View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Repositorio Institucional Universidad Católica de Colombia

BIOHACKING PARA LA PROTECCION DE LOS ACTIVOS DE INFORMACIÓN EN LAS PYMES POR MEDIO DE UN SISTEMA DE DOBLE FACTOR DE AUTENTICACION

Erik Fabricio Cifuentes Díaz

Maikol Estiven Martínez Vásquez

Trabajo de Grado presentado para optar al título de Especialista en Seguridad de la Información

Asesor: MSc. Nelson Augusto Forero Páez, PhD (c)

Universidad Católica de Colombia

Facultad de Ingeniería

Especialización en Seguridad de la Información

Bogotá D.C., Colombia

2019

Agradecimientos

Cordial saludo el agradecimiento de este proyecto va dirigido primero a Dios por proveernos salud, sabiduría y las herramientas para poder entregar un trabajo de calidad, también a nuestras familias quienes nos han apoyado desde el inicio de la especialización, agradeciendo también al Ing. Nelson Forero. Ing. Carlos Fernando Pérez, al ing. Jaime Fernando Pérez, a la Ing. Sandra Bernate, a la Esp. En D.P Liseth Rodríguez, a la A.E Carmen Forero quienes gracias a sus conocimientos colaboraron para poder concluir con este este proyecto. De igual manera a la Universidad Católica de Colombia por abrirnos las puertas y así formarnos como especialistas en seguridad de la información en bien de la sociedad.

creative commons

Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)

La presente obra está bajo una licencia:
Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)
Para leer el texto completo de la licencia, visita:
http://creativecommons.org/licenses/by-nc/2.5/co/

Usted es libre de:

Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra

hacer obras derivadas

Bajo las condiciones siguientes:

Atribución — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).

No Comercial — No puede utilizar esta obra para fines comerciales.

TABLA DE CONTENIDO

RESUMEN

Las organizaciones tienen sus propias necesidades, pero todas con un objetivo en común, proteger sus activos de información y no verse afectados por atacantes. De esta manera se brindará información de qué es y en qué consiste la integración de diferentes factores para la autenticación de usuarios. Por la cual este documento tiene como finalidad dar a conocer el biohacking como una técnica a utilizar en la protección de activos de información en las compañías. Definiendo que la técnica de Biohacking es la mejora del cuerpo humano mediante el uso de recursos tecnológicos, y la autenticación doble factor o multifactorial como el uso de dos o más herramientas distintas que trabajan en un mismo sistema. Con base a lo mencionado el uso de dispositivos biométricos aplicados a la seguridad de la información e implementados estratégicamente en conjunto con los factores externos de autenticación como: (Token, Tarjetas de proximidad, passwords, Etc.). Da lugar a la integración del doble factor de autenticación que proporciona una capa más en la seguridad, siendo este uno de los controles mayormente implementados por las PYMES para la protección de activos de información, partiendo de esto las corporaciones se encuentran en la obligación de crear mecanismos para mantener y garantizar la confidencialidad de la información, tarea en la que un sistema de doble factor de autenticación (A2F), puede ser de gran utilidad.

Palabras clave: Biohacking, Activos de información, Seguridad, doble factor de autenticación A2F, Control de Acceso, PYMES.

I. INTRODUCCIÓN

Todas las organizaciones tienen sus propias necesidades, pero todas con un objetivo en común: **proteger sus activos de información** y no verse afectados por cyber delincuentes. De esta manera se brindará información básica de qué es y en qué consiste la integración del sensor biométrico y el dispositivo para doble factor. Los activos y sistemas de información, redes de datos y la manipulación no adecuada de la información por los usuarios, han logrado que día a día se presenten más oportunidades para los cyber delincuentes, por esto el aseguramiento de los mismos tienen una suma importancia frente a posibles ataques, con el fin de garantizar la triada de la seguridad de la información y evitando poner en riesgo las mismas. Con lo anterior mencionado se requiere la implementación de un sistema y/o técnicas de aseguramiento como un sistema de doble factor de autenticación en adelante (A2F) en las áreas donde se almacena la información sensible de la organización, disminuyendo riesgos como reputación, daño físico a instalaciones y/o personal de la organización. Entre otros riesgos que podría causar la pérdida de información. Observando en el desarrollo de este proyecto, estará enfocado en la implementación de un sistema A2F para el personal, situado en los lugares con acceso a información sensible de la PYME, ofreciendo una capa más de seguridad a los riesgos de la organización a los cuales están expuestos. [1] En la actualidad las organizaciones están sujetas a las nuevas tecnologías de la información donde se embarcan en nuevos retos frente a procesos encaminados a la seguridad de la información, mitigando así ataques informáticos en el interior de la empresa o ataques realizados por externos a la misma, en el desarrollo de proyecto de aseguramiento de los activos de información de una organización se presentarán evidencias documentadas respecto al nivel de seguridad antes y después de implementar el método (A2F).Se implementará un dispositivo adicional (microchip o nano sensor) en un usuario voluntario piloto bajo el término de Biohacking, con el fin de evidenciar la mejora de la seguridad especialmente en el control de accesos con la implementación del (A2F) lo que incidirá directamente en el aseguramiento de los activos de información. Y se estará dando a conocer información recolectada en el transcurso del proyecto, pues con esto se quiere poner en conocimiento a la organización de que se encuentra involucrada o comprometida con la seguridad de la información, con diversas herramientas y posibilidades para usarse de manera estratégica. Toda esta información está inmersa en la implementación de este sistema, pero dejando el conocimiento de que no hay sistema totalmente inmune a riesgos.

II. GENERALIDADES

A. Línea de Investigación

Software Inteligente y Convergencia Tecnológica

Mantener la dinámica investigativa y las tasas de contribución a los índices de producción intelectual del sistema nacional de ciencia y tecnología. Apoyados en la visión de GISIC para el año 2022 el grupo de investigación en software inteligente y convergencia tecnológica será un referente local en la investigación y desarrollo de componentes de software basados en inteligencia artificial, que integren soluciones para la salud, educación y pequeña empresa maximizando la producción y optimización de recursos económicos y ambientales. [1]

B. Planteamiento del Problema

Con la dinámica y evolución tecnológica, hoy día no se tiene conocimiento detallado en cuanto a los problemas de seguridad y vulnerabilidades de los sistemas de los dispositivo /o sensores biométricos en las organizaciones que se utilizan para restringir o mejorar el control de acceso a lugares de mayor riesgo o que requieren un mayor nivel de seguridad por sus activos de información que se están protegiendo, siendo uno de los mayores problemas que enfrenta cualquier organización con su tecnología de seguridad en controles digitales, ya que, constantemente los cyber delincuentes están pensando en cómo comprometerlos, y a pesar de que diferentes mecanismos como las huellas poseen patrones únicos, pero es posible realizar una copia física de la huella, con el uso de técnicas de clonación de tipo forense, convencional y digital.

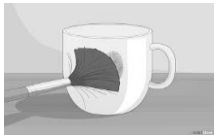
En la actualidad existen tres maneras de comprometer la seguridad de los lectores biométricos dactilares [2]:

- Consiste en que de manera voluntaria, se hace una réplica de su huella en algún método de impresión, con la finalidad de poder darle su huella a otras personas.(**ver** Error! Reference source not found.)
- Consiste en la aplicación de métodos forenses convencionales para obtener la huella de una persona sin consentimiento de la misma; El uso de esta técnica tiene dos aplicaciones:
    - la primera es utilizada por organizamos de investigación los cuales cuentan con toda la infraestructura y tecnología para la obtención de huellas de manera legal.
    - La segunda se remonta a métodos forenses artesanales como el polvillo de carbón, en donde un delincuente puede hacer una copia de la huella, dejada en espejos, envases, picaportes y muchas otras superficies planas, que hacen que la huella conserve toda su forma, puesto que, en superficies rugosas, este tipo de procedimiento no sería tan exacto, ya que se necesita como mínimo un 75% de la

totalidad de la huella, para que esta pueda ser cotejada. (**ver** Error! Reference source not found.Error! Reference source not found.)

