

Universidad CENFOTEC

Maestría en Ciberseguridad

Documento Final de Proyecto de Investigación
Aplicada 2

NEUROQWERTY

Exponenciando la seguridad en paneles físicos

Brenes Umaña Erick Alfonso

Agosto 2020

Derechos de autor

En el presente documento queda prohibido la consulta y reproducción por un periodo de cinco años a partir del mes de agosto del 2020.

Dedicatoria

Mi principal dedicatoria se las doy a mis padres. Ellos me dieron todas las herramientas para llegar a ser la persona que soy hoy en día. A mi familia que siempre me apoyó en todo. A mis mentores que me han pasado su conocimiento y, en especial, a Yensy De La O, mi compañera de vida, quien me ha impulsado a seguir superándome y sobre todo quien ha creído en mí.

A todos ustedes, que sin su motivación este esfuerzo no hubiera brindado frutos.

Muchas gracias.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Erik Alfonso Brenes Umaña.**

M. Sc. Juan Matías Matías
Tutor

REBECA ESQUIVEL FLORES (FIRMA)
Firmado digitalmente por REBECA ESQUIVEL FLORES (FIRMA)
Fecha: 2020.08.31 08:26:05 -06'00'

M. Sc. Rebeca Esquivel Flores
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2020.08.31 16:29:05 -07'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 29 de agosto de 2020

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°.

Agradecimientos

El autor desea expresar su más sincero agradecimiento a los profesores de la maestría de ciberseguridad impartida por la Universidad CENFOTEC. En especial, al profesor Juan Matías, por su colaboración en la preparación de este manuscrito.

De igual manera, al Dr. Julio Mayol, quien junto al equipo del MIT empezaron el estudio del NEUROQWERTY, el cual representa la inspiración de este proyecto.

Contenido

Derechos de autor……3
Dedicatoria ……4
Agradecimientos ……6
Contenido……7
Lista de figuras……..11
Resumen……12
Introducción ……..18
1.1 Generalidades……20
1.2 Antecedentes del problema ……..20
1.3 Definición y descripción del problema ……21
1.4 Justificación ……..22
1.5 Viabilidad ……22
1.5.1 Punto de vista técnico ……22
1.5.2 Punto de vista operativo……23
1.5.3 Punto de vista económico ……23
1.6 Objetivos ……..24
1.6.1 Objetivo general……25
1.6.2 Objetivos específicos ……25
1.7 Alcances y limitaciones ……26
1.7.1 Alcances……26
1.7.2 Limitaciones ……27
1.8 Marco de referencia organizacional y socioeconómico……27
1.8.1 Historia ……27
1.8.2 Tipo de negocio y mercado meta ……29
1.8.3 Misión ……..29
1.8.4 Visión ……..29
1.8.5 Valores ……29

1.8.6 Políticas institucionales……30
2 Definiendo la seguridad ……32
2.1 Riesgos ……32
2.1.1 Riesgos organizacionales ……32
2.1.2 Riesgos personas ……..32
2.1.3 Riesgos de sistemas ……33
2.1.4 Riesgos en las características del lugar que vamos a proteger ….33
2.2 Controles ……34
2.2.1 Políticas de mantenimiento ……..34
2.2.2 Acciones ante bloqueo y fallos del sistema ……34
3 Estado de la cuestión ……36
3.1 Tipo de investigación……37
3.2 Alcance investigativo ……..37
3.3 Enfoque ……38
3.3.1 ¿Qué es el NEUROQWERTY y cómo funciona? ……...38
3.3.1.1 Sobre MIT-CS1PD ……40
3.3.1.2 Sobre PD_MIT-CS2PD ……42
3.3.1.3 Los resultados ……44
3.3.2 El nuevo dispositivo de control ……45
3.3.2.1 El Arduino ……46
3.3.2.2 Los sensores de fuerza ……47
3.3.2.3 Teclados mecánicos ……48
3.3.2.3.1 Spring Switch ……49
3.3.2.3.2 Tecnología ALPS ……50
3.3.2.3.3 Switches Mattias ……51
3.3.2.3.4 Cherry MX Switches……52
3.3.2.3.4.1 Cherry MX RED ……..53
3.3.2.3.4.2 Cherry MX Blue ……..54

