto de vista de la seguridad, lo más importante es que no puede ser duplicada. Esto otorga a los sistemas de control de accesos implementados con esta tecnología un grado máximo de seguridad.

Hoy en día, las tarjetas de proximidad, es una de las tecnologías más moderna y efectiva, por su practicidad y bajo costo de mantenimiento. Tiene un costo medio, sin embargo su duración hace que resulte, la más económica, porque no requiere recambios por desgastes.

Existen dos tipos de tarjetas de proximidad: las tarjetas pasivas y las activas. Las tarjetas pasivas toman la energía generada por el lector para emitir su código, son más livianas, más económicas y más durables y tienen un alcance hasta 70cms. Las tarjetas activas tienen incorporada una batería de duración limitada y no recambiable, su ventaja radica en su rango de lectura el cual puede llegar a 1,5 m contra los 70cm. alcanzables hoy por las tarjetas pasivas. La siguiente figura muestra una tarjeta de proximidad.

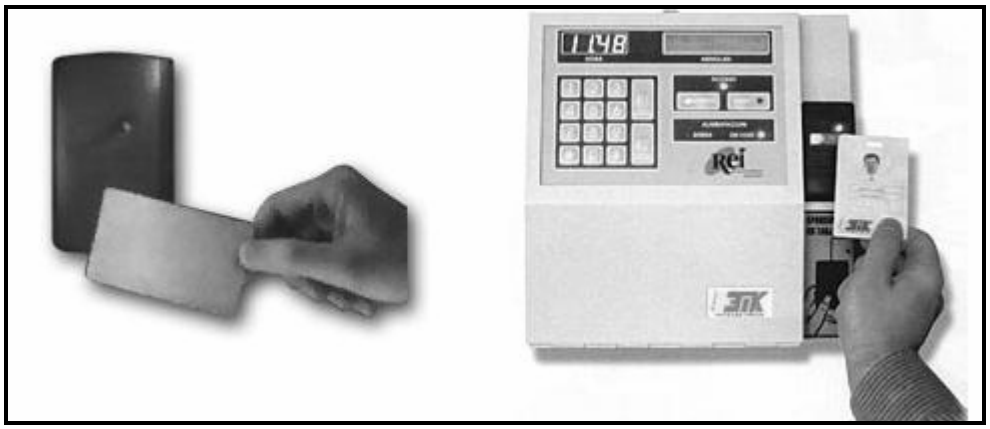
Figura 7. Tarjeta de proximidad

La tecnología RFID ha revolucionado la industria de la identificación automática ofreciendo avances significativos en comparación con sistemas tradicionales como código de barras y tarjetas de banda magnéticas. De la manera más simple, un sistema RFID integra un número de identificación único en un pequeño microchip, y éste va a ser colocado en el objeto a ser identificado. El microchip se activa sólo cuando hay una señal de radio en una frecuencia específica mandada por un lector o transmisor. Cuando el microchip es activado, inmediatamente responde mandando de regreso una señal de radio modificada que contiene el número de identificación de ese microchip. El lector o transmisor se desempeña como radio transmisor y radio receptor. Cuando el microchip responde a la señal y manda su número de identificación, el lector puede automáticamente mandar la señal a una computadora para su procesamiento. Este sistema tiene la ventaja sobre otros sistemas de identificación automática que no requiere línea de vista o contacto físico del lector con el microchip para ser leído.

Para la lectura de las tarjetas de proximidad, el lector de proximidad constantemente transmite una señal de radiofrecuencia fija de bajo nivel, la cual provee energía a la tarjeta de proximidad. Cuando la tarjeta es presentada a cierta distancia del lector, la señal de RF es absorbida por una pequeña bobina dentro de la tarjeta y energiza al chip de la tarjeta, el cual contiene un único código de identificación. Una vez energizada, la tarjeta transmite el código al lector. El proceso es completado en milisegundos.

Los beneficios de este tipo de tarjetas es la rapidez y exactitud ya que el microchip y el lector se comunican en milisegundos, además no necesita contacto, por lo que es posible colocar el microchip por debajo, sobre o cubierto por otro material. El RFID es extremadamente confiable en cuanto a su rango de error, que es de 1 en 2 millones, también es robusto y de bajo mantenimiento, ya que se puede leer a través de cualquier material no metálico y los componentes internos (microchip, antena, lectores) se pueden empacar de manera que pueden ser resistentes a todo tipo de ambiente.

Figura 8. Lectores de tarjetas de proximidad

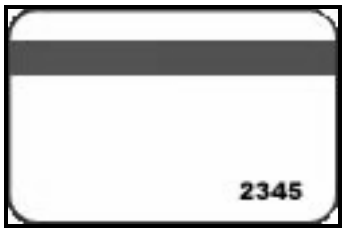


2.3.1.2.2. Tarjetas de banda magnética

Los medios de cinta magnética proporcionan un medio barato y flexible de mantener información que deba ser modificable. Una cinta magnética consiste de material magnético combinado con pintura o encuadernado; dicho material es sujeto a un campo magnético. Este campo alinea los polos magnéticos del material magnético, y lo hace adecuado para la lectura y la escritura. La cinta magnética puede ser laminada o estampada en cualquier superficie lisa, la información es leída o escrita de la cinta por un lector.

Las ventajas de las tarjetas de banda magnética son su difusión, popularidad y el bajo costo, pero en sí es, de todos los medios de identificación, el más vulnerable de todos. Su banda magnética, debe ser tratada con cierto cuidado, para evitar que se raye o sea expuesta a campos magnéticos que la borren, por tal motivo, no son recomendables para usar en ambientes industriales. Sólo se recomiendan en oficinas o establecimientos administrativos.

Figura 9. Tarjeta de banda magnética



Un lector consiste de una cabeza de grabación magnética, la cual puede leer y grabar información magnética en la cinta. La información en la tarjeta consiste de un código binario. Desde esta forma de datos de bajo nivel, un formato de datos de alto nivel es usado para convertir el código binario a caracteres alfanuméricos.

La cinta magnética y el lector se comunican vía un campo magnético. La lectura es llevada a cabo deslizando la tarjeta de banda magnética a través del lector (aunque de igual modo puede hacerse que la cabeza de grabación se mueva a lo largo de la tarjeta). El lector recoge los cambios en la polaridad en la cinta con la cabeza de grabación magnética. Para la escritura, el lector crea un campo magnético que alterará la polarización de una pequeña región de la cinta, y de este modo escribirá información en la cinta. El intercambio de datos entre la tarjeta y la unidad de lectura / grabación típicamente ocurre a velocidades de cerca de 12,000 bits por segundo.

El cabezal magnético del lector sufre cierto desgaste al pasar las tarjetas por el lector. En realidad cada tarjeta que se pasa, deja micropartículas depositadas sobre la cabeza lectora. Ahora bien, si esas partículas son abrasivas, comienzan a rayar las tarjetas sucesivas y las tarjetas rayadas o rotas, deterioran aun más el cabezal, obligando al recambio del lector y de las tarjetas dañadas. El tiempo de duración, depende exclusivamente del ambiente, frecuencia de uso y el trato con el que se los utilice, pero el promedio está entre 9 meses y 3 años.

La cinta magnética es susceptible a alteración o borrado causada por otros campos magnéticos; de igual modo es susceptible a daño físico y a daño causado por el medio ambiente. La necesidad de prevenir el daño a la información mantenida en la cinta como resultado de un contacto inadvertido con campos magnéticos que pueden ser encontrados en el uso diario de una tarjeta ha llevado a muchos fabricantes, integradores e ingenieros a desarrollar tarjetas con propiedades magnéticas más resistentes. La resistencia de una cinta magnética es típicamente discutida en términos de coercitividad (medida en oersteds), la cual es definida como la fuerza del campo magnético requerido para borrar una cinta codificada. Generalmente, las tarjetas de baja coercitividad [300 oersteds] son más fácilmente cambiadas o codificadas que las tarjetas de alta coercitividad [3000 oersteds]. Existen limitaciones para manejar niveles útiles de coercitividad, de cualquier modo, dado que cintas con una coercitividad de entre 3,000 y 5,000 oersteds pueden ser difíciles de leer, grabar o modificar.

El mejor ambiente para las tarjetas de banda magnética es un área limpia, seca y fría. Las temperaturas típicas de almacenamiento son entre -40 y 80 °C. Las temperaturas típicas de operación son entre 0 y 55 °C.

El control de accesos, tiempo y asistencia son aplicaciones en las que la versatilidad y el bajo costo de la cinta magnética son un gran beneficio. La cinta magnética es lo suficientemente versátil como para desempeñar estas funciones.

Figura 10. Lector de tarjetas de banda magnética

2.3.1.2.3. Tarjetas de código de barras

El código de barras es un arreglo en paralelo de barras y espacios que contienen información codificada. Esta información puede ser leída por dispositivos ópticos, los cuales envían la información leída hacia una computadora como si dicha información se hubiera tecleado. El código de barras, una representación digital binaria en una serie de líneas y espacios paralelos anchos y delgados, codifican en unos y ceros el valor de un dígito o de una letra, de tal forma que la computadora pueda ver, reconocer y entender el lenguaje para dar entrada a un dato reduciendo el margen de error y aumentando la velocidad. Con este patrón de barras y espacios, se codifica al número que identifica en forma única a cada uno de los productos, vehículos o personas.

Existen diferentes simbologías (una simbología es la forma en que se codifica la información en las barras y espacios del símbolo de código de barras) para diferentes aplicaciones, cada una de ellas con diferentes características. Las principales características que definen una simbología de código de barras son las siguientes:

- Numéricas o alfanuméricas.
- De longitud fija o de longitud variable
- Discretas o continuas
- Número de anchos de elementos
- Autoverificación.

Un símbolo de código de barras (es decir, la impresión física de un código de barras) puede tener, a su vez, varias características, entre las cuales se pueden nombrar:

- Densidad: Es la anchura del elemento (barra o espacio) más angosto dentro del símbolo de código de barras. Está dado en milésimas de pulgada. Un código de barras no se mide por su longitud física, sino por su densidad.

- WNR: Es la razón del grosor del elemento más angosto contra el más ancho.
- Usualmente es 1:3 ó 1:2.

- Quiet Zone: Es el área blanca al principio y al final de un símbolo de código de barras. Esta área es necesaria para una lectura conveniente del símbolo.

La tarjeta de código de barras, es una tarjeta de apariencia similar a la magnética, pero en lugar de la banda, lleva impresa un código de barras, el cual puede incluso ser protegido con una banda protectora (código oculto) que evita la duplicación de la tarjeta por fotocopias. El código de barras oculto, es cuando por encima del código de barras se coloca un filtro infrarrojo de forma tal que el código no puede ser leído por el ojo humano. Esto aumenta su seguridad ya que no es fotoduplicable. Sin embargo, sigue siendo relativamente fácil copiarla mediante el lápiz óptico adecuado y una simple impresora láser o de chorro de tinta, haciendo de las tarjetas de código de barras muy vulnerables.

La ventaja de esta tarjeta, es que al pasarla por el lector, no existe rozamiento, sólo hay un haz de luz que lee el código en cuestión, con lo cual su vida útil es levemente mayor. No hay que olvidar tampoco que no se pueden rayar, porque de esa forma se altera o incluso llega a hacerse ilegible el código, obligando al cambio de tarjeta.