- Consiste en utilizar métodos tecnológicos para su obtención de los rasgos biométricos, donde utiliza la suplantación de hardware y de software a través de ataques informáticos. (**ver**
-
-)

Tabla 1Captura Huellas Forenses

 *Ilustración 1 Técnica Clonación por Goma*
 *Ilustración 2Técnica Recolección por Polvillo*
 *Ilustración 3Técnica de Recolección por Software*

C. Antecedentes del problema

El reto de la Autenticación Biométrica (AB) principalmente radica en lograr que los dispositivos tecnológicos puedan llevar a cabo operaciones que son, en apariencia, simples de forma rápida y libre de errores. Dotar a las máquinas con la capacidad de llevar a cabo la AB de manera precisa se ha revelado como una tarea muy compleja, gracias a años de investigación, algunos productos

como los reconocedores de huellas digitales o los escáneres de iris han pasado de la ficción a la vida cotidiana.

La identificación de las personas, según Researchgate [4], se constituyen dos tipos: el aspecto físico, que siempre se encuentran presentes, por ejemplo, la huella dactilar, el iris, la geometría de la mano, la cara, etc. y la conducta, donde siempre tiene que hacer una "realización" de los mismos por ejemplo, escritura, la firma, el tecleo o la forma de andar.

Cualquier característica física puede usarse como biométrica mientras cumpla las siguientes propiedades:

- Universalidad: Todo el mundo debe poseerla.
- Unicidad: Solo debe ser de una persona.
- Permanencia: Debe estar presente constantemente.
- Evaluabilidad: El rasgo debe poder ser medido cuantitativamente.

Aparte de estas propiedades, hay otro conjunto de propiedades que deben satisfacerse:

- Rendimiento: Debe satisfacer las necesidades de uso.
- Aceptabilidad: El personal debe estar dispuesto a hacerlos parte de su día a día.
- Fraude: Alto grado de seguridad

Adicionalmente la AB está enfrentada a técnicas de hacking como la que se presenta a continuación, en la que investigadores han utilizado una red neuronal para generar huellas artificiales, la cual podría ser la herramienta perfecta para un 'hacker', pues podría servir como llave maestra para los sistemas de identificación biométrica. Expertos de la Escuela de Ingeniería de la Universidad de Nueva York (EE.UU.) [5]han desarrollado un sistema llamado **DeepMasterPrints**, según un informe presentado sobre biométrica en octubre 2018 en Los Ángeles. De acuerdo con la investigación, las huellas falsas, generadas por el sistema, se pueden replicar una de 5 huellas digitales reales en un sistema de identificación biométrica. Conocido como ataque de diccionario el cual es un método para averiguar una contraseña probando todas las palabras del diccionario, pero en vez de contraseñas, una herramienta inspirada en DeepMasterPrints podría probar varias huellas dactilares falsas a través de un sistema para ver si alguna coincide con una real, una coincidencia parcial y una característica común de DeepMasterPrints, donde provecha dos propiedades de los sistemas de autenticación basados en huellas dactilares. La primera es que, por razones ergonómicas, la mayoría de los escáneres de huellas dactilares no leen el dedo completo, sino una parte del dedo que toca el escáner. Eso simplifica la tarea del 'hacker', ya que no tiene que conseguir una coincidencia completa, sino solo de una porción de la huella. La segunda, se relaciona con algunas características de las huellas dactilares que son más comunes que otras. Eso significa que una huella falsa que contiene muchas características comunes es más probable que

coincida con otras huellas dactilares de lo que sugiere el azar. Para mayor información ver anexo 15

Basándose en esas ideas, los investigadores utilizaron una técnica de aprendizaje automático común, llamada red de confrontación generativa, para crear artificialmente nuevas huellas dactilares que coincidían con la mayor cantidad posible de huellas dactilares reales. Haciendo poco probable que se pueda usar la técnica para ingresar y/o autenticarse. Los investigadores dicen que "es probable que el método subyacente tenga muchas aplicaciones en la seguridad de la huella digital, así como en la síntesis de la misma".

El grupo de investigadores reconoce que sus huellas maestras no son infalibles. De hecho, por el momento tan solo son capaces de replicar una de cada cinco huellas digitales reales en un sistema de identificación biométrica, tal y como recoge The Next Web. Sin embargo, los expertos explican que el algoritmo está diseñado para modificar determinados parámetros de las mismas a través de la técnica del abecedario (repetir una y otra vez) para que se ajusten a las que están memorizadas en el dispositivo. Por esa misma razón, el grupo de investigadores incita a los responsables de estos sistemas de seguridad biométricos a que estudien nuevas técnicas que ayuden a los escáneres convencionales.

En esta investigación se pudo evidenciar que unos estudiantes con conocimientos en IA (inteligencia artificial) dirigidos por Philip Bontrager [5], desarrollaron una herramienta “DeepMasterPrints”, capaz de crear huellas dactilares, como un software que ejecuta millones de contraseñas comunes, podría ejecutar varias huellas dactilares falsas para ver si alguna de ellas coincide con alguna cuenta. La clave de la investigación realizada por estos especialistas enseña un punto importante y que la mayoría de los lectores solo leen un porcentaje de la huella. Así que los investigadores crearon nuevas huellas digitales e introduciéndolas en la red. Solo necesitan crear una serie de impresiones que coincidan con ciertas partes de otras huellas digitales, “Un sistema similar al nuestro podría usarse con fines perversos, pero es probable que no tenga una tasa de éxito como la nuestra a menos que la optimicen”, dijo Bontrager a Gizmodo. “Esto requeriría un trabajo de ingeniería brutal para aplicarlo a un sistema así”.

las nuevas tecnologías permiten a los atacantes escanear las huellas dactilares, según Isao Echizen [7]. Investigador del Instituto Nacional de Informática de Japón (NIII, por sus siglas en inglés), realizó el experimento con las fotografías donde personas mostraban sus yemas de los dedos. Una vez escaneadas, las huellas quedan "ampliamente disponibles" para reproducción indiscriminada y "cualquiera puede hacerlo”. Los sistemas de verificación biométrica (tecnologías de reconocimiento facial y de identificación por voz o por huellas dactilares), que se utilizan para acceder a dispositivos y aplicaciones no son lo suficientemente seguras y se exponen a la suplantación de identidad.

Jan Krissler, también conocido por su alias Starbug [8], un investigador de la Universidad Técnica de Berlín (Alemania), demostró que es capaz de reproducir la huella a partir una foto y de instantáneas desde diferentes ángulos.

Pero, ¿es posible, sencillo y directo como dicen estos expertos? No todos los especialistas en seguridad informática creen que es así, ya que debe cumplirse una serie de condiciones específicas.

Según Ted Dunstone [5], director ejecutivo y fundador de la consultora Biometix -y presidente del Biometric Institute en Australia y Nueva Zelanda, un organismo independiente especializado en ese sector dijo que, efectivamente, "es posible que nos roben las huellas dactilares de una fotografía" pero "sólo bajo determinadas circunstancias específicas". Krissler está de acuerdo: "Depende de la calidad de la fotografía y del sensor", pero si es la adecuada "se puede crear en tan sólo unas horas. Ted Dunstone, también dice que, para que exista la posibilidad de que obtengan nuestra huella dactilar a través de una foto, deben darse las siguientes condiciones:

- RESOLUCIÓN: muy alta resolución.
- PROXIMIDAD: gran campo de visibilidad
- ILUMINACIÓN: debe ser adecuada para abarcar el dedo sin alteración
- COMPRESIÓN: la compresión de la imagen

Además, Isabelle Moeller, directora ejecutiva del Biometrics Institute [10], le comenta que "en realidad, no es tan fácil falsificar un sistema biométrico" y que el riesgo "se puede reducir usando autenticación multifactorial"(un sistema que combina más de una forma de autenticación, como contraseñas y códigos),"la biometría tiene vulnerabilidades que necesitan abordarse". Es posible en el resto de sensores actuales. El motivo: la resolución con la que los sensores actuales trabajan, crean instantáneas de 500-550 puntos por pulgada (dpi), algo insuficiente para que un desmotivo reconozca la huella auténtica de la falsa.

El problema es que algunos dispositivos biométricos no almacenan la información de manera cifrada. Si un delincuente logra acceder, tendría toda la información, para poder acceder a ese dispositivo, actualmente existen una serie de ataques como lo son:

- Esfuerzo cero o Falsa Aceptación mayor que cero: (en inglés, zero-effort), aprovechando que la tasa de error nunca es cero, debido a la similitud en el personal como para confundirlo o
- Adversario: (en inglés, adversary), da la posibilidad de que una persona pueda hacerse pasar por otra, mediante la manipulación de los dispositivos de lectura biométrica.

Los ataques “esfuerzo cero” se aprovechan de la aceptación mayor a 0, puesto que es posible encontrarse con individuos de rasgos muy similares. Estadísticamente, si el resultado es 1 %, se transmite en que 1 de cada 100 intentos tendrá éxito. La manera de ejecutar este ataque es mediante software el cual genera y cargar en el sistema un registro de datos hasta que este coincida con uno valido.