3.3.2.3.4.3 Cherry MX Brown……54
3.3.2.4 Teclados de membrana……55
3.3.3 Los prototipos ……..……57
3.3.3.1 Prototipo con sensores ……57
3.3.3.2 Prototipo con teclado mecánico ……..59
3.3.4 Mejorando el prototipo con la seguridad informática ……..61
3.3.4.1 El proceso del sistema……61
3.3.4.2 La base de datos ……..65
3.3.4.2.1 Los controles en la base de datos……65
3.3.4.2.1.1 Inventario de tablas ……..66
3.3.4.2.1.2 Sensibilidad de los datos ……..67
3.3.4.2.1.3 Políticas de respaldos……68
3.3.4.2.1.4 Plan de recuperación ……69
3.3.4.2.1.5 Plan antirrobos de la información ……70
3.3.4.2.1.6 Cuentas fuera de uso ……71
3.3.4.2.1.7 Políticas de parches y actualización ……71
3.3.4.2.2 La nueva huella biométrica……..72
3.3.4.2.3 La semilla y el enmascaramiento de los datos……73
3.3.4.2.4 Las llaves públicas y privadas ……73
3.3.4.3 El código dentro del *Web Service* ……..74
3.3.4.4 El algoritmo de encriptación……...75
3.3.4.5 Las reglas del juego ……76
3.3.4.5.1 El aprendizaje de la huella biométrica……76
3.3.4.5.2 El tiempo de vida de los datos de usuario……77
3.3.4.5.3 Bitácora de errores de conexión ……..77
3.3.4.5.4 Bitácora de incidentes ……77
3.3.4.5.5 Reglas de los usuarios ……77
3.3.4.6 Módulo de administración ……78

3.3.4.6.1 Registro de dispositivos ……..79
3.3.4.6.2 Registro de usuarios…….80
3.3.4.6.3 Mantenimiento de los usuarios ……80
3.3.4.6.4 Manejo de los usuarios bloqueados …….81
3.3.4.6.5 Manejo de fallos ……..81
3.3.4.6.6 Manejo de datos antiguos ……82
Conclusiones ……83
Recomendaciones …….84
Bibliografía ……..85

Lista de figuras

Figura 1. Representación gráfica de las dinámicas de pulsación de teclas 39
Figura 2. Gráfica de porcentaje-tiempo de la afectación de la enfermedad 40
Figura 3. Resultado de las pruebas 1 42
Figura 4. Resultado de las pruebas 2 43
Figura 5. Histograma circular del estado de deterioro psicomotor 44
Figura 6. Diferentes modelos dentro de la gama de los Arduino 47
Figura 7. IBM PC 5150 con teclado 49
Figura 8. Diseño del modelo Spring Switch 50
Figura 9. Los 11 componentes para crear una tecla ALPS 51
Figura 10. Plano de un interruptor para switches Mattias 52
Figura 11. Comparación de pulsaciones de los Cherry 53
Figura 12. Visualización gráfica del funcionamiento del Cherry MX Red 54
Figura 13.Visualización gráfica del funcionamiento del Cherry MX Black 54
Figura 14. Visualización gráfica del funcionamiento del Cherry MX Brown 55
Figura 15. Modelo de estándar de un diseño de teclado de membrana 56
Figura 16. Diseño del prototipo con sensores 58
Figura 17. Desarrollo del prototipo con sensores 59
Figura 18. Desarrollo del prototipo con teclado mecánico. 61
Figura 19. Diseño de procesos 62
Figura 20. Capa de presentación 63
Figura 21. Capa de Lógica (Web Services) 64
Figura 22. Modelo entidad relación 66

UNIVERSIDAD CENFOTEC

Resumen

EXPONENCIANDO LA SEGURIDAD EN PANELES FÍSICOS

POR ERICK BRENES

Presidente del comité supervisor: Juan Matías

Esta tesis es presentada como propuesta para una nueva generación de dispositivos perimetrales inteligentes (paneles físicos), con base en parte del estudio del NEUROQWERTY; estudio científico-médico que explica la relación entre el uso diario de las computadoras o dispositivos móviles para la detección temprana de enfermedades degenerativas.

Por esta razón, nace la idea de unir estos estudios con algo ya existente: la seguridad perimetral. Por lo tanto, se plantea una solución utilizando un teclado mecánico, una base de datos relacional (*machine learning*) y el estudio del NEUROQWERTY (un algoritmo que representará el estudio). El proyecto propone la documentación y esquemas para la elaboración de un prototipo funcional.

Tras el proceso de investigación, se muestra que la propuesta e implementación de este proyecto es algo ambicioso, pero factible de realizar. Su objetivo principal es minimizar la vulnerabilidad actual de los dispositivos de panel físico; además, como objetivo secundario, se visualiza permitir la persistencia de varios usuarios con sus claves respectivas y la creación de bitácoras.

Palabras clave: investigación, NEUROQWERTY, seguridad, perimetral, innovación, protección, mejora, vulnerabilidad.

Glosario

ID	Palabra	Descripción
1	Activo	Son los bienes, derechos y otros recursos de los que dispone una empresa. Estos pueden abarcar muebles, construcciones, equipos informáticos o información.
2	Algoritmo	Conjunto de instrucciones definidas y no ambiguas, ordenadas y finitas diseñadas para llegar a la solución de un problema.
3	Arduino	Es una plataforma de desarrollo basada en una placa electrónica de *hardware* libre que incorpora un microcontrolador programable y una serie de pines hembra.
4	Base de datos relacional	Recopilación de elementos de datos con relaciones predefinidas entre ellos. Estos elementos se organizan como un conjunto de tablas con columnas y filas.
5	Base de datos	Lugar de almacenamiento del conjunto de información que se registrara sobre los usuarios; además, puede ser extendido para la creación de métricas y alertas tempranas.
6	Bitácora	Documento en el cual se hace registros de incidentes relacionados con un sistema. Cada registro debe tener como mínimo fecha, hora, código de error y una descripción.
7	Brecha de seguridad	Es un suceso que ocasiona destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.
8	*Core*	Palabra proveniente del inglés que significa centro. En este proyecto es la parte central del sistema.
9	Criptografía asimétrica	Es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje.