El costo de las tarjetas es similar a las magnéticas, sin embargo, con estas tarjetas se permite una construcción rápida y económica por el mismo usuario, teniendo como ventaja el bajo costo y la facilidad de generar las credenciales.

Figura 11. Tarjeta de código de barras

La función de los lectores de código de barras es leer la información codificada en las barras y espacios del símbolo, y enviarla a un decodificador que a su vez la envía a una computadora o terminal. Los lectores generan una señal digital pura de las barras y espacios. En el caso de los lápices ópticos esta señal es de baja frecuencia, pues es generada por el barrido de las barras y espacios que hace el operador al deslizar el lápiz sobre el símbolo de código de barras (la señal generada es llamada wand). En el caso del láser, la señal es similar a la generada por el lápiz, sólo que a una frecuencia mucho mayor. Esta última señal es conocida como HHLC (Hand Held Laser Compatible),

Existen varios tipos de lectores de código de barras:

- Lápiz óptico: debe ser deslizado haciendo contacto a lo ancho del código, se envía una señal digital pura de las barras y espacios a una frecuencia igual a la velocidad con que se desliza el lápiz.

- Láser de pistola: Realiza un barrido mediante una luz láser y que genera una señal similar a la del lápiz óptico, pero a una mayor frecuencia. Esta señal es conocida como HHLC (Hand Held Laser Compatible).

- CCD (Dispositivo de Carga Acoplada): Mediante un arreglo de fotodiodos toma una foto del símbolo de código de barras y la traduce a una señal, que puede ser similar a la enviada por el láser (HHLC) o a la del lápiz óptico.

- Láser omnidireccional: Es un lector que envía un patrón de rayos láser y que permite leer un símbolo de código de barras sin importar la orientación del mismo.

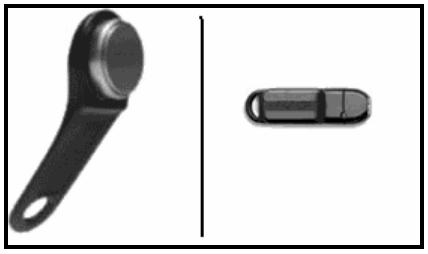
Figura 12. Lector de tarjetas de código de barras

2.3.1.3. Sistemas de llaves electrónicas

La llave electrónica, es una pastilla electrónica encapsulada en acero inoxidable de unos 16 mm. de diámetro, que se transportan con un soporte plástico de unos 5 cm. de largo con un ojalillo en su parte superior para poder colgarlo en un llavero. Brindan un muy alto nivel de seguridad, ya que son altamente resistentes al desgaste, siendo ideales para ambientes industriales en donde la probabilidad de falla, vandalismo o sabotaje sea alta, aunque no son recomendables para ambientes con alto grado de generación de corriente estática, por ejemplo, oficinas con mucha alfombra y ambientes muy secos.

Las llaves son duraderas y funcionan sin pila ni batería. Cada llave tiene un código único (más de 280 mil millones de combinaciones), con esta tecnología, evita la posibilidad de duplicarlas, haciéndolas muy confiables. En precio son unos de los medios más caros, aunque en relación nunca se desgastan, como puede suceder con una tarjeta, con lo cual a largo plazo resulta conveniente.

Figura 13. Llaves electrónicas



La lectura de las llaves, se realiza con contacto y cada llave es utilizable sobre varios lectores, pero cada lector sólo reconoce llaves autorizadas. El lector es de acero inoxidable y por ende no tiene desgaste con el uso.

Figura 14. Lector de llaves electrónicas

2.4. Sistemas biométricos

2.4.1. Biometría

La biometría es la disciplina que permite identificar y/o obtener rasgos de la persona basándose en sus características físicas y/o en sus pautas de comportamiento. De esta forma estas tecnologías permiten establecer una relación entre una persona y un determinado patrón asociado a ella de forma segura e intransferible.

La biometría permite que, mediante unos dispositivos especiales de lectura, podamos tener acceso a los lugares físicos, por medio de las características de la persona.

2.4.2. Características de un indicador biométrico

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquiera sea el indicador, debe cumplir con cuatro requerimientos:

- Universalidad: cualquier persona posee esa característica.
- Unicidad: la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña.
- Permanencia: la característica no cambia en el tiempo.
- Cuantificación: la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como indicador biométrico. Luego de seleccionar algún indicador que satisfaga los requerimientos antes señalados, es necesario imponer restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores.

2.4.3. Definición de Sistema biométrico

Un sistema biométrico es un sistema automatizado que realiza labores de biometría. Estos sistemas, en cuestión de segundos obtienen una muestra biométrica del individuo, extraen aquellos datos y los comparan con la base de datos para decidir finalmente si corresponden o no a la identidad de la persona en cuestión. Es decir, son sistemas de chequeo de patrones.

Un sistema biométrico se fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. Los sistemas biométricos "identifican" la parte del cuerpo humano para posteriormente generar un código único que reconozca las características individuales de la persona. A este tipo de código, el cual está formado por patrones biológicos se le llama código biológico.

La diferencia principal de los métodos biométricos de identificación con los métodos clásicos radica en que la propia persona proporciona la identificación única, la cual, no puede ser perdida ni robada y su falsificación resulta cuanto menos costosa.

Un sistema Biométrico por definición, es un sistema automático capaz de:

- Obtener la muestra biométrica del usuario final.
- Extraer los datos de la muestra.
- Comparar los datos obtenidos con los existentes en la base de datos.
- Decidir la correspondencia de datos.
- Indicar el resultado de la verificación.

2.4.4. Características de un sistema biométrico

Las características básicas que un sistema biométrico para identificación personal debe cumplir pueden expresarse mediante las restricciones que deben ser satisfechas. Ellas apuntan, básicamente, a la obtención de un sistema biométrico con utilidad práctica. El sistema debe considerar:

- El desempeño: El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

- La aceptabilidad: Indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar confianza a los mismos.

- La fiabilidad: Refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva.

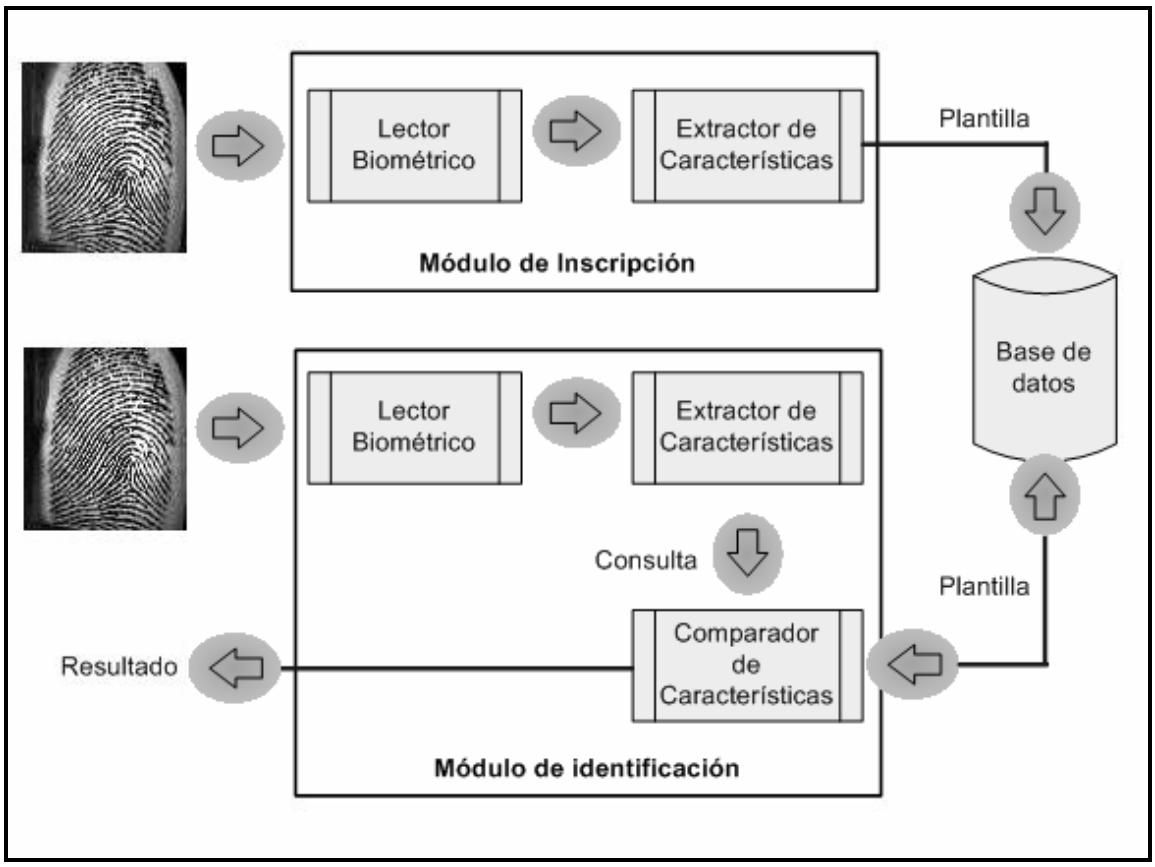
2.4.5. Arquitectura de un sistema biométrico

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos con los datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema. La arquitectura típica de un sistema biométrico puede entenderse conceptualmente como dos módulos:

- Módulo de inscripción: El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características. El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del indicador. El conjunto de características anterior, que será almacenado en una base de datos central u otro medio, recibirá el nombre de plantilla. En otras palabras una plantilla es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso.

- Módulo de identificación: El módulo de identificación es el responsable del reconocimiento de individuos, por ejemplo en una aplicación de control de acceso. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de las plantillas. La representación resultante se denomina consulta y es enviada al comparador de características que confronta a éste con uno o varias plantillas para establecer la identidad.

Figura 15. Arquitectura de un sistema biométrico, ejemplificado con huellas dactilares



El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de fase de inscripción, mientras que los procesos realizados por el módulo de identificación reciben la denominación de fase operacional.

2.4.6. Fase operacional de un sistema de identificación personal

Un sistema biométrico en su fase operacional puede operar en dos modos:

- Modo de verificación: La verificación consiste en cotejar los datos disponibles en una base de datos con los datos obtenidos por el mecanismo biométrico, para asegurarse de que la persona presente es quien dice ser. Un sistema biométrico operando en el modo de verificación comprueba la identidad de algún individuo comparando la característica sólo con las plantillas del individuo, respondiendo a la pregunta: ¿eres tú quién dices ser? Esto conduce a una comparación uno-a-uno para determinar si la identidad reclamada por el individuo es verdadera o no.

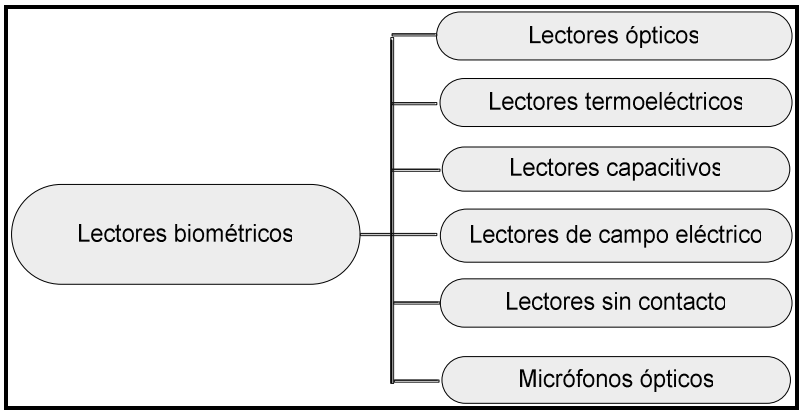
- Modo de Identificación: La identificación consiste en que, a partir del elemento que se está utilizando para verificar (por ej.la huella dactilar), se pueda llegar a los datos de la persona que pone su dedo sobre el lector biométrico. Un sistema biométrico operando en el modo de identificación descubre a un individuo mediante una búsqueda exhaustiva en la base de datos con las plantillas, respondiendo a la pregunta ¿quién eres tú?. Esto conduce a una comparación del tipo uno-a-muchos para establecer la identidad del individuo.