Los ataques “Adversario”, debido a que la mayoría de factores biométricos están presentes y notorios, hace el uso de diversas técnicas de clonación o suplantación como: fotografías, métodos

forenses como la recolección de huella, etc. Para presentarse en un sistema e intentar acceder como el individuo original.

Aparte de esto, hay otros posibles ataques contra un sistema biométrico:

- Ataque MIM: se basa en el uso mecanismos informáticos o físicos, que intercepten los datos trasmitidos.
- Ataque de Repudio: se basa en suplantar al individuo original y realizar acciones sin su conocimiento, desde su punto oficial.
- Ataque de confabulación: se basa en aprovechar los privilegios concientizados desde un administrador del sistema.
- Ataque de Coacción se basa en forzar al individuo original para que se autentique y el poder realizar el ataque.
- Ataque Denegación de servicio: se basa provocar que el sistema colapse y evitar el acceso de los usuarios

Además, los ataques a los sistemas biométricos no tienen que ver con la capacidad de reconocimiento de un rasgo biométrico, sino en la seguridad informática.

D. Pregunta de investigación

¿Cómo incrementar la seguridad de los ACTIVOS DE INFORMACION EN LAS PYMES que son protegidos o resguardados bajo un sistema biométrico dactilar?

E. Justificación

Hoy en día la seguridad informática representa un papel importante para las organizaciones como un actor ante el control y tratamiento de la información, por ende, las organizaciones se enfrentan a constantes ataques, equipos de cómputo, infraestructura, recurso humano. Por esto el aseguramiento de la información para la empresa INTELIBPO S.A.S se convierte en una prioridad. la cual requiere tomar una acción ante las nuevas técnicas que utilizan los atacantes informáticos para el cyber crimen. Con el fin de capacitar a los usuarios de la empresa con acceso a información sensible en cuanto a las herramientas y técnicas existentes al día de hoy disponibles y en pro de aumentar el nivel de la seguridad de los activos de información en la organización, y actualizando los conocimientos de las técnicas y herramientas que se van implementando hoy en día para el aseguramiento de la información, Según La universidad veracruzana [11].

La identificación, valoración y gestión de los activos de información, en función del impacto que representan para una organización. Es un concepto amplio que se centra en todos los activos de información que son de alto valor para las empresas, y las cuales se enfrentan a amenazas como: fraudes por computadora, espionajes, sabotajes, vandalismo, fenómenos naturales, descuido,

desconocimiento o mal uso del tratamiento de la información por parte del recurso humano. Muchas de esas amenazas provienen de ingenieros sociales, hackers, empleados negligentes, errores, entre otros, que buscan dañar la integridad de una organización.

Existen dos factores importantes de la seguridad de la información:

- El valor de los datos de acuerdo con los intereses y necesidades.
- El acceso a la información.

La universidad veracruzana así nos enseña que existe una necesidad sobre toda compañía en proteger los activos de información sensibles y se debe implementar un sistema que ayude con el aseguramiento de está, cumpliendo con los estándares mínimos logrando identificar posibles vulnerabilidades en la seguridad, y el impacto que se tendría sobre la información teniendo como finalidad el análisis de los resultados obtenidos para reforzar los puntos débiles que fueron identificados y así prevenir riesgos.

III. OBJETIVOS

F. Objetivo general

Mejorar la seguridad de los activos de información en las PYMES mediante la implementación de un sistema de doble factor de autenticación(A2F).

G. Objetivos específicos

- Identificar y analizar políticas de seguridad de la información a tener en cuenta para el aseguramiento de activos de información
- Definir las variables que permitan seleccionar la mejor tecnología de doble autenticación que aplique en Colombia y que se encuentre dentro de los presupuestos de las PYMES
- Evidenciar las mejoras en el control de acceso mediante la implementación del doble factor de autenticación.

IV. MARCOS DE REFERENCIA

A. Marco conceptual

Biohacking

El término biohacking (biología do it yourself) nace de la unión de las palabras biología y hacking, que contextualmente se refiere a la gestión de la propia biología utilizando una serie de técnicas médicas, nutricionales y electrónicas con el objetivo de ampliar las capacidades físicas y mentales del sujeto.

Aseguramiento de información

Es el uso de medidas preventivas y reactivas y/o correctivas de las empresas y de los sistemas que permiten resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Aseguramiento de los activos de información

Es proteger todos los recursos de información que resulta fundamental para cualquier organización situación que suponga un riesgo o amenaza, según la norma ISO 27001 [12], [13].

Autenticación Biométrica (AB)

Se centra en los rasgos que, además de ser distintos en cada persona, no sufren variaciones a lo largo del tiempo, generalmente los dedos., siendo el análisis principal de los rasgos físicos o del comportamiento, de cada individuo, para autenticar su identidad [14] . Una de las más eficientes son las huellas dactilares. En el sentido literal y el más simple, la biometría significa la "medición del cuerpo humano [6]".

Biometría dactilar

Se basa en dispositivos que son capaces de leer, guardar e identificar los rasgos únicos de los individuos y así, verificar la identidad de un sujeto, para de esta manera identificar los elementos

morfológicos que sólo se dan para ese único sujeto. Es decir que la AB recopila información acerca de un rasgo distintivo (su voz, su huella dactilar), para más tarde comparar este dato con otro, y poder comprobar si son iguales o no, siendo fundamental la determinación de los rasgos distintivos que identifican sin lugar a error a cada persona. En este sentido, desde hace décadas se acepta comúnmente que rasgos como la huella digital, el iris del ojo o la voz son únicos para cada persona y completamente válidos para la automatización de la AB, y otros rasgos menos conocidos o que implican mayores dificultades para la suplantación son: el sistema venoso de la retina, los rasgos de la cara o la forma de las manos.

Autenticación de doble factor (A2F) o en dos pasos

La autenticación de doble factor, es el proceso en el que se combinan dos factores de autenticación posibles. Aportando una capa adicional a la seguridad, y asegurándose de que el usuario es quien dice ser. La categoría en las que un mecanismo puede pertenecer y ser considerado como forma de autenticación son:

- Lo que se sabe.
- Lo que se tiene.
- Lo que se es.

Considerando además otras dos categorías poco implementadas como lo son:

- Lo que hago
- Donde estoy

Autenticación de múltiple factor (AMF)

La autenticación multifactorial o (MFA) es un sistema que requiere más de una forma de autenticación para verificar la legitimidad de un individuo, en el cual el usuario verifica su identidad con una combinación de 3 factores y de esta manera hacer que sea más difícil para una persona no autorizada acceder.

Autenticación offline

Las aplicaciones offline son aplicaciones parcialmente conectadas, son aplicaciones autónomas. Si se pierde esa conexión mediante alguna vial la aplicación va a seguir funcionando y posterior la sincronización entrara en marcha. Entonces decimos que son aplicaciones que funcionan en todo momento, ya sea que tengan o no tengan conexión, y que acceden a datos locales con la posibilidad de ejecutar lógica compleja del lado del dispositivo.

Combinación biometría con NFC

Como objetivo de proteger determinadas aplicaciones, son utilizadas técnicas biométricas en dispositivos del común como teléfonos inteligentes(Smartphone). Como ejemplo, la tecnología NFC (Near Field Comunication) integrada en los Smartphone para realizar pagos, y existen aplicaciones que combinan esta tecnología con la biometría para comprobar la identidad del usuario.