Generalmente es más difícil diseñar un sistema de identificación que uno de verificación. En ambos casos es importante la exactitud de la respuesta. Sin embargo, para un sistema de identificación, la rapidez también es un factor crítico. Un sistema de identificación necesita explorar toda la base de datos donde se almacenan las plantillas, a diferencia de un sistema verificador.

2.4.7. Lectores biométricos

En la siguiente figura se muestran los diferentes tipos de lectores biométricos que existen.

Figura 16. Tipos de lectores biométricos



2.4.7.1. Lectores ópticos

Este tipo de lectores es uno de lo más comunes, los cuales están formados por cámaras de video de tipo CCD.

La cámara CCD contiene de un circuito que consiste de varios cientos de miles de elementos de píxeles localizados en la superficie de un diminuto circuito integrado.

Cada píxel se ve estimulado con la luz que incide sobre él, almacenando una carga de electricidad. Los píxeles se encuentran dispuestos en forma de malla con registros de transferencia verticales y horizontales que transportan las señales a los circuitos de procesamiento de la cámara. Esta transferencia de señales ocurre 6 veces por segundo.

2.4.7.2. Lectores termoeléctricos

Actualmente estos sensores están solamente aplicados al reconocimiento de huella dactilar, estos utilizan un sistema único para reproducir el dedo completo a través del sensor. Durante este movimiento se realizan tomas sucesivas y se pone en marcha un software que reconstruye la imagen dactilar.

El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos. Este tipo de tecnología permite su uso bajo condiciones medioambientales extremas, como temperaturas altas, humedad, suciedad o contaminación. Además, cuenta con la ventaja de autolimpiado del sensor, con lo que se evitan las huellas latentes.

Como primera desventaja de estos lectores tenemos que la cualidad de la imagen depende un poco de la habilidad del usuario que utiliza el escáner, la segunda desventaja es el calentamiento del sensor. Lo cual aumenta el consumo de energía considerablemente. Este calentamiento se produce para evitar la posibilidad de un equilibrio térmico entre el sensor la superficie de la yema dactilar.

2.4.7.3. Lectores capacitivos

Este tipo de lector es bastante utilizado para el reconocimiento de huella dactilar. Su funcionamiento es que se genera una imagen de las crestas y valles del dedo. En la superficie de un circuito integrado de silicona se dispone un arreglo de platos sensores capacitivos conductores que están cubiertos por una capa aislante. La capacitancia en cada plato sensor es medida individualmente depositando una carga fija sobre ese plato.

Las ventajas de este diseño es su simplicidad. Una desventaja es que debido a la geometría esférica del campo eléctrico generado por el plato sensor se obtiene un efecto de solapamiento sobre los platos vecinos, lo que provocará una reducción de la resolución de imagen. Otra desventaja es que no trabajan adecuadamente cuando no se tienen condiciones óptimas en la piel.

2.4.7.4. Lectores de campo eléctrico

Estos lectores funcionan con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel). Este tipo de lectores pueden trabajar bajo cualquier condición.

El sensor de campo eléctrico para reconocimiento de huella dactilar origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Los sensores reproducen una imagen mucho más nítida que la producida por lectores ópticos o capacitivos.

2.4.7.5. Lectores sin contacto

Un lector sin contacto funciona de forma asimilar al sensor óptico. Normalmente con un cristal de precisión óptica a una distancia de dos o tres pulgadas de la huella dactilar mientras se escanea el dedo. La yema del dedo se introduce en un área con un hueco. Las huellas escaneadas son esféricas, lo que origina la utilización de un algoritmo mucho mas complejo.

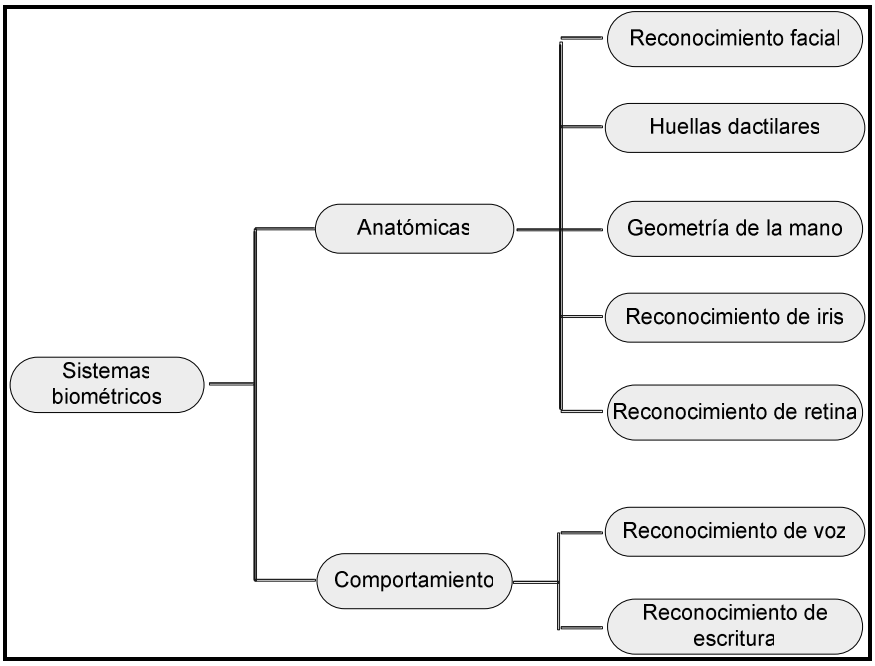
2.4.7.6. Micrófonos ópticos

Estos micrófonos son utilizados para reconocimiento de voz. La luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica. Cuando las ondas de sonido golpean a la membrana, ésta vibra; cambiando de esta manera las características de la luz reflejada. Un foto-detector registra la luz reflejada que en conjunto con una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido.

2.4.8. Técnicas de sistemas biométricos

Existen una gran variedad de sistemas biométricos que pueden ser clasificados de acuerdo a la característica del individuo que capturan para efectuar la autenticación. Algunas veces, un sistema basado solamente en una característica biométrica no es suficiente, por lo que se puede utilizar la técnica multimodal, la cual combina diferentes métodos biométricos para aumentar el nivel de seguridad.

Figura 17. División de los sistemas biométricos



2.4.8.1. Reconocimiento facial

Analiza las características faciales por medio de una imagen óptica que explora algunos aspectos sobresalientes del rostro, eso es registrado por medio de un algoritmo en una base de datos.

Los métodos utilizados en el reconocimiento de rostro van desde la correlación estadística de la geometría y forma de la cara, hasta el uso de tecnología de redes neuronales que buscan imitar la manera en que funciona el cerebro humano. Muchos de estos sistemas pueden reconocer a una persona aún cuando esta se haya dejado crecer la barba o el bigote, se pinte o se cambie el estilo del cabello, tenga maquillaje o use anteojos.

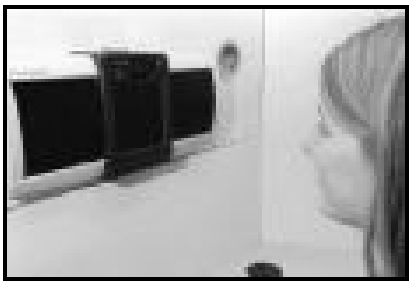
Los sistemas de reconocimiento facial no sólo trabajan con imágenes del rostro, algunos, incrementan la seguridad almacenando vistas frontales y laterales. Esto produce un mapa en 3 dimensiones, que elimina la posible falla de seguridad utilizando fotos de legítimos usuarios. En estos casos, si el sistema no detecta que se trata de una imagen tridimensional, rechaza el acceso.

El proceso de reconocimiento facial consta de dos partes importantes: la detección y el reconocimiento.

2.4.8.1.1. Etapa de detección

Para poder capturar la imagen tridimensional del rostro, la persona se para frente a una cámara digital para que el proyector recorra el rostro con un patrón de luz invisible codificado. La imagen que se crea tiene un nivel de detalle que permite ver la cabeza del individuo de oreja a oreja, con lo que es posible distinguir incluso a los gemelos más idénticos ya que la máquina mide, a través de algoritmos, las distancias entre cierta cantidad de puntos en la superficie de la cara, luego la cámara genera una imagen de video y una fotografía biométrica. Finalmente, la plantilla está lista para ser usada.

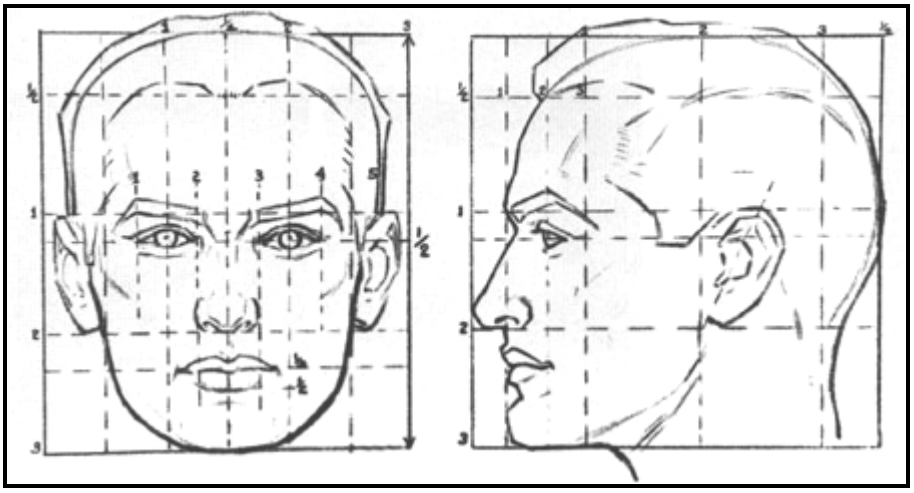
Figura 18. Lector de reconocimiento facial



Durante la detección, la combinación de los equipos y programas de computación aíslan los elementos faciales de una imagen y eliminan la información extraña. El software examina la imagen en sus estructuras faciales típicas y una vez que los ha encontrado, calcula el resto de la cara. Entonces corta los detalles que dan como resultado una cara dentro de un marco rectangular llamado máscara binaria.

La técnica básica de imágenes faciales, se encarga de encontrar bases de espacios vectoriales compuestas por pocas imágenes que expliquen de forma apropiada el espacio de las imágenes faciales. Un sistema basado en imágenes faciales considera cada imagen fácil como un conjunto de las áreas claras y obscuras dispuestas en un modelo determinado. Estos sistemas se centran en características específicas tales como nariz, ojos, bocas, cejas, curvaturas del hueso y las distancias relativas entre ellos.

Figura 19. Rostro con parámetros extraídos



2.4.8.1.2. Etapa de reconocimiento

El algoritmo de reconocimiento compara las imágenes faciales con las de la base de datos.

La verificación para la aceptación se produce también por coincidencia del registro con el rostro actual, lo cual se basa en la utilización de una cámara Web como sensor y software apropiado para el reconocimiento. Cuando una persona se ubica frente a la cámara, el programa utilizado para reconocimiento, proyecta distintas coordenadas mediante cálculos matemáticos para formar la cara del usuario dentro de un rectángulo virtual. Luego del reconocimiento se comparan las características faciales con los patrones almacenados y cuando se encuentra coincidencia, se permite el acceso.

2.4.8.2. Reconocimiento de huellas dactilares

La identificación por huella digital, consiste en obtener imágenes ópticas o electrónicas del dedo por un proceso de enrolamiento, estas se registran en una base de datos o en una tarjeta inteligente en forma de algoritmo. La transacción positiva se produce cuando el dedo de quien pretende ser aceptado por el sistema coincide con el registro existente. Para este reconocimiento, el usuario sólo tiene que situar la yema de un dedo sobre una superficie con un lector especializado.

La arquitectura de los sistemas de huella digital consta de 3 etapas: Etapa de adquisición de datos, etapa de extracción de características y etapa de comparación de patrones.

2.4.8.2.1. Etapa de adquisición de datos

Es la adquisición mediante escáner de la imagen de la huella dactilar. Existen diferentes tipos de lectores. Los lectores ópticos utilizan una cámara y un prisma para capturar la imagen. Otros utilizan campos eléctricos, ultrasonido y métodos termales.

Figura 20. Lector de reconocimiento de huellas dactilares

2.4.8.2.2. Etapa de extracción de características

En esta etapa, a partir de la adquisición de datos se extraen automáticamente las características de la huella.

Este método, se basa en distinguir las líneas en las yemas de los dedos, bifurcaciones, islotes, etc. Al colocar el dedo en un dispositivo que capta huellas digitales, la superficie de la piel es explorada y se convierte en una imagen formada por píxeles que se comparan con los patrones guardados y permiten el acceso o lo rechazan.

Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un lector, éste toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella).

La extracción de las características biométricas se realiza en las siguientes etapas:

- Adelgazamiento: En esta etapa se aplican algoritmos consecutivos de adelgazamiento de imágenes con el fin de reducir el grosor de las crestas de la imagen binaria a un solo píxel. Estas operaciones son necesarias con el fin de poder extraer las minucias de la huella digital.

- Eliminación de imperfecciones: Se aplica un algoritmo de eliminación de todas las líneas que no son crestas, y de conexión de todas las crestas rotas.

- Extracción de minucias: Finalmente, se extraen los puntos característicos que constituye el patrón biométrico de la huella. Para ello se determina si cada píxel de la imagen adelgazada pertenece o no a una cresta, y en el caso de que así sea, si pertenece a una bifurcación o un principio o final de cresta. Hay cinco características diferentes de puntos de minucia:
    - Crestas que finalizan y las crestas que crean bifurcaciones.
    - Orientación: cada punto de minucia se orienta en una dirección particular.
    - Frecuencia espacial: la frecuencia espacial se refiere a la densidad de las crestas en una superficie determinada.

- Curvatura: referente al ratio de cambio de orientación de las crestas.
- Posición: la posición de los puntos de minucia referentes a la localización en el plano x, y, y también en concordancia a los puntos fijos.

Figura 21. Detalles minucia

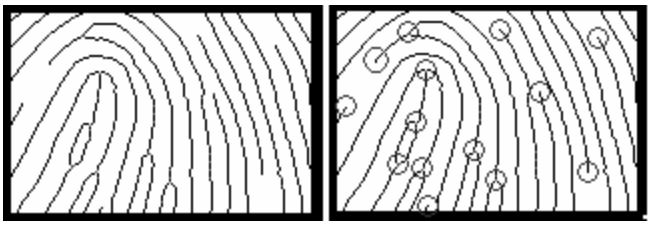


Figura 22. Huella digital con minucias

Existen ciertos factores externos a la extracción de minucias, que hay que tomar en cuenta:

- El entorno: Factores tales como la lluvia, humedad alta/baja, suciedad pueden reducir la calidad de las imágenes de las huellas capturadas.

- Demografía: Ciertos segmentos de la población (personas que trabajan con productos químicos, etc.) presentan dificultades sistemáticas para la extracción de los puntos de minucia y la detección de las características globales de la huella digital. Sin embargo, estas huellas generalmente contienen una gran cantidad de características no convencionales.

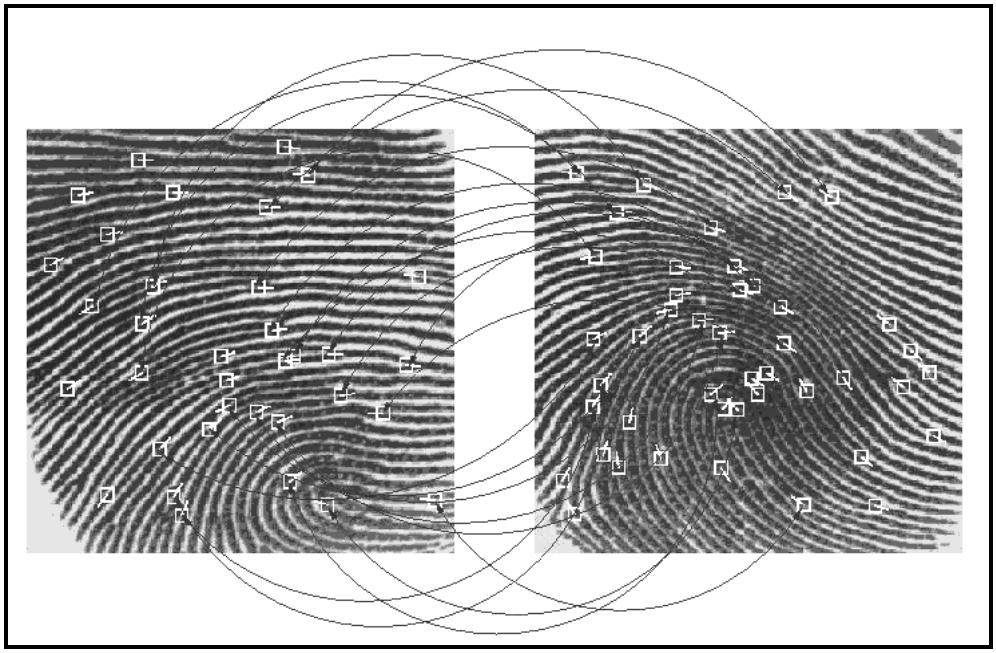
- Colocación del dedo: En los lugares destinados al reconocimiento de huellas por métodos convencionales como por ejemplo una comisaría de policía, existe personal entrenado para realizar las muestras de las huellas digitales del individuo marcándolas con tinta en una plantilla. Por otro lado, no es así en lugares no destinados a tal efecto como en una oficina, donde la captura de la imagen por medio de un sensor es la solución ideal. Problemas posibles que se pueden originar en estos entornos son la rotación, distorsiones de la piel en el registro, deformidades por presión, etc.

2.4.8.2.3. Etapa de comparación de patrones

En esta etapa, el patrón biométrico capturado es comparado con el patrón registrado en la base de datos. El grado de similitud resultante de la comparación de los dos patrones es cuantificado dentro de un rango de valores.

Las minucias se comparan contra las que tiene en su base de datos; es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí sino que son estas minucias, concretamente la posición relativa de cada una de ellas. Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos 30 o 40 de éstas. Si la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, denegándosele obviamente en caso contrario.

Figura 23. Proceso de comparación de huellas dactilares



2.4.8.3. Reconocimiento de la geometría de la mano

Los sistemas de autenticación basados en el análisis de la geometría de la mano, son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quién dice ser. Estos sistemas, utilizan el tamaño y forma de la mano y los dedos para verificar la identidad.

Los sistemas basados en la geometría de la mano, se caracterizan por su bajo índice de falsos rechazos, aún en condiciones desfavorables; es decir, la posibilidad de que no reconozca la mano de una persona autorizada. La geometría de la mano se basa en el hecho de que las dimensiones de las manos y los dedos son únicas en cada individuo. Si lo comparamos con otros parámetros biométricos, la precisión de la geometría de la mano es un poco más baja. No obstante, en combinación con un NIP, resulta muy adecuada para la gran mayoría de las aplicaciones.

2.4.8.3.1. Etapa de identificación

La persona sitúa su mano abierta sobre un escáner específico, el cual captura la mano y sus características principales de modo tridimensional. El reconocimiento, se realiza a partir de la forma y geometría de la misma.

Cuando el usuario, sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos -anchura, longitud, área y determinadas distancias-.

Estos datos se transforman en un modelo matemático que se contrasta contra una base de patrones, con lo cual, el sistema es capaz de permitir o denegar acceso a cada usuario.

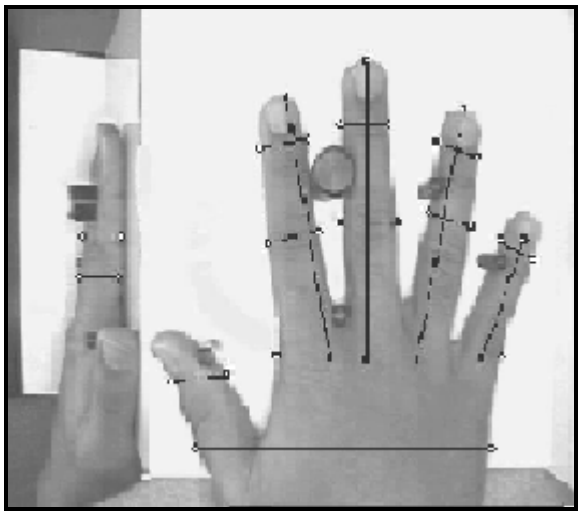
Figura 24. Lector de la geometría de la mano

Uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra -un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida-; de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones: no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

El reconocimiento de la mano se puede realizar en dos y tres dimensiones. Los sistemas de dos dimensiones buscan en la palma de la mano patrones en las líneas, esos patrones son casi tan distintivos como lo son las huellas digitales.

Los sistemas en tres dimensiones miden las dimensiones de la mano, por ejemplo: largo de los dedos, ancho de los dedos, tamaños de falanges, anchuras en las articulaciones de dos dedos, tamaño de la palma, altura de la mano, etc. Para obtener esos datos es necesario un procesamiento de la imagen más complejo de detección de las articulaciones y segmentación de cada dedo. Se pueden obtener hasta 70 medidas geométricas basándose en medidas físicas.

Figura 25. Verificación de la mano con parámetros extraídos



2.4.8.3.2. Etapa de verificación

Si el reconocimiento es realizado en dos dimensiones, el sistema toma los puntos de minucia de la palma y los compara contra el modelo de referencia.

Si el reconocimiento es realizado en tres dimensiones entonces toman los datos de las dimensiones de la mano para realizar la comparación.

2.4.8.4. Reconocimiento de iris

El iris es un componente de la anatomía realmente estable e inalterable, que permite identificar a un individuo de una forma tan precisa como la huella dactilar. El iris es un órgano interno del ojo, es el anillo visible de color que rodea a la pupila, el cual está localizado por detrás de la cornea y del humor acuoso, pero en frente de los lentes.