B. Marco teórico

Es importante exponer y definir el significado de biometría y seguridad biométrica como un sistema de seguridad. Dicho esto, La biometría es la ciencia del análisis de las características físicas o del comportamiento, propias de cada individuo, con el fin de autenticar su identidad. La biometría funciona sobre la base del supuesto de que ciertos rasgos físicos o conductuales son únicos al individuo, ya sea por sí solos o en combinación con otros; y a partir de estos datos, transformados en una plantilla (la representación digital de este rasgo), se crea la posibilidad de la identificación o la autentificación del individuo. La autentificación, o el modelo biométrico de uno contra uno, consisten en comparar uno o más rasgos de un individuo con una plantilla correspondiente a la identidad de ese mismo individuo, es decir, es un proceso mediante el cual se verifica la declaración de identidad hecha por una persona en cuyo poder reside, por ejemplo, un carnet de identidad. La identificación, por su parte, es una comparación de uno a muchos, lo que significa que requiere una base de datos que contiene los rasgos biométricos de un grupo determinado de individuos, almacenados en una base de datos centralizada, con la finalidad de: a) determinar si el individuo en cuestión se encuentra en esa base de datos (por ejemplo, en un modelo de entrega de servicios asistenciales), o b) identificar quién es el individuo dentro del rango de esa base de datos (por ejemplo, en el caso de la búsqueda de un sospechoso en una base de datos de antecedentes penales). Durante las últimas décadas, países desarrollados y en desarrollo han impulsado la adopción de tecnologías de reconocimiento biométrico para un amplio rango de fines, desde avanzar planes de identificación universal de la población hasta llevar a cabo procesos electorales o facilitar la entrega de servicios básicos y asistenciales. Los sistemas basados en la identificación biométrica son vistos como un mecanismo más seguro para garantizar la identificación legal de un individuo, y mientras los mecanismos analógicos de reconocimiento –como las huellas digitales convencionales– han sido usados desde mucho antes del desarrollo de las tecnologías digitales, el crecimiento de la adopción de sistemas biométricos se debe a la evolución acelerada del sector tecnológico. Cualquier característica, biológica o de comportamiento, puede ser empleada como identificador biométrico, siempre que cumpla con cuatro requisitos básicos:

- La coleccionabilidad, o la posibilidad de ser medido.
- la universalidad, o la existencia del elemento en todas las personas.
- la unicidad, o el hecho de que el elemento sea distintivo a cada persona.
- la permanencia del elemento en el tiempo.

Según un estudio de la universidad militar nueva granada [14] ,al realizar un análisis de la huella dactilar como un método de identificación para la restricción o permitir el acceso a un lugar sistema determinado se puede resaltar la importancia que se ha dado dentro del sector de seguridad, empresarial, impidiendo suplantaciones e infiltraciones que traen como consecuencia fuga de información y pérdida de recursos tangible e intangible como los pueden ser loa cativos de información sensible de una organización y los que esta almacenados en un sistema lógico.

El sistema biométrico dactilar es el sistema de acceso más utilizado donde los avances en la identificación de la huella han abierto un gran campo en el área de la seguridad. Mucho sistema requiere el ingreso y salida masivos de personal a instalaciones en donde algunas personas deben acceder o ser restringidas, como también el personal debe realizar el ingreso a lugares donde se tienen activos de información demasiado sensible de la organización los cuales por medio de algún sistema se pueden permitir o denegar y es donde las herramientas de identificación dactilar presentan una solución a este problema. Es importante aclarar que ningún sistema de acceso es 100% seguro todos poseen un índice de vulnerabilidad, pero también hay unos más robustos que otros, en el reconocimiento dactilar se pueden encontrar falencias al momento de realizar la verificación.

A continuación, se muestra una tabla con el resumen de las ventajas y desventajas de las técnicas biométricas más usadas al día de hoy (ver **Error! Reference source not found.**).

Tabla 2 Registros biométricos

	VENTAJAS	**Desventaja**
Rostro	Cómodo, fácil, rápido, barato	Uso de tecnología de alta calidad Garantizar la iluminación del artefacto.
Huella	Muy madura, segura y económica	Posibilidad de falsificación por diferentes técnicas
Iris/Retina	muy seguro y detección de vida	Tecnología especifica Poca aceptabilidad
Venas	Detección de vida, muy seguro y coste medio	Aceptabilidad del usuario
Geometría	Fácil uso y bajo coste	Lento y poco seguro
Firma	Muy barato	bajo índice de similitud Demasiado robusto
Voz	Barato y necesario para telefonía	Lento, reproducible

Seguridad de los activos de información de una organización.

La seguridad de la información, según ISO 27001, consiste en la preservación de su triada para los sistemas implicados en el tratamiento de la información dentro de una organización [15]. Así pues, estos constituyen la base en la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada de manera adecuada, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización [15], desde un enfoque de riesgo empresarial. En esto se basa el Sistema de Gestión de la Seguridad de la Información SGSI. Se entiende por información todo el conjunto de datos que da valor a una empresa, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración [8].

Identificación biométrica

Consiste en determinar la identidad de una persona. El objetivo es capturar un elemento biométrico, por ejemplo, tomando una foto del rostro, grabando la voz, o capturando una imagen de la huella dactilar. Luego, esos datos se comparan con los datos biométricos de otras varias personas, alojados en una base de datos [9].

Autenticación biométrica

También conocida como verificación, es el proceso por el que se comparan los datos de las características de una persona con la "plantilla" biométrica de esa persona, con el fin de determinar su semejanza. En primer lugar, el modelo de referencia se almacena en una base de datos o en un

elemento seguro portátil, como una tarjeta inteligente. Luego se comparan los datos almacenados con los datos biométricos de la persona para autenticarse. Aquí, lo que se está verificando es la identidad de la persona [10].

C. Marco jurídico

Ley 1581 de 2012

La ley de protección de datos personales – Ley 1581 de 2012 – es una ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales [21] [17] para mayor información ver (anexo 1)

Ley 1341 de 2009

Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. [23][18] Para mayor información(ver anexo 2).

Resolución 76434 de 2012

Resolución número 76434 de 2012, por la cual se deroga el contenido del Título V de la Circular Única de la Superintendencia de Industria y Comercio, sobre Acreditación, y se imparten instrucciones relativas a la protección de datos personales, en particular, acerca del cumplimiento de la Ley 1266 de 2008.[25] [19] Para mayor información (ver anexo 3).

Decreto 1727 de 2009

Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información [27][20].

Decreto 2952 de 2010

Que dicha Ley Estatutaria tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 ibídem. [29] [21] Para mayor información (ver anexo 4).

Decreto 1377 de 2013

Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1°, tiene por objeto "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma". [31] [22], para mayor información (ver anexo 6).

Decreto 886 de 2014

La inscripción se realizará de manera independiente, cada una de las bases que contengan datos personales sujetos a tratamiento. Por ejemplo, una empresa deberá registrar la base de datos de sus clientes, y de sus empleados [33] [23], para mayor información (ver anexo 7.)

DECRETO 090 DE 2018

El Gobierno Nacional expidió el Decreto 090 del 18 de enero de 2018, en el cual reduce el universo de personas jurídicas obligadas a inscribirse en el Registro Nacional de Bases de Datos de la Superintendente de Industria y Comercio. [35][24] Para mayor información (ver anexo 8).

LEY 41 DE 2002 de España

La Ley 41/2002 Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Sanitaria, reglamenta cuestiones que la Ley General de Sanidad de 1986 trataba de forma insuficiente, como el derecho a la información sanitaria, el consentimiento informado, la documentación [37] [25], para mayor información (ver anexo 9).

Norma ISO-27001

La norma ISO es un estándar internacional orientado a los sistemas de gestión de seguridad de la información en las empresas. La alta competencia internacional acentuada por los procesos globalizadores de la economía y el mercado y el poder e importancia que ha ido tomando la figura y la opinión de los consumidores, ha propiciado que dichas normas, pese a su carácter voluntario, hayan ido ganando un gran reconocimiento y aceptación internacional. [39][26], para mayor información (ver anexo 10)

D. Marco geográfico

Para el sector de las PYMES Tecnológicas en la empresa INTELIBPO S.A.S la cual está ubicada en el barrio la castellana, dirección Cl. 93 ## 45a - 13, Bogotá, Cundinamarca. (Ilustración 4Error! Reference source not found.).