Debido a que el iris es una estructura muscular que controla la cantidad de luz que ingresa a los ojos, sus detalles intrincados pueden ser medidos en base a las estrías, incisiones, y surcos. La cantidad de información que puede ser extraída de un único iris es mayor que la que puede encontrarse en las huellas dactilares, y la exactitud mayor que la de un ADN.

El reconocimiento del iris se caracteriza por su elevado grado de precisión. Ofrece la posibilidad de identificar a las personas con una certeza del 100%, porque el sistema recupera, rápida e infaliblemente, el código correcto de la base de datos que contiene los códigos del iris de millones de ojos. Así se garantiza la selección de la persona correcta.

Para realizar el reconocimiento del iris se siguen dos etapas: la etapa de detección y la etapa de reconocimiento.

2.4.8.4.1. Etapa de detección

La imagen del iris (el área de color) se captura con una cámara de alta resolución y el sistema analiza sus dobleces y patrones, que son utilizados para identificar a la persona.

Existen dos métodos para efectuar la adquisición del iris, estos son la forma activa y la forma pasiva.

La forma activa requiere que la persona se mueva hacia atrás y adelante de manera tal que la cámara pueda ajustar el foco en el iris. Con la forma activa, es necesario que la persona se localice entre 15 y 35 centímetros de la cámara.

La forma pasiva es diferente y más amigable, debido a que se incorporan una serie de cámaras que localizan y enfocan el iris, lo cual permite al usuario estar a una distancia de un metro y medio.

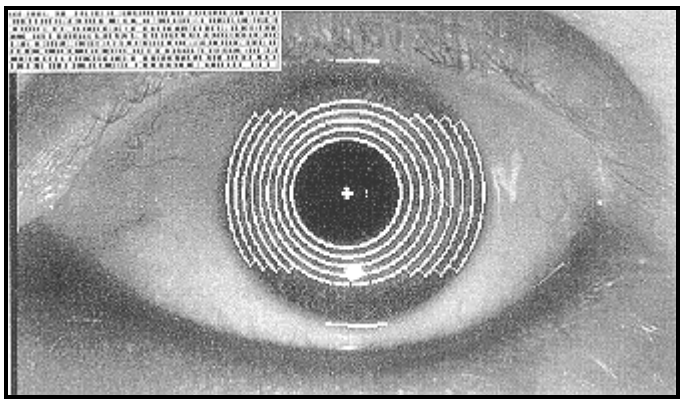
Una cámara de reconocimiento de iris toma una fotografía en blanco y negro de entre 5 y 24 pulgadas, dependiendo del tipo de cámara. Las cámaras certificadas por los estándares internacionales de iluminación segura, utilizan un método no invasivo de rayos cercanos al infrarrojo (similar al utilizado en los controles remotos) que es escasamente visible y muy seguro.

Figura 26. Lectores de iris

La imagen del ojo es primeramente procesada por un programa, que localiza los bordes interiores y exteriores del iris, y el contorno de los párpados, con el objeto de extraer solamente la porción que corresponde al iris. Las pestañas y reflejos que pueden estar cubriendo partes del iris son también detectados y eliminados. Luego, un sofisticado programa matemático codifica los patrones del ojo en un proceso que se denomina demodulación. Este proceso crea un código para la secuencia de textura en el iris similar al código de secuencia utilizado para el ADN.

El proceso de demodulación realiza una muy compacta pero completa descripción de los patrones del iris. Esta secuencia se denomina *IrisCode*, el cual es un código de 256 bytes, el cual representa las características únicas de un iris de una manera robusta que permite una comparación muy rápida y fácil contra una gran base de datos de patrones.

Figura 27. Iris humano y su IrisCode



2.4.8.4.2. Etapa de reconocimiento

El *IrisCode* generado desde la imagen en vivo será comparado con los previamente almacenados para ver si coincide con alguno de ellos, esta etapa se realiza en sólo algunos segundos, incluso con una base de datos de millones de registros. El umbral de decisión se ajusta automáticamente al tamaño de la base de datos de búsqueda para asegurar que no ocurran falsos positivos.

2.4.8.5. Reconocimiento de la retina

Los sistemas basados en las características de la retina analizan la capa de vasos sanguíneos localizados en la parte posterior del ojo. La forma de los vasos sanguíneos de la retina humana es un elemento característico en cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en su reconocimiento.

2.4.8.5.1. Etapa de identificación

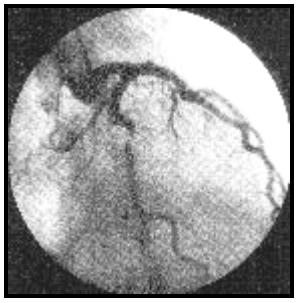
En los sistemas de autenticación basados en patrones de la retina, el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia interocular y el movimiento de la cabeza, mirar a un punto determinado, , lo que redunda en un proceso intrusivo y un contacto cercano con el dispositivo de lectura. Luego de realizar esto, la persona debe pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis.

Figura 28. Lector de retina

Esta técnica requiere del uso de una fuente de luz de baja intensidad para develar el modelo único de la retina (irrepetible en otros individuos, como las propias huellas digitales), lo que le convierte en una de las pocas tecnologías biométricas utilizadas en "identificación" de individuos.

En ese momento se escudriña la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal.

Figura 29. Retina humana



2.4.8.5.2. Etapa de reconocimiento

Luego de detectar los nodos y las ramas del área retinal, se procede a compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

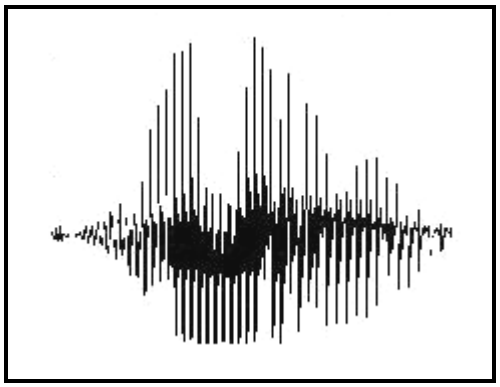
2.4.8.6. Reconocimiento de voz

En un sistema para el reconocimiento de voz, se emplea la biometría física y de conducta con el objetivo de analizar patrones de habla e identificar al interlocutor. Para llevar a cabo está tarea, el patrón creado previamente por el interlocutor, debe ser digitalizado y mantenido en una base de datos

Para el reconocimiento de voz se debe hablar sobre un dispositivo que se encargará de establecer un patrón de voz analizando la frecuencia, los tonos bajos y agudos, vibración de la laringe, tonos nasales y de la laringe, así como otras características de los sonidos emitidos y los comparará con los patrones previamente almacenados para determinar la coincidencia y permitir o no el acceso.

En los sistemas de reconocimiento de voz, se trata de identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

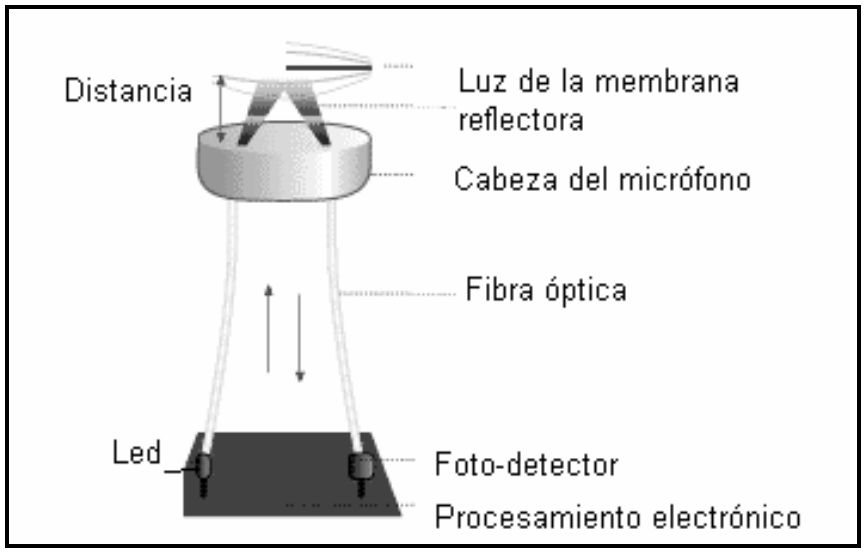
Figura 30. Codificación de la voz



Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer, por ejemplo, el nombre, el teléfono, un NIP, de forma que el reconocedor lo entienda y lo autentique. Lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar (por ejemplo, frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales, etc). Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos.

Los micrófonos ópticos actúan como sensores para el reconocimiento de la voz, los cuales operan de la siguiente forma: La luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica. Cuando las ondas de sonido golpean a la membrana, ésta vibra; cambiando así las características de la luz reflejada. Seguidamente, un foto-detector registra la luz reflejada que en conjunto con una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido.

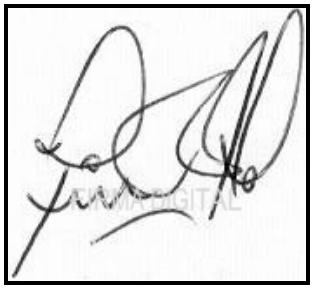
Figura 31. Micrófono óptico



2.4.8.7. Reconocimiento de escritura

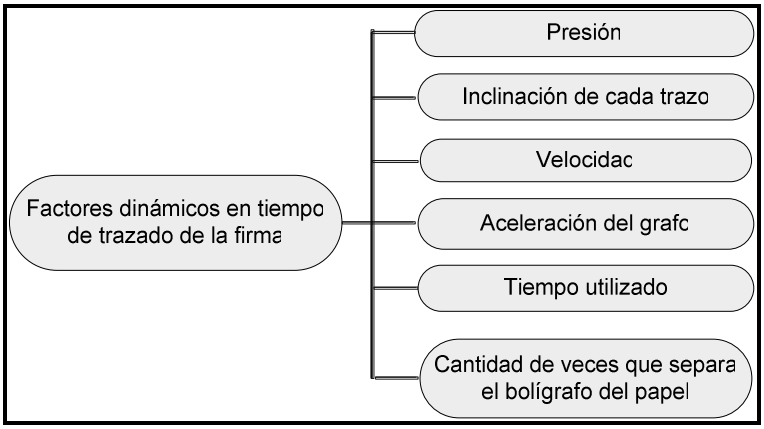
Aunque la escritura -generalmente la firma- no es una característica estrictamente biométrica, se suele agrupar dentro de esta categoría, el objetivo aquí no es interpretar o entender lo que el usuario escribe, sino autenticarlo basándose en ciertos rasgos característicos.

Figura 32. Firma para la verificación de escritura



Un sistema biométrico de este tipo puede identificar mejor una firma que un experto calígrafo, ya que además de analizar la geometría, es decir el trazo de la firma, toma en cuenta las características dinámicas de la firma (DSV), que son factores que indican “como” fue realizado el acto de firmar.

Figura 33. Factores dinámicos en tiempo de trazado de la firma



Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se decrementa su seguridad.

Una vez que el sistema conoce las firmas de sus usuarios, cuando ellos desean acceder a él, se les solicita tal firma, con un número limitado de intentos. La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

Figura 34. Lector de reconocimiento de escritura

3. COMPARACIÓN DE LAS TECNOLOGÍAS DE CONTROL DE ACCESO

3.1. Factores a tomar en cuenta

En función de la situación en que se necesite realizar una autenticación segura del usuario, existen diferentes parámetros que son necesarios tomar en cuenta para elegir un sistema en particular.

Los parámetros identificados son la fiabilidad, facilidad de uso, aceptación del usuario, estabilidad del medio de identificación, desgaste del lector, tiempo de acceso, mantenimiento del lector, precio del medio de identificación y precio del lector.

Debido a que los sistemas basados en conocimiento, basados en posesión y los sistemas biométricos, tienen diferentes características y su funcionamiento es distinto, existen muchos de los parámetros que se identificaron, que no aplican para algún tipo de sistema.

3.1.1. Fiabilidad

La fiabilidad es un elemento importante para solventar la necesidad de autenticar de forma segura la identidad de las personas que pretenden acceder a un determinado servicio o recinto físico.

La fiabilidad está relacionada con las tasas de falso rechazo y de falsa aceptación. Por tasa de falso rechazo (FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad, ya que se está proporcionando acceso a un recurso a personal no autorizado a acceder a él.

La fiabilidad de los sistemas basados en posesión (tarjetas y llaves), es mucho menor que la de los biométricos ya que una tarjeta puede perderse fácilmente y la puede utilizar otro individuo.

3.1.2. Facilidad de uso

La facilidad de uso de los sistemas de control de acceso es un factor de vital importancia, hay que tomar en cuenta que para la implementación de cualquiera de los sistemas, se requiere que las personas aprendan a utilizar los dispositivos. La facilidad de uso se ve afectada por la inexperiencia de las personas y por la poca relación con la tecnología.

3.1.3. Aceptación del usuario

Algunos sistemas provocan menos rechazo que otros en la gente común debido a que sus características están incorporadas en la vida cotidiana. La aceptación del usuario siempre será un factor esencial en la implementación exitosa de un sistema de control de acceso. Para que las personas acepten un medio de identificación, es necesario que los dispositivos no causen ningún tipo de inconveniente, incomodidad física, ansiedad por alta tecnología, que mantengan la privacidad, ni generar dudas acerca de la salud de los individuos.

3.1.4. Estabilidad del medio de identificación

La estabilidad se refiere a cuan estable es el medio de identificación (las tarjetas, el indicador biométrico, etc.), es decir, a la poca o ninguna variación que puedan sufrir el indicador utilizada para dicha identificación.

Existen dos causas que pueden incidir en la ocurrencia de errores de la lectura, estos son los factores ambientales (ruido, iluminación, suciedad, clima, etc.) y condición del miembro corporal (cortaduras, desgaste, envejecimiento, etc.).

La estabilidad para los sistemas basados en posesión se refiere al desgaste que sufre la tarjeta. El desgaste de las tarjetas, es un elemento importante a considerar, debido al costo, el tiempo utilizado y los cuidados que se deben realizar. Si el medio de identificación se desgasta fácilmente, la persona que lo utiliza tendrá problemas al identificarse.

La estabilidad es importante, ya que en todo momento se puede autenticar al usuario al efectuar la comparación con la muestra obtenida, sin embargo siempre existen interferencias, las cuales son factores que van a afectar el correcto desempeño de los sistemas. Estos factores son externos y provocan que el sistema no identifique correctamente a la persona, produciendo una tasa de error mayor de la que se espera.

3.1.5. Tiempo de acceso

La velocidad es un factor primordial para medir el rendimiento de los diferentes sistemas de control de acceso. El tiempo en una organización es de vital importancia, por lo que es necesario que los usuarios tengan una identificación rápida para que puedan acceder a las instalaciones.

El tiempo de acceso abarca desde que la persona utiliza su medio de identificación hasta que el sistema valida o deniega el acceso.

3.1.6. Mantenimiento del lector

El mantenimiento debe ser efectuado constantemente para prolongar la vida útil del dispositivo, sin embargo, este mantenimiento implica un costo, lo cual repercute en la elección de la tecnología del SCA a utilizar.

Se debe considerar que todos los equipos requieren de un mantenimiento programado para su buen funcionamiento y para la detección temprana de fallas, evitando así contratiempos con lo cual se conserva la disponibilidad necesaria, por lo tanto, el costo del mantenimiento debe ser lo mas bajo posible, pero conservando un balance en cuanto a la seguridad que se necesite como se menciona anteriormente.

La falta de mantenimiento del lector, puede provocar un acceso no autorizado o la no identificación de las personas. Es por ello, que se debe evaluar esta característica, ya que ella influye en la calidad del sistema que se requiere.

3.1.7. Precio del medio de identificación

Para los sistemas basados en posesión, se toma en cuenta el precio de la tarjeta ya que por la maniobrabilidad y la cantidad de usuarios de la empresa la demanda de tarjetas aumenta considerablemente, afectando los recursos económicos de la empresa. En el caso de los sistemas biométricos este precio no aplica, ya que el medio de identificación son características propias de la persona a identificar, lo cual no tiene ningún costo para la organización.

3.1.8. Precio del lector

El precio del lector es importante tomarlo en cuenta antes de implementar un sistema de control de acceso, debido a la inversión inicial que se requiere.

3.2. Análisis de cada factor

Habiendo explicado los factores que se deben tomar en cuenta, se analizan los factores para cada tecnología de SCA.

Tabla IV. Argumentos de Fiabilidad

Tecnología de SCA	Fiabilidad
Sistemas basados en conocimiento	Existe muy poca fiabilidad con sistemas de este tipo, ya que es muy fácil averiguar el número de identificación personal. Este esquema es muy frágil: basta con que una de las partes no mantenga la contraseña en secreto para que toda la seguridad del modelo se pierda.
Tarjeta de proximidad	La fiabilidad es mayor que la las de banda magnética y código de barras, ya que las tarjetas poseen un código único de fábrica que nunca se repite. Sin embargo, la fiabilidad disminuye al ser una tecnología de tarjetas, la cual puede ser prestada a otra persona.
Tarjeta de banda magnética	Es más fiable que el código de barras, ya que es más difícil la duplicación, sin embargo, los códigos pueden ser leídos con un lector estándar y duplicados con una grabadora magnética. La fiabilidad disminuye al ser una tecnología de tarjetas, la cual puede ser prestada a otra persona.
Tarjeta de Código de barras	La fiabilidad es baja, ya que los códigos de barras visibles pueden ser fotocopiados fácilmente, además, el código oculto puede ser duplicado con un programa de impresión de códigos de barras. La fiabilidad disminuye aún más al ser una tecnología de tarjetas, la cual puede ser prestada a otra persona.
Llave electrónica	La fiabilidad es buena, ya que su tecnología avanzada evita la posibilidad de duplicarlas, haciéndolas muy confiables. Sin embargo, la llave electrónica puede ser prestada a otra persona, lo cual disminuye la fiabilidad.

Reconocimiento Facial	La fiabilidad del reconocimiento facial es alta, debido a que se toman diferentes características de la cara para corroborar la identidad del individuo, sin embargo, se puede dar el caso de que existan dos caras con las mismas características, provocando que el sistema falle.
Reconocimiento de huellas dactilares	La huella dactilar de un individuo, es un patrón fiable para determinar la identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona.
Reconocimiento de geometría de la mano	El método de geometría de la mano, posee un alto grado de fiabilidad, ya que se extraen ciertos datos de la mano en tres dimensiones, tales como la anchura, longitud, áreas y determinadas distancias. Sin embargo, es posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda
Reconocimiento de iris	Utilizar el iris es un sistema muy seguro, ya que éste cuenta con 266 características que pueden ser medidas y no hay dos personas en todo el mundo con el mismo iris. Además, el iris derecho es diferente al izquierdo y no puede ser manipulado, copiado ni robado. Por otro lado, las características del iris son muy complejas, con lo que se proporciona un modelo muy preciso para la autenticación de cada persona, teniendo una tasa de error de entre 1 y 1,2 entre un millón.
Reconocimiento de retina	El reconocimiento de retina es totalmente fiable, ya que para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi 0, y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.
Reconocimiento de voz	Su fiabilidad se ve afectada cuando un atacante reproduce las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Sin embargo esto es difícil que suceda.
Reconocimiento de escritura	Tiene uno de los niveles más bajos de exactitud entre los lectores biométricos, el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución (aparte de una concienciación de tales usuarios) es relajar las restricciones del sistema a la hora de *aprender* firmas, con lo que se decrementa su fiabilidad.

Tabla V. Argumentos de facilidad de uso

Tecnología de SCA	Facilidad de uso
Sistemas basados en conocimiento	Estos sistemas son muy fáciles de utilizar, ya que el usuario únicamente debe introducir el número de identificación personal.
Tarjeta de proximidad	Es muy fácil de utilizar, ya que no se necesita que la tarjeta sea pasada por una ranura o en un sentido específico. Además, el hecho de que la lectura se realiza por radio frecuencia permite incluso, que pueda ser leída dentro de una billetera, una cartera, un maletín, etc.
Tarjeta de banda magnética	Son fáciles de utilizar, pero deben de pasarse por un lector, provocando un rozamiento, lo cual las hacen más difíciles de utilizar que las tarjetas de proximidad.
Tarjeta de Código de barras	Poseen la misma facilidad de uso que las tarjetas de banda magnética.
Llave electrónica	Provee un fácil manejo y uso ya que únicamente se utiliza la llave con el lector y se facilita el ingreso.
Reconocimiento Facial	Únicamente, es necesario que el usuario se coloque frente a la cámara en la posición correcta. Puede ser difícil registrarse porque algunas personas tienen dificultad para alinear la cara en la posición correcta.
Reconocimiento de huellas dactilares	El sistema es fácilmente de utilizar, ya que cuando un usuario desea autenticarse ante el sistema, solamente sitúa su dedo en un área determinada.
Reconocimiento de geometría de la mano	El sistema es fácil de utilizar, ya que cuando un usuario necesita ser autenticado, únicamente sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura. Sin embargo, es necesario que la mano este bien pegada a las guías para facilitar la lectura.
Reconocimiento de iris	El sistema no es complicado de utilizar. La imagen del iris es capturada a través de una cámara de precisión sin necesidad de tener un contacto físico con la misma, evitando de este modo posibles preocupaciones sobre la higiene del equipo.
Reconocimiento de retina	Estos sistemas son difíciles de utilizar, ya que el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia Ínter-ocular y

	el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis.
Reconocimiento de voz	Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo, debiendo el usuario, poner atención a las frases que debe repetir.
Reconocimiento de escritura	Para utilizar un sistema de autenticación basado en firmas se solicita a los futuros usuarios un número determinado de firmas, lo cual no lo hace un método extremadamente fácil de utilizar.

Tabla VI. Argumentos de aceptación del usuario

Tecnología de SCA	Aceptación del usuario
Sistemas basados en conocimiento	Los sistemas basados en conocimiento son aceptados por el usuario, ya que únicamente deben teclear el número de su identificación, sin provocarle daño alguno.
Tarjeta de proximidad	Las tarjetas de proximidad son bien aceptadas por el usuario, ya que no les causa ninguna incomodidad física, ni temor alguno, además de que son muy prácticas de utilizar.
Tarjeta de banda magnética	Son bien aceptadas por el usuario ya que no atenta contra su salud, ni les proporciona ninguna incomodidad física.
Tarjeta de Código de barras	Son bien aceptadas por el usuario, ya que no les causa ninguna incomodad física o daños a su salud.
Llave electrónica	Es de gran aceptación ya que no requiere un cuidado especial.
Reconocimiento Facial	Debido a que los usuarios se ubican frente a una cámara, existe cierta resistencia a este tipo de análisis.
Reconocimiento de huellas dactilares	Debido a que el reconocimiento de huellas se asocia a los criminales, muchos usuarios recelan del reconocedor y de su uso, es por ello que no son tan aceptados como una tarjeta.
Reconocimiento de geometría de la mano	Es un método con un mediano grado de aceptación de los usuarios por la fuente de contaminación que existe, lo que provoca un desagrado en colocar la mano, en donde otros usuarios la han colocado.