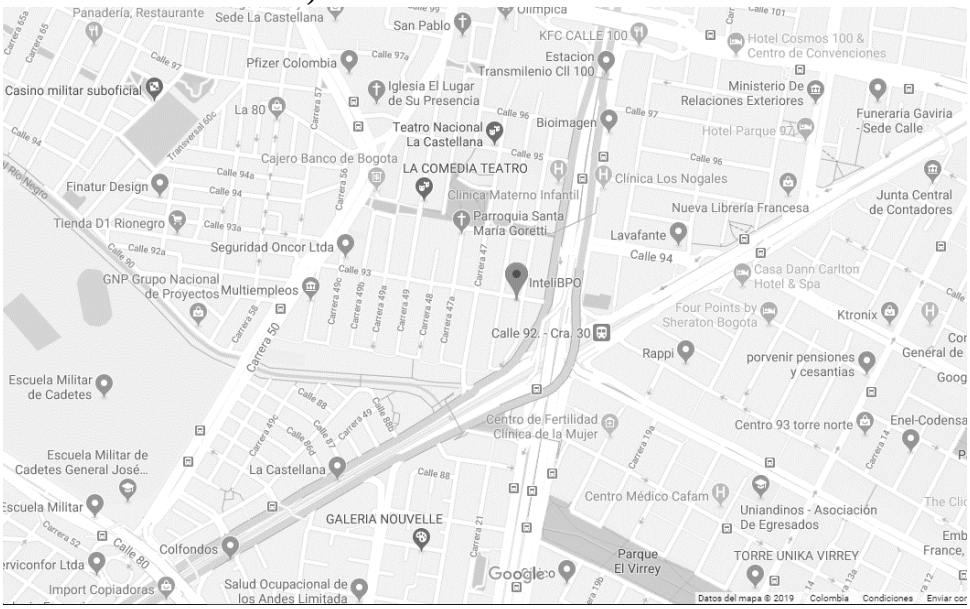


Ilustración 4Marco Demográfico Empresa

E. Marco demográfico

La Empresa INTELIBPO S.A.S ubicada en el sector de la Castellana con 50 empleados en donde la muestra será realizada con un (1) usuario voluntario para el proyecto BIOHACKING PARA LA PROTECCION DE LOS ACTIVOS DE INFORMACIÓN EN LAS PYMES POR MEDIO DE UN SISTEMA DE DOBLE FACTOR DE AUTENTICACION

V. METODOLOGÍA

A. Fases del trabajo de grado

Las fases en las cuales se va a desarrollar el proyecto de seguridad biométrica de doble factor son:

- En la fase de Gerencia de Proyecto: Se realizará la gestión del proyecto desde su formalización con el Acta de constitución del proyecto, su ejecución soportada en los diseños de la EDT y los cronogramas, monitoreo y control, frente a las líneas base de tiempo y costo, hasta su finalización.
- En la fase de diseño: Una vez aprobado el proyecto se diseñará el control para la implementación de la tecnología Biométrica con el Microchip NFC para el protocolo de doble autenticación
- En la fase de implementación: se procederá a realizar la instalación del A2F en el área indicada por la empresa.
- En la fase de documentación: se llevará un registro del proyecto en sus diferentes fases y sus avances.
- En la fase de cierre: Los entregables y sus resultados para el cumplimiento de los objetivos

del proyecto.

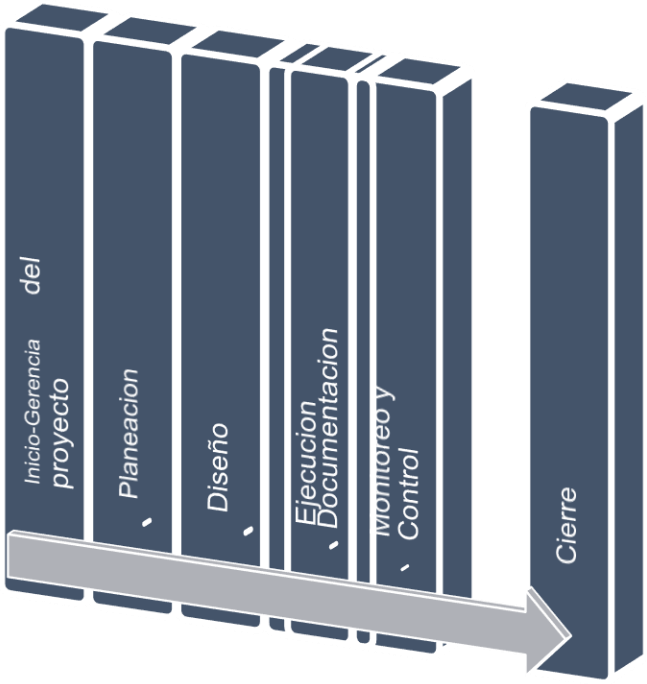


Ilustración 5Fases del Proyecto

B. Instrumentos o herramientas utilizadas

- MS Project 2013
- Dispositivo lector Biométrico Dactilar
- NFC micro Chip ISO 14443ª
- Jeringa ISO11784
- Dispositivo Biométrico Anviz VF30
- Tarjeta de Proximidad Anviz VF30
- Electro Imán

C. Población y muestra

Dirigido a las PYMES en Colombia con la empresa Piloto INTELIBPO S.A.S, y con la muestra de 1 voluntario, de 50 empleados que la conforman.

D. Alcances y limitaciones

Alcances

- No se realizará la implementación de ningún estándar o norma o librería para la implementación, solo se gestionarán sugerencias acordes al proyecto.
- Se trabajará bajo los lineamientos y políticas implementados por la compañía, de ser el caso se brindarán sugerencias que no alteren el SGS de la compañía
- El proyecto está enfocado a una sección específica física de la empresa. la cual está centrada en el lugar donde se fija el recurso (equipos, servidores, medios de almacenamiento) que alojan la información del procedimiento y/o la gestión del negocio
- Se entregará a la organización el modelo un prototipo del A2F establecido de: un (1) lector Biométrico dactilar y un (1) microchip subcutáneo
- Se entregará el proyecto A2F funcional acorde a las políticas, objetivos de la empresa
- Se brindará el soporte del proyecto de A2F durante los 2 meses de la fase de implementación del proyecto
- No se realizará la labor del implante del microchip se procederá a tercerizar
- No se rediseñará el modelo de seguridad informática a excepción del área identificada
- No se desarrollará políticas o procedimientos para el SGSI

Limitaciones

- Que no genere impacto la implementación del A2F
- Que los dispositivos biométricos usados no toleren el A2F
- Que las políticas de seguridad establecidas no sean ajustables al A2F
- Que cierre la compañía
- Que se corte el presupuesto por acciones forzosas
- Que la tecnología usada no sea competente
- Que el presupuesto no alcance para la adquisición de los dispositivos propuesto a implementar implementados.

VI. PRODUCTOS A ENTREGAR

A continuación, se van a describir los productos por los responsables del proyecto.

- Documento con los casos de éxito de intrusión física en las áreas sensibles de información vs el resultado de la implementación del A2F de los casos de éxitos de intrusión.
    - Con este documento se planea evidenciar el impacto en seguridad que se obtuvo a la hora de implementar el A2F.
- Análisis de SGSI en la PYME INTELIBPO S.A.S .si es necesario se realizarán (recomendaciones y/o Sugerencias):
    - Estudio de los estándares o políticas implementadas en la compañía para la protección de sus activos de información
- Documentación de las ventajas y desventajas de la implementación del sistema A2F:
    - Documento de apoyo para proyectar los pros y los contras de la implementación de un sistema A2F en la empresa INTELIBPO S.A.S,
- Investigación de los protocolos y políticas a utilizar en la implementación de un sistema 2AF para el aseguramiento de los activos de información.
    - Estudio de los estándares o políticas implementadas en la compañía para la protección de sus activos de información
- Encuesta para identificar el doble factor más acorde para los usuarios y conformar el A2F. (Análisis de las encuestas).
    - Se busca determinar mediante un estudio cual es el método que mejor se adapta a los usuarios de la compañía
    -
- Documento de implementación:
    - Documento de registro y procedimiento de la Implantación del sistema A2F del proyecto.
- Trabajo de grado:
    - Documento donde se verá refleja todo el proceso del proyecto desde la fase de inicio hasta su fase de cierre.

A continuación se presentaran lo resultado obtenidos para los entregables.

VII. ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

En este punto se desarrolló el esquema que se ha dado durante el transcurso del proyecto para mostrar el contenido de la investigación. De forma resumida, se describirán los aspectos abordados a lo largo del proyecto, los resultados obtenidos y su análisis. Todo ello se recoge en el compendio de publicaciones que acompaña el proyecto. Se construye aquí un hilo argumental que facilita la presentación y el análisis del proyecto. La conexión entre el tema tratado en cada capítulo y la publicación o las publicaciones en las que aparece se irán mencionando mediante las oportunas referencias. Dando continuidad se detalla el proceso del proyecto de la siguiente manera.

Para InteliBPO S.A.S, empresa que accedió a la implementación de este proyecto en la cual se realizaron pruebas para identificar la cantidad de personal interno y/o externo, que podía acceder a las áreas con información sensible de la empresa considerados, así como casos de éxito en intrusión.

De esta manera se logran evidenciar las brechas que existían en el sistema de gestión de Seguridad de la Información en adelante (SGSI) de la empresa.