Reconocimiento de iris	No son tan aceptados por el usuario, pero son los menos incómodos de usar de los lectores de ojo, porque no se realiza un contacto cercano con el lector.
Reconocimiento de retina	Este método no es aceptado por los usuarios, ya que el hecho de mirar a través de un binocular (o monocular), no es cómodo para los usuarios, ni aceptable para muchos de ellos: los usuarios no se fían de un haz de rayos analizando su ojo, y por otro un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas.
Reconocimiento de voz	El reconocimiento de voz posee la cualidad de una excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente
Reconocimiento de escritura	Este tipo de verificación es aceptada por los usuarios, ya que se encuentran acostumbrados a realizar firmas, sin embargo, puede provocar disgustos cuando el sistema les solicite realizar varias firmas porque no los reconoce.

Tabla VII. Argumentos de estabilidad

Tecnología de SCA	Estabilidad
Sistemas basados en conocimiento	La estabilidad es muy buena, ya que no existen factores externos que puedan afectar la identificación.
Tarjeta de proximidad	La estabilidad es afectada por el desgaste de la tarjeta de proximidad. La cual es menor que de la de las demás tarjetas, ya que la lectura del código se realiza sin contacto mediante la transmisión de una onda de radiofrecuencia, lo que significa que no tiene desgaste por rozamiento. Sin embargo, una flexión excesiva puede dañar la antena interna de la credencial.
Tarjeta de banda magnética	El desgaste de la tarjeta de banda magnética es la más alta de todas las tarjetas, ya que el rozamiento continuo con el cabezal magnético

	desgasta la banda. Exponer este tipo de tarjetas a campos magnéticos intensos, produce que la tarjeta se dañe. Es necesario, manejar las credenciales cuidadosamente para prolongar su vida útil.
Tarjeta de Código de barras	El desgaste de la tarjeta de código de barras es mayor que las tarjetas de proximidad pero menor que las de banda magnética, ya que las credenciales generadas con impresoras de transferencia térmica son afectadas por el rozamiento continuo con el lector y las credenciales generadas con impresoras estándar son afectadas por la humedad.
Llave electrónica	El desgaste de la llave es bajo, ya que la pastilla es altamente resistente al desgaste, ya que está encapsulada en acero inoxidable de unos 16 mm. de diámetro.
Reconocimiento Facial	La estabilidad es afectada por los cambios de los rasgos faciales, los cuales son muy comunes, estos se pueden dar por cambios en el cabello, la edad, o deformidades físicas.
Reconocimiento de huellas dactilares	Poseen una estabilidad alta, ya que las huellas dactilares no cambian a lo largo del tiempo. Sin embargo, características como la suciedad, heridas o inclusive la pérdida del miembro pueden provocar una menor estabilidad.
Reconocimiento de geometría de la mano	Este sistema tiene una estabilidad media debido a los cambios que pueda sufrir el usuario, como por ejemplo el crecimiento o distorsiones que pueda sufrir la mano por la edad, enfermedad u otros factores. Además, la perdida del miembro puede afectar.
Reconocimiento de iris	El patrón del iris es constante durante la vida de una persona, por lo tanto tiene una estabilidad alta.
Reconocimiento de retina	Al igual que el iris, la retina es constante durante la vida de una persona, pero puede también disminuir su estabilidad por factores como la luz o la irritación de la retina. Además, para que el lector pueda realizar su trabajo, el usuario no debe de tener lentes puestos.
Reconocimiento de voz	Las características de la voz pueden ser alteradas fácilmente por varios factores, como inclemencias del tiempo (meteorología, temperatura), edad, ruido, etc.
Reconocimiento de escritura	La escritura puede variar mucho por una gran cantidad de factores como firmas fáciles o cambiantes, analfabetismo, nerviosismo, estar contra el tiempo, etc.

Tabla VIII. Argumentos de tiempo de acceso

Tecnología de SCA	Tiempo de acceso
Sistemas basados en conocimiento	El tiempo de acceso oscila entre 1 y 2 segundos, siendo rápido, ya que el usuario debe ingresar su código, luego se verifica que el número ingresado sea válido
Tarjeta de proximidad	Únicamente es necesario, que se acerque la tarjeta al lector, llevando un tiempo aproximado de 1 segundo.
Tarjeta de banda magnética	Es necesario tener en cuenta la posición de la banda respecto del cabezal y mantener una velocidad constante, llevando un tiempo aproximado de 2 o 3 segundos, ya que las velocidades varían entre 10 y 127 cms/seg.
Tarjeta de Código de barras	Para la lectura de este tipo de tarjetas, se debe tener en cuenta la posición del código respecto del lente óptico y mantener una velocidad constante. Un lector de código de barras puede hacer aproximadamente 100 lecturas/seg. El tiempo de acceso total es de 2 o 3 seg.
Llave electrónica	La lectura de las llaves, se realiza con contacto, el tiempo de acceso oscila entre 1 y 2 segundos.
Reconocimiento Facial	Consume el tiempo en el que el usuario se ubica frente a la cámara y en el que se compara las características faciales con los patrones almacenados. El tiempo de acceso oscila de 3 a 6 seg.
Reconocimiento de huellas dactilares	Para estos sistemas, se debe ingresar el NIP del empleado desde el teclado y colocar la huella en la misma posición con la que se la registró originalmente. El tiempo de verificación es menor de 0.5 segundos. En total, puede consumiendo consumir un tiempo aproximado de 3 a 6 seg.
Reconocimiento de geometría de la mano	Son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser. Poseen buena velocidad de análisis de las plantillas. El tiempo de verificación oscila entre 0.2 y 0.5 seg. En total puede consumir un tiempo aproximado de 2 a 5 seg.
Reconocimiento de iris	El proceso de autenticación no es todo lo rápido que debiera en poblaciones de usuarios elevada. El tiempo de acceso oscila entre 3 y 6

	segundos.
Reconocimiento de retina	Además de consumir el tiempo en el que el usuario se ajusta el binocular para la lectura, el proceso de autenticación es lento. El tiempo total de acceso es mayor de 6 segundos.
Reconocimiento de voz	Para la verificación de voz, el usuario emplea tiempo hablando delante del analizador, al que se añade el que éste necesita para extraer la información y contrastarla con la de su base de datos; aunque actualmente en la mayoría de sistemas basta con una sola frase. El tiempo de acceso, es habitual que el usuario se vea obligado a repetirla porque el sistema le deniega el acceso. El tiempo de acceso es de 3 a 6 segundos
Reconocimiento de escritura	Es uno de los que emplea mayor tiempo, debido a que el usuario emplea tiempo realizando la firma, después de introducida, es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

Tabla IX. Argumentos de mantenimiento del lector

Tecnología de SCA	Mantenimiento del lector
Sistemas basados en conocimiento	Es necesario el mantenimiento del dispositivo del teclado, el cual puede ser realizado 2 o 3 veces al año.
Tarjeta de proximidad	Los lectores son unidades totalmente selladas y sin partes móviles, lo que garantiza un funcionamiento correcto sin límite de uso. Los mismos se pueden instalar, también al intemperie y no los afectan las inclemencias del tiempo, las altas y bajas temperaturas, ni la lluvia. Además, estos lectores tienen muy poco desgaste, ya que el lector puede quedar en el interior de la puerta, o incluso ser embutido dentro de la pared.
Tarjeta de banda magnética	El lector de la tarjeta de banda magnética tiene un desgaste bastante alto, ya que posee carcaza plástica, y al quedar el cabezal de lectura expuesto, puede ser dañado desde el exterior o afectado por el polvo y la

	humedad, es por ello que se requiere de limpieza general en la cabeza lectora de la banda magnética.
Tarjeta de Código de barras	El mantenimiento es menor que el de las magnéticas. Este lector tiene un desgaste muy bajo, ya que posee carcaza metálica y buena resistencia a la humedad. Sin embargo, el lente de enfoque puede ser dañado desde el exterior o afectado por el polvo y la luz solar excesiva, por lo que se requiere de limpieza general y en especial el área de lectura del código de barras.
Llave electrónica	El mantenimiento es muy bajo, ya que el lector es de acero inoxidable.
Reconocimiento Facial	Es necesario darle mantenimiento a la cámara, esto es recomendable unas 3 veces al año, esto es debido al polvo y la humedad que pueda existir
Reconocimiento de huellas dactilares	Debido a que el lector esta sellado, se recomienda darle un mantenimiento unas 2 o 3 veces al año para eliminar el polvo y la suciedad que ingrese. También es necesario darle mantenimiento al teclado.
Reconocimiento de geometría de la mano	Las fallas más comunes en estos equipos ocurren en el teclado, el cual tiene movimiento mecánico y también, la base de posición de la mano, la cual puede desgastarse con el uso. Sólo requiere de limpieza general y en especial en la base donde se coloca la mano y los espejos
Reconocimiento de iris	El mantenimiento se debe realizar a la cámara que capta los patrones del iris. Es necesario abrir el lector para eliminar el polvo y la suciedad que ingrese.
Reconocimiento de retina	Debido a que la persona debe tener un contacto cercano, es necesario darle un mantenimiento frecuente para evitar la suciedad que se genera y limpiar los binoculares.
Reconocimiento de voz	E micrófono óptico requiere muy poco mantenimiento, ya que es un dispositivo cerrado.
Reconocimiento de escritura	El lector del reconocimiento de escritura requiere muy poco mantenimiento, ya que únicamente es necesario realizar una limpieza en la parte donde se realiza la firma.