Con el apoyo de gerencia se aplicó la estrategia de no supervisión presencial, y apoyados por el circuito cerrado de televisión (CCTV) de seguridad de la empresa a las áreas de información sensible, se evidencio que todo el personal interno sin importar su cargo o privilegios, y externo sin relación directa al área podía acceder e interactuar con los activos de información. Para mayor detalle de los resultados (ver anexo 11).

A continuación, se darán a conocer los principales hallazgos de las pruebas realizadas:

1. No poseen controles y/o herramientas robustas para el control de accesos
2. No existen mecanismos funcionales de validación, autorización y seguimiento para el control de acceso
3. La herramienta de seguridad y control de acceso es una cerradura de llave convencional
4. La herramienta de registro y seguimiento es una planilla alimentada de manera manual que frecuentemente es evadida.

Como resultado se evidencia el estudio de técnicas, mejores prácticas, normas, controles, herramientas y/o políticas a mejorar y/o implementar en el SGSI de la empresa, para garantizar la protección de los activos de información.

Con los resultados obtenidos en el estudio de casos de éxito de intrusión física, se realizó el estudio y análisis del (SGSI), para identificar las fortalezas y/o debilidades de las políticas y/o controles establecidos en la empresa que permitan la implementación o mejora de los controles de acceso para la puesta en marcha de un sistema de doble factor de autenticación (A2F), siguiendo el principal objetivo de establecer y mejorar el (SGSI), para controlar y conservar la confidencialidad, integridad y disponibilidad de la información dentro de la empresa. Alineados a las buenas prácticas de la norma IEC/ISO 27002 en la sección 11 control de accesos, se comparó con el SGSI de la empresa, donde se identificó que no es lo suficientemente apropiado para la

protección de los activos de información, por su bajo nivel de aplicabilidad y definición en los controles. Llegando a la conclusión de mejorar los mismos y/o las políticas, dar mejora al control de accesos para observar a detalle los hallazgos del análisis de SGSI de la empresa (ver anexo 12).

Se dan a conocer los principales hallazgos que se evidenciaron durante el análisis:

1. No poseen mecanismos de autenticación en las áreas críticas de tratamiento de información.
2. El control de acceso físico al área de operaciones es una cerradura de llave universal
3. No hay segregaciones de roles para el acceso al área de operaciones.
4. El seguimiento del personal para acceso al área de operaciones es realizado por medio de una planilla alimentada y realizada de manera manual.

Posterior al estudio del SGSI de la empresa, se procedió con el estudio de las ventajas y desventajas de los factores para la implementación de un sistema de doble factor de autenticación (A2F), y de esta manera conocer, identificar y aplicar los mecanismos, técnicas y herramientas en el A2F. Mediante diferentes asesorías, consultas, análisis de estudios se tuvieron en cuenta los aspectos tecnológicos, culturales y económicos, como se observa en la (tabla 4).

Para ver el estudio general de las ventajas y desventajas de las categorías para los factores de seguridad (ver anexo 13).

Tabla 3 Categorías factores de seguridad

Factor	Tipo	Ventajas	Desventajas
Lo que tengo	Token. Tarjetas de proximidad. Microchip RFID.	Fácil adquisición. No requiere de gran presupuesto. Gran porcentaje de aceptabilidad. Fácil enrolamiento con diferentes. Dispositivos tecnológicos.	Fácil de interceptar. Exclusividad. Diseño.
Lo que se	Contraseñas. Patrones. Palabras.	No genera gran costo. Fácil implementación. Universalidad. Aplicabilidad. No genera costos adicionales. Administración de la seguridad.	Fáciles de interceptar. Cambio constante. Varía su seguridad de acuerdo al rango.
Lo que soy	Huellas. Rasgos. ADN.	Patrón único de validación de autenticidad. Aumenta los protocolos de seguridad. No genera costos de adquisición. Confiabilidad. Aceptabilidad.	Costes para dispositivos lectores. Genera costos de implementación. Dependiente dela condición física de la persona.
Donde estoy	Donde estoy.	Anticipación de destinos para protocolos de seguridad. Robusto para interceptar.	Grandes costes para dispositivos de verificación y validación. Poco porcentaje de aceptabilidad por parte del personal. Poco porcentaje de confiabilidad por parte del personal.

Lo que hago	Acciones del día a día Tareas programadas.	Algoritmos de estrategia. Fortalece los controles de seguridad.	Fácil de predecir propenso a interceptación. Requiere de gran presupuesto para implementación. Poco porcentaje de aceptabilidad por parte del personal. Poco porcentaje de confiabilidad por parte del personal.

Fuente: Autores.

En base a la información de la (tabla 4), cada grupo debe cumplir con una serie de requisitos como lo es:

- La universalidad
- La unicidad
- La permanencia
- La Evaluabilidad
- La aceptabilidad
- El rendimiento

Siguiendo estos requisitos se identificaron los factores que mejor se adaptan y cumplen con las políticas de la empresa, el cual da como resultado la selección de las categorías más universales y adoptadas como el que tengo, que se y que soy para la implementación del sistema A2F.

En base a las conclusiones del análisis del SGSI de la empresa, y los resultados de las ventajas y desventajas de la implementación del A2F, se da continuidad al estudio de los controles, protocolos y/o políticas a mejorar o implementar, y así identificar una solución general que no afecte los objetivos de la empresa y de sus colaboradores.

Basados en la definición de la norma IEC/ISO 27002 para el control de acceso donde especifica que: “Los controles de acceso son tanto lógicos como físicos y se deberían considerar en conjunto.”, fueron adoptados los siguientes ítems de la norma:

1. 11.2.1. Registro de usuarios
2. 11.2.4. Revisión de los derechos de acceso de usuario
3. 11.3.1. Uso de contraseñas
4. 11.5.2. Identificación y autenticación de usuario
5. 11.5.4. Uso de los recursos del sistema
6. 11.6.1. Restricción de acceso a la información
7. 11.6.2. Aislamiento de sistemas sensibles

De acuerdo a los ítems mencionados anteriormente se identificaron los controles a ser aplicados al SGSI de la empresa, los cuales se dan a conocer a continuación.

- Como factor biométrico principal se considera la huella a excepción de las personas cuya condición física lo impida
- Como factor secundario será considerada la retina ocular a excepción de las personas cuya condición física lo impida
- Como factor principal externo de autenticación será considerado el microchip sub dérmico siempre y cuando la persona sea informada previamente y conozca todo lo posible respecto al tema
- Como factor secundario externo de autenticación será considerada la tarjeta de proximidad.

De igual manera se dan a conocer las políticas identificadas y a ser aplicadas al SGSI durante el estudio:

- Solo tendrá acceso a la información el personal calificado y autorizado, a excepción de roles como CEO.
- Implementar los controles correspondientes de accesos (físico, lógico), para garantizar la confidencialidad, disponibilidad, integridad de la información.
- Todo acceso al personal interno y/o externo que no tenga relación directa con las áreas sensibles de tratamiento y control de información debe estar aprobado con anterioridad por el CEO o su representante.

Dando como resultado la mejora a las políticas y controles del SGSI de la compañía. Para información detallada de las políticas y controles identificados y aplicados en el estudio a implementar (ver anexo 14).

En base a los resultados de las mejoras a los controles y/o políticas, se realizó una encuesta al personal de la empresa con un total de 50 empleados, planteando 4 alternativas para la implementación al control de acceso y A2F. Para ver a detalle el contenido de las propuestas planteadas (ver anexo 15).

A continuación, se dan a conocer de manera general las propuestas para el A2F.

- Biometría dactilar + Token
- Biometría dactilar + Tarjeta proximidad
- Biometría dactilar + Contraseña
- Biometría dactilar + Chip NFC Subcutáneo

Como resultado de la encuesta, se evidencia la elección de 3 alternativas para la implementación del sistema A2F, como se observa en la (Ilustración 6), el 49% de los empleados que aplicaron a la encuesta indicaron que el A2F más apropiado para la protección de activos de información es el de biometría dactilar + chip NFC subcutáneo, para ver de manera detallada el resultado de la encuesta (ver anexo 16).

Ilustración 6 Resultado encuesta selección A2F

En base a los resultados de la encuesta, se realizó el análisis a diferentes herramientas tecnológicas, para identificar aquellas que cumplen con los estándares. Y, alineados a las categorías de los factores de autenticación como se detallaron en la (tabla 3) para la implementación del A2F.

Mediante una extensiva evaluación de diferentes dispositivos tecnológicos de control de acceso, se consideraron solo aquellos que cumplieran como mínimo un 80% con las políticas y controles:

1. Su configuración debe permitir la integración de dos o más factores de seguridad
2. Su adquisición, configuración y mantenimiento no deben generar interrupciones operativas en la organización

En base a esto el lector Biométrico Anviz modelo VF30 se adapta perfectamente a los requerimientos de la empresa por su configuración, dado que:

1. Permite más de dos factores de autenticación, como se observa en la (ilustración 7).
2. La tecnología de identificación es NFC (Near Field Comunication).

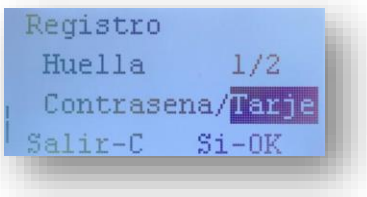


Ilustración 7Servicios autenticación usuario

A continuación, se dan a conocer las herramientas adquiridas para su implementación.

- Lector Biométrico marca Anviz VF30
- Microchip NFC ISO 14443A
- Tarjeta de Proximidad Anviz VF30
- Electro Imán
- Botón de salida Touch
- Software control de acceso AnvizVF30

Se procedió a la instalación del aplicativo como se observa en la (Ilustración 8,9), en el equipo de cómputo principal de Recursos humanos ya que es el área destinada a la administración del mismo. Y así, realizar la configuración de acuerdo a los cargos y roles ya establecidos por la empresa. basados en los perfiles suministrados por la misma, se identificaron 3 categorías principales y sus respectivas subcategorías expuestas a continuación;

- Administrador
  - General
  - Especifico
- Administrativo
  - Líder
  - Responsable
- Operativo
  - Líder
  - Responsable

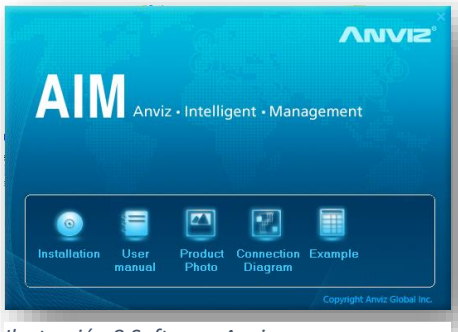


Ilustración 8 Software Anviz

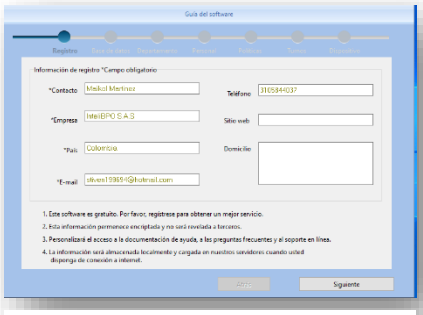


Ilustración 9 Opciones de instalación software Anviz

Una vez registradas las categorías y subcategorías en el aplicativo para el control de acceso, se realiza el cargue de los empleados siguiendo la plantilla que ofrece el mismo.

Departamento	Nro. de usuario	ID de usuario	Nombre	Rol	Fecha/Hora	Tipo de registro	Turno	Código de identificación	Identificación	Código de tarea	Dispositivo Nro.	Marcado
Tecnologia	1	1010	Maikol Martinez	Operativo N1	22/10/2019 7:42:08	In	Diurno	9	Tarjeta+Huella 1	0	1	False
operaciones	1	2020	Erik Cifuentes	Administrador	22/10/2019 8:25:30	In	Diurno	1	Huella 1	0	1	False
Administrativo	1	3030	Carmen Forero	Operativo N2	22/10/2019 8:25:40	In	Diurno	1	Huella 1	0	1	False
Desarrollo	1	4040	Sandra Aponte	Administrador	22/10/2019 8:29:29	In	Diurno	9	Tarjeta+Huella 1	0	1	False
Comercial	1	5050	Jazmin Castellanos	Operativo N1	22/10/2019 8:36:07	In	Diurno	9	Tarjeta+Huella 1	0	1	False

Ilustración 10 Plantilla cargue usuarios

Ya realizado el cargue del empleado se asignaron los permisos de acceso de acuerdo a su perfil.

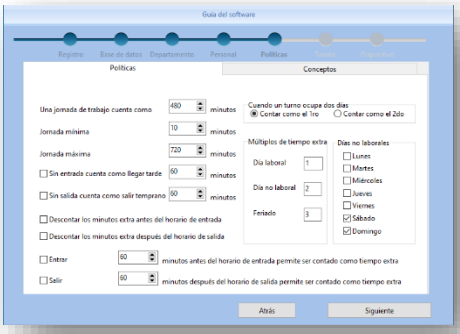


Ilustración 10 Opciones de configuración para el control de acceso

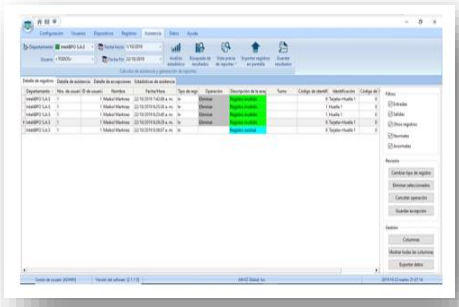


Ilustración 12 Registro del control de acceso

Una vez configurado el aplicativo, se validaron los accesos del personal. Para ver el detalle de la instalación y configuración del aplicativo (ver anexo 17).

se realizó un nuevo test de intrusión física al área de operaciones con un total de 5 intentos en diferentes días. Aplicando la estrategia de no supervisión presencial, y apoyados por el circuito cerrado de televisión (CCTV) de seguridad de la empresa. Se evidencio la mejora en el control de acceso al área, con 0 casos de éxito de ingresos no autorizados como se evidencia en el anexo 11, dejando como anotación que existen excepciones como lo son:

- El acompañamiento directo del responsable de área
- Formato de externos. firmado y aprobado por el responsable de área. y/o CEO.

Se identificaron lecciones aprendidas durante el proyecto como:

- Mejora continua de los controles para la seguridad los activos de información.
- Los alcances de las políticas no deben ser limitadas, pero si detalladas.

- La tecnología implementada no debe interferir con los objetivos de la empresa.

Oportunidades de mejora para los controles y políticas como:

- Definir la segregación de usuarios para el control de accesos.
- Implementar los controles correspondientes de acceso (físico, lógico) para garantizar la protección de los activos de información.

En cumplimiento al punto 6 numeral 7 de este documento, se realiza la entrega de un manual técnico. Denominado como (Anexo 17), para la empresa InteliBPO S.A.S como registro a futuras instalaciones o configuraciones del mismo.

Como conclusión general y en respuesta a la pregunta ¿Cómo incrementar la seguridad de los activos de información en las PYMES que son protegidos o resguardados bajo un sistema biométrico dactilar? Se identificó como buena práctica la implementación de un segundo factor de autenticación en los dispositivos de control de acceso, bien sea que incorpore la opción de varios métodos de autenticación o en conjunto de herramientas externas.
Siendo una de las estrategias y controles más adoptados por las PYMES en la seguridad de la información.

Estrategias de Comunicación y Divulgación

1. La Comunicación Interna:
    a. Correo
    b. Memorando de comunicación
2. La Difusión del Proyecto
    a. Marketing digital
    b. Divulgación del proyecto a PYMES aledañas
3. La Diseminación de los Resultados
    a. Participación en foros
    b. Publicaciones en Blogs

VIII. NUEVAS ÁREAS DE ESTUDIO

En la actualidad se mantienen dos fuentes muy importantes en el campo de investigación enfocadas al biohacking o human Augmentation como lo son:

1. La línea de investigación mediciones fisiológicas, morfológicas o biológicas. En los análisis morfológicos, consisten, principalmente, en las huellas dactilares, la forma de la mano, del dedo, el patrón de las venas, el ojo (iris y retina) y la forma de la cara. Los análisis biológicos, el ADN, la sangre, la saliva o la orina pueden usarse por parte de los equipos médicos y la policía forense [27].
2. La Línea de investigación a mediciones del comportamiento. Son las formas más comunes como el reconocimiento de voz, la dinámica de la firma (velocidad de movimiento del bolígrafo, aceleraciones, presión ejercida, inclinación), la dinámica de la pulsación de las teclas, la manera en que se utilizan los objetos, la marcha, el sonido de los pasos, los gestos, etc. Las diferentes técnicas utilizadas son objeto de investigación y desarrollo constante, y, por supuesto, se mejoran continuamente.