Tabla X. Argumentos de precio del medio de identificación

Tecnología de SCA	Precio del medio de identificación
Sistemas basados en conocimiento	No aplica.
Tarjeta de proximidad	Debido a que estas tarjetas llevan incorporados un chip, Se depende siempre de un proveedor ya que las credenciales vienen con un código de fábrica fijo grabado en el chip electrónico. Su precio es mayor que las tarjetas de banda magnética o de barras.
Tarjeta de banda magnética	El costo disminuye con relación a las de proximidad, debido que únicamente se debe generar e imprimir la banda.
Tarjeta de Código de barras	Su costo disminuye considerablemente ya que el código de barras es de fácil impresión. Puede utilizarse un kit de autogeneración (software e insumos) de manera de generarlas en una impresora común (láser o chorro de tinta), teniendo como ventaja el bajo costo y la facilidad de generar las credenciales.
Llave electrónica	En precio son unos de los medios más caros, aunque en relación (salvo que alguien lo pierda) nunca se desgastan, como puede suceder con una tarjeta, con lo cual a largo plazo resulta conveniente.
Reconocimiento Facial	No aplica
Reconocimiento de huellas dactilares	No aplica
Reconocimiento de geometría de la mano	No aplica
Reconocimiento de iris	No aplica
Reconocimiento de retina	No aplica
Reconocimiento de voz	No aplica
Reconocimiento de escritura	No aplica

Tabla XI. Argumentos de precio del lector

Tecnología de SCA	Precio del lector
Sistemas basados en conocimiento	El precio del lector es uno de los más económicos, su precio es menor de 80 USD.
Tarjeta de proximidad	El precio aumenta con respecto a los de banda magnética y código de barras debido a la tecnología que este representa, existen lectores desde 130 USD dependiendo la tecnología que utilicen.
Tarjeta de banda magnética	Dependiendo de la tecnología que utilicen, estos lectores se encuentran entre los 80 y 120 USD.
Tarjeta de Código de barras	El precio del lector es bajo. Los lectores con alta velocidad, oscilan entre 80 y 120 USD
Llave electrónica	El precio del lector de la llave electrónica, es uno de los más económicos de toda la línea de lectores. Su precio es menor de 80 USD.
Reconocimiento Facial	El precio de este tipo de sistemas anda alrededor de los 1500 USD
Reconocimiento de huellas dactilares	Es uno de los que posee mejor precio dentro de los biométricos. El precio de este tipo de sistemas se encuentra por los 1200 USD
Reconocimiento de geometría de la mano	El precio de este lector tiene un costo desde 2,100 USD.
Reconocimiento de iris	Este tipo de sistema, tiene un precio elevado ya que su precio es mayor de los 4000 USD.
Reconocimiento de retina	El precio es similar a los sistemas de reconocimiento de iris, es mayor que los 4000 USD.
Reconocimiento de escritura	A comparación de los demás sistemas biométricos, el costo es bajo, ya que oscila entre 80 y 120 USD.
Reconocimiento de voz	El lector de reconocimiento de voz junto con el reconocimiento de escritura son los que poseen el costo más bajo de los biométricos.

3.3. Comparaciones

En esta parte se muestra el resumen de comparaciones según el análisis de cada factor que se identificó

3.3.1. Escala a utilizar

En la siguiente tabla, se presenta las escalas a utilizar para realizar las comparaciones entre las diferentes tecnologías de control de acceso.

Tabla XII. Escala a utilizar para las comparaciones

Abreviatura	Escala
DB	Demasiado Bajo
B	Bajo
MB	Medio bajo
MA	Medio alto
A	Alto
DA	Demasiado Alto
NA	No Aplica

3.3.2. Cuadro comparativo

En la siguiente tabla se muestran las comparaciones de los factores identificados para cada tecnología de control de acceso.

Tabla XIII. Comparaciones entre los diferentes medios de identificación

		Sistemas basados en posesión				Sistemas biométricos						
Factor de evaluación	**Sist. Conoc.**	**Tarj. Prox**	**Tarj. Magn.**	**Tarj. Barras**	**Llaves elect.**	**Facial**	**Huellas Dact.**	**Geom. Mano**	**Iris**	**Retina**	**Escritura**	**Voz**
Fiabilidad	DB	MB	B	DB	MB	A	DA	A	DA	DA	MA	MA
Facilidad de uso	DA	DA	DA	DA	DA	MB	A	A	MB	DB	MA	MA
Aceptación del usuario	DA	DA	DA	DA	DA	B	MA	MB	B	DB	A	MA
Estabilidad del medio de id.	DA	MB	DB	B	MB	A	DA	A	A	A	MA	MB
Tiempo de acceso	B	DB	B	B	DB	MA	MA	MB	MA	A	A	MA
Mantenimiento del lector	MB	DB	A	MB	DB	MA	MA	MA	MA	A	MB	MB
Precio medio de identificación	NA	MA	B	DB	DA	NA	NA	NA	NA	NA	NA	NA
Precio lector	DB	MB	B	B	DB	MA	MA	A	DA	DA	B	B

Tabla XIV. Aplicaciones de cada medio de identificación

Medio de Identificación	Aplicaciones
Sistema basado en conocimiento	Control de acceso de muy baja seguridad.
Tarjeta de proximidad	Control de acceso de alta seguridad: control de personal en lugares de alto tránsito.
Tarjeta de banda magnética	Control de acceso de bajo costo: Clubes, gimnasios, obras sociales, etc.
Código de barras	Control de acceso de bajo costo: Control de horario de personal.
Llave electrónica	Control de acceso para ambientes industriales.
Reconocimiento Facial	Los casinos los utilizan para identificar estafadores. Complejos comerciales y edificios los utilizan para identificar delincuentes y personas no gratas.
Huellas dactilares	Uso general. Además de control de acceso de máxima seguridad y de acceso restringido: Control de personal en sitios con tendencia al fraude.
Geometría de la mano	Uso general.
Reconocimiento de iris	Instalaciones nucleares, servicios médicos, centros penitenciarios.
Reconocimiento de retina	Instalaciones nucleares, servicios médicos, centros penitenciarios.
Verificación de voz	Accesos remotos.
Verificación de escritura	Industrial.

CONCLUSIONES

1. Es necesario que una tecnología de control de accesos tenga las características de autenticación para que identifique a la persona, para que indique los lugares a los cuales tiene acceso y un registro de auditoría para tener control de lugares y tiempos en los que el sistema le ha otorgado permisos o denegaciones para acceder a determinada área.

2. Debido a que los requerimientos de seguridad en una empresa son cambiantes a lo largo del tiempo, es necesario revisar y actualizar el diseño de un plan de seguridad, en el cual es necesario reconocer áreas para agruparlas en base al nivel de seguridad que se necesite, reconocer, identificar y abordar los riesgos que pueden surgir, agrupar personas e identificar los accesos que necesita cada persona por cada área reconocida.

3. La biometría es la respuesta práctica a los problemas de seguridad de muchas empresas, pues, soluciona los problemas que tienen los sistemas basados en posesión y en conocimiento, debido a que reducen el riesgo de falsificación de identidad, extravío y/o deterioros de identificadores personales. A pesar de que el precio del lector es mayor, se reduce el costo de fabricación de medios de identificación, lo que ocasiona un ahorro a largo plazo.

4. Para evaluar las diferentes tecnologías de control de acceso, existen factores comunes que se analizan para las diferentes tecnologías de control de acceso, estas son: fiabilidad, facilidad de uso, aceptación del usuario, estabilidad del medio de identificación, desgaste del lector, tiempo de

acceso, mantenimiento del lector, precio del medio de identificación y precio del lector. Sin embargo, para la elección de la tecnología, es necesario tomar en cuenta la cantidad de seguridad que la organización necesita y los recursos con los que dispone.

5. En general, los sistemas basados en posesión pueden utilizarse cuando no se necesita mayor seguridad y los recursos son muy limitados. Dentro de los sistemas biométricos, se identifica que el reconocimiento de la mano y de huellas ofrece mayor conveniencia para el usuario, el reconocimiento del dedo y del iris ofrece mayor fiabilidad. El reconocimiento de voz y escritura son los más críticos con respecto al entorno, el lector de reconocimiento de iris y retina son los más caros. No obstante, la elección correcta requiere un cierto conocimiento y experiencia en biometría y control de accesos.

RECOMENDACIONES

1. Es necesario que las organizaciones comprendan los beneficios que les puede otorgar un SCA. Una organización no se debe enfocar solamente en el precio del sistema, sino que debe de realizar un análisis costo-beneficio.

2. Cuando una organización tenga implementado un SCA, debe de continuarse con el análisis de las actividades del plan de seguridad. Este proceso es continuo y se debe realizar para identificar nuevas necesidades, tipos de controles o riesgos que puedan surgir.

3. Con el crecimiento que se tienen en las empresas actuales los sistemas biométricos son las soluciones más aplicables a los diversos problemas de verificación existentes.

4. La elección del sistema de verificación se debe escoger de acorde a las características de la empresa o de acorde a la utilización que se le de a las mismas con el fin de mantener un balance entre la aceptación de los usuarios y las necesidades de la empresa.

BIBLIOGRAFÍA ELECTRÓNICA

1. Acerca del control de accesos
   http://www.tdsi.co.uk/es/about_access.htm

2. Autenticación de usuarios
   http://www.rediris.es/cert/doc/unixsec/node14.html

3. Biometría
   http://sircbaleares.com/control/biometria.htm

4. Biometría Perú
   http://www.biometria.com.pe

5. Biometric Consortium
   http://www.biometrics.org/

6. Código de barras
   http://www.geocities.com/SoHo/Cafe/8909/barcode.html

7. Código de barras y lectores biométricos
   http://www.digitalcode.com/c%C3%B3digo.htm

8. Control de acceso y presentismo
   http://www.intelektron.com/sitio/noticias/notas%20de%20%20interes/4.htm

9. Controles de acceso
http://www.weco-sa.com.ar/controles-acceso.htm

10. ¿En que consiste la biometría?
http://www.investigaciones.cl/paginas/noticias/notagos_05/22ago05/link01.htm

11. Equipos biométricos y el control de acceso
http://www.neotec.com.pa/ComoPorque/handreader/HRpresenteyfuturo.htm

12. Firma facial única
http://www.terra.es/tecnologia/articulo/html/tec8348.htm

13. Gestión de seguridad:
http://www.nedap-aeos.com/new/es/products/bio_hand.php

14. Identificación personal.
http://www.zator.com/Internet/A6_6.htm

15. Introducción a los biométricos:
http://www.tress.com.mx/boletin/julio2005/biometricos.htm.

16. Introducción a los sistemas biométricos:
http://www.xiden.com/site/noticias/detalle_noticia.asp?idnoticia=55

17. La biometría al alcance de la mano
http://www.nec.cl/bases/i-510-2-1124301099.pdf

18. Las tecnologías biométricas
www.internacional.edu.ec/academica/informatica/creatividad/uide-bits/uide-bits-04-2003.pdf+biometria+iris&hl=es

19. Medios de identificación
http://www.simicro.com/medios_de_identificacion.htm

20. Medios para Identificación del Personal.
http://www.securitytag.com.ar/Api/idparapersonal.htm

21. Pros y contras de los sistemas biométricos en el control de personal
http://www.lagente.com/cgi-bin/contenido.pl?Art=56

22. ¿Qué es biometría?
http://www.homini.com/biometria.htm

23. Reconocimiento del iris
http://www.nedap-aeos.com/new/es/products/bio_iris.php

24. Reconocimiento de manos
http://www.nedap-aeos.com/new/es/products/bio_hand.php

25. Sistemas biométricos
http://www.udabol.edu.bo/biblioteca/sistemas/sistemas/10redneuro/7r1sisbio19e/sisbiometricos.htm

26. Sistemas de Identificación
http://www.aceproject.org/main/espanol/et/et73.htm

27. Tabla comparativa de tecnologías
http://www.larconsia.com/tecnologias.asp

28. Tarjetas con chip
http://www.condusef.gob.mx/informacion_sobre/t_chip/t_chip.htm

29. Tarjetas credenciales
http://www.genera.cl/productos/credenciales/credenciales.htm

30. Técnicas biométricas para la identificación y verificación de personas.
http://revista.robotiker.com/articulos/articulo67/pagina1.jsp

31. Tecnología de tarjetas:
http://www.geocities.com/gcataneo/tarjetas/tecnologia.htm

32. Tecnología por proximidad
http://www.securynet.com/rubros/rev/temas/temas10433.htm

33. Verificación de escritura
http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node115.html

34. Verificación de la geometría de la mano
http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node120.html