IX. CONCLUSIÓN

En base a la revisión bibliográfica consultada durante el transcurso del proyecto, permitió el análisis de diferentes técnicas y herramientas, y consideradas como factores de seguridad, de la cual se fue seleccionada la técnica denominada BIOHACKING. Mediante la metodología de encuestas. Se incluyó como la alternativa más adecuada para su implementación y aplicación a la empresa InteliBPO S.A.S. en las que se plantearon diversas alternativas en las encuestas, y su principal objetivo es permitir el enrolamiento con diferentes tecnologías de la empresa, y para la cual su aplicación es amplia, su estructura y facilidad de uso son amigables y no requieren de personal experto. Además, dispone de herramientas de evaluación. Aunque no se cuenta de una metodología para su aplicación.

X. REFERENCIAS

[1] M. R. Duarte, «alai,» 17 04 2018. [En línea]. Available: https://www.alainet.org/es/articulo/192321.

[2] colciencias, «GISIC,» enero 2010. [En línea]. Available: https://scienti.colciencias.gov.co.

[3] l. b. H. Huellas, «bbc,» [En línea].

[4] Ortega-Garcia, J. & Alonso-Fernandez, Fernando & Coomonte-Belmonte, R.. (2008). Seguridad Biométrica. , «Researchgate,» Seguridad Biometrica, mayo 2018. [En línea]. Available: https://www.researchgate.net/publication/280722075_Seguridad_Biometrica.

[5] Alex Hern, «theguardian,» 15 Nov 2018. [En línea]. Available: https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research.

[6] B. Ross, «DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent,» 0 Octubre 2018. [En línea]. Available: https://www.cse.msu.edu/~rossarun/pubs/BontragerRossDeepMasterPrint_BTAS2018.pdf. [Último acceso: 25 Octubre 2018].

[7] TuSitioWeb, «TuSitioWeb,» 2017.

[8] «ABC Moviles,» Los hackers pueden «copiar» las huellas dactilares a partir de una fotografía, [En línea]. Available: https://www.abc.es/tecnologia/moviles-telefonia/20141229/abci-copiar-huellas-dactilares-fotos-201412291139.html. [Último acceso: 30 12 2014].

[9] BBC Mundo , «Info Security NJEWS,» Febrero 2017. [En línea]. Available: http://www.infosecurityvip.com/newsletter/hacking_feb17.html.

[10] Biometrics Intitute, «Biomtrics Institute,» [En línea]. Available: https://www.biometricsinstitute.org. [Último acceso: 10 10 2019].

[11] universidad veracruzana, «Seguridad de la Informacion Universidad Veracruzana,» [En línea]. Available: https://www.uv.mx/infosegura/. [Último acceso: 14 Diciembre 2016].

[12] «sgsi,» [En línea]. Available: http://www.iso27000.es/download/doc_sgsi_all.pdf.

[13] R. Eíto-Brun, Gestión de contenidos, Editorial UOC, 2013.

[14] Á. S. Calle, Aplicaciones de la visión artificial y la biometría informática, Dykinson, 2005.

[15] «gemalto,» 05 05 2019. [En línea]. Available: https://www.gemalto.com/latam/sector-publico/inspiracion/biometria.

[16] A. Maya Vargas, «Universidad Militar Nueva Granada,» Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida, [En línea]. Available: https://repository.unimilitar.edu.co/handle/10654/11168. [Último acceso: 17 Abril 2014].

[17] R. M. R. S. D. J. R. Gema Escrivá Gascó, Seguridad informática, Macmillan Iberia, S.A., 2013.

[18] D. L. Michael Howard, «19 puntos críticos sobre seguridad de software,» p. 305, 2017.

[19] «gemalto,» 05 03 2019. [En línea]. Available: https://www.gemalto.com/latam/sector-publico/inspiracion/biometria.

[20] «gamelto,» 05 03 2019. [En línea]. Available: https://www.gemalto.com/latam/sector-publico/inspiracion/biometria.

[21] Banco Caja Social, «Banco Caja Social,» Ley 1581 de 2012 Protección de Datos Personales, [En línea]. Available: https://www.bancocajasocial.com/abc-ley-1581-de-2012-proteccion-de-datos-personales.

[22] Congreso de la Republica, «ley 1581 de 2012,» 17 Octubre 2012. [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html. [Último acceso: 18 Octubre 2012].

[23] Secretaria Distrital de Hábitad, «Ley 1341 de 2009,» Secretaria Distrital de Hábitad, 30 Julio 2009. [En línea]. Available: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913. [Último acceso: 30 Julio 2009].

[24] Mintic, «Mintic,» [En línea]. Available: https://www.mintic.gov.co/portal/inicio/3707:Ley-1341-de-2009. [Último acceso: 29 Julio 2009].

[25] Sic, «Sic,» Resolucion Numero 76434 de 2012, 04 Diciembre 2012. [En línea]. Available: http://www.sic.gov.co/sites/default/files/normatividad/Resolucion_76434_2012.pdf. [Último acceso: 04 Diciembre 2012].

[26] www.sic.gov.co, «Resolución 76434,» 2012. [En línea]. Available: https://www.sic.gov.co/sites/default/files/normatividad/Resolucion_76434_2012.pdf. [Último acceso: 4 Diciembre 2012].

[27] Suin Juriscol, «Suin Juriscol,» DECRETO 1727 DE 2009, [En línea]. Available: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1338429. [Último acceso: 15 Mayo 2009].

[28] www.sic.gov.co, «Decreto 1727 de 2012,» 2009. [En línea]. Available: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1338437. [Último acceso: 16 Agosto 2012].

[29] Suin Juriscol, «Suin Juriscol,» DECRETO 2952 DE 2010, [En línea]. Available: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1503907. [Último acceso: 06 Agosto 2010].

[30] www.secretariadesenado.gov.co, «Decreto 2952 de 2010,» [En línea]. Available: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1503907. [Último acceso: 06 Agosto 2010].

[31] Gestor normativo , «Decreto 1377 de 2013,» Decreto 1377 de 2013, [En línea]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646. [Último acceso: 27 Junio 2013].

[32] TURISMO, MINISTERIOS DE INDUSTRIA Y COMERCIO, «DECRETO NÚMERO 1317 DE 2013,» MINISTERIOS DE INDUSTRIA Y COMERCIO, 27 junio 2013. [En línea]. Available: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf.

[33] «Derecho Informatico,» DECRETO 886 DE 2014. REGISTRO NACIONAL DE BASES DE DATOS, [En línea]. Available: http://derechoinformatico.co/decreto-registro-nacional-de-bases-de-datos/. [Último acceso: 13 mayo 2014].

[34] Juriscol, «DECRETO 886 de 2014,» 13 MAYO 2014. [En línea]. Available: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1184150.

[35] «Super Intendencia de Industria y Comercio,» Super Intendencia de Industria y Comercio, [En línea]. Available: https://www.sic.gov.co/gobierno-nacional-reduce-universo-de-obligados-a-cumplir-el-registro-de-bases-de-datos-ante-superintendencia-de-industria-y-comercio. [Último acceso: 18 Enero 2018].

[36] Ministrerios de Industria y comercio, «Decreto 090 de 2018,» 18 Enero 2018. [En línea]. Available: https://www.ccce.org.co/biblioteca/decreto-90-del-18-de-enero-de-2018-rnbd.

[37] «Boe,» Boe Legislacion Consolidada, [En línea]. Available: https://www.boe.es/buscar/pdf/2002/BOE-A-2002-22188-consolidado.pdf. [Último acceso: 15 Noviembre 2002].

[38] ley 41, «ley 41 de 2002 de España,» 14 Noviembre 2002. [En línea]. Available: http://www.isciii.es/ISCIII/es/contenidos/fd-investigacion/fd-evaluacion/fd-evaluacion-etica-investigacion/pdf_2015/Ley_41-2002_autonomia_del_paciente_texto_consolidado.pdf.

[39] «IsoTools,» Qué son las nomas ISO, [En línea]. Available: https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/. [Último acceso: 19 Marzo 2015].

[40] NORMA ISO 27001, «Normas ISO,» 25 Septiembre 2013. [En línea]. Available: https://www.normas-iso.com/iso-27001/.

[41] Brickley, L (Brickley, London), «Bodies without Borders The Sinews and Circuitry of "folklore+",» vol. 78, nº 5, p. 37, 2019.

[42] Universidad Autónoma de MAdrid, «Citas y elaboración de bibliografía: el plagio y el uso ético de la información: Estilo IEEE,» 26 07 2019. [En línea]. Available: https://biblioguias.uam.es/citar/estilo_ieee. [Último acceso: 29 07 2019].