10	Dinamómetro	Es un instrumento utilizado para medir fuerzas o para calcular el peso de los objetos.
11	Dispositivos perimetrales	Son todos los componentes electrónicos o mecánicos que se utilizan para la protección del perímetro de un lugar.
12	Encriptación	Técnica que utiliza un algoritmo especial para la protección de datos sensibles, haciendo una conversión para imposibilitar la lectura de los datos.
13	Falsos negativos	Es un error que se da tras efectuar una prueba. El resultado de dicha prueba otorga un valor que no es el correcto.
14	*FrontEnd*	Es la parte del sistema que se encarga de la interacción con el usuario.
15	Huella biométrica	Estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos, mas no mecánicos.
16	Investigación exploratoria	Es un primer acercamiento al problema que se pretende estudiar y conocer. Estas se realizan para conocer el tema que se abordará, lo que nos permitirá "familiarizarnos" con algo que hasta el momento desconocemos.
17	*Machine learning*	Capacidad de un sistema de aprender del usuario sobre la marcha.
18	Microcontrolador	Es un circuito integrado programable, capaz de ejecutar las órdenes grabadas en su memoria.
19	MySQL	Es un sistema de gestión de bases de datos relacional.
20	NEUROQWERTY	Estudio científico-médico que explica la relación entre el uso diario de las computadoras o dispositivos móviles para la detección temprana de enfermedades degenerativas.
21	Panel físico de entrada de datos	Este tipo de dispositivo se utiliza para permitir o denegar el acceso de las personas a sistemas de información.

22	PD	*Parkinson's dissease* o enfermedad de Parkinson.
23	*Protoboard*	Es una especie de tablero con orificios, en el cual se pueden insertar componentes electrónicos y cables para armar circuitos. Normalmente, sirve para experimentar con circuitos electrónicos; es de uso temporal.
24	Proximidad	Es la propiedad de detectar objetos o señales que se encuentran cerca de ellos.
25	*Raspberry*	Es una computadora de placa simple y de bajo costo, desarrollada en el Reino Unido.
26	*Rayleigh*	Es un análisis muy específico para datos direccionales y se emplea con éxito en muchos campos científicos, que van desde la física hasta la neurociencia.
27	Respaldo	Es una copia fidedigna de un dato, siendo esta una copia exacta de dicho valor inicial.
28	Robustez	Capacidad para hacer frente a errores mientras se está ejecutando.
29	RPO	*Recovery point objective*: máximo periodo de tiempo tolerable de pérdida de datos.
30	RSA	Es un sistema criptográfico de clave pública desarrollado en 1979 que se basa en la factorización de números enteros.
31	RTO	*Recovery time objective*: el tiempo máximo que un sistema puede estar fuera de línea.
32	Sensor de fuerza	Son dispositivos que permiten obtener una señal eléctrica proporcional a la fuerza que se aplica sobre ellos.
33	Shields Arduino	Es una placa de circuito impreso que se coloca sobre la placa central del Arduino.

34	Tarea Programada	Es una secuencia de comandos, programas o documentos programados para ser ejecutados automáticamente a la hora más adecuada, de acuerdo con una calendarización.
35	Taxonomía de Churches	Es la actualización de la revisión de la taxonomía de Bloom efectuada por el Dr. Andrew Churches para ponerla a tono con las nuevas realidades de la era digital.
36	Taxonomía de TI	Son sistemas de organización de contenidos.
37	Tiempo de presión	Medida en milisegundos del tiempo en el que una tecla está siendo presionada.
38	Transductores	Componentes que convierten una fuerza de tensión, compresión o presión a señales eléctricas permitiendo obtener valores medibles que se pueden llegar a estandarizar.
39	Vector biométrico	Es la nueva huella biométrica creada a partir del conjunto de fuerza, velocidad y presión.
40	Vector de comparación biométrico	Es el conjunto de huellas biométricas almacenadas en la base de datos; se usa en la comparación para autentificar un vector biométrico.
41	Velocidad	Es un valor numérico calculado por el intervalo de tiempo desde que se presiona la primera tecla hasta que se presiona la última.
42	Vulnerabilidad	Es una debilidad o fallo en un sistema que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas, o en su defecto mitigarlas.
43	*Web Service*	Componente cerrado que se comunica con otros sistemas o componentes por medio de interfaces; permite tener la lógica del negocio encapsulada para evitar fuga de información, pero

		con funciones tan completas y robustas que facilite a otros componentes autorizados poder obtener la información necesaria y cumplir con sus objetivos.

Introducción

Desde tiempos ancestrales, los seres humanos hemos tenido la necesidad de proteger información, lugares o personas. Entre las primeras invenciones para este tipo de actividades, se encuentra la creación de dispositivos para la protección del perímetro físico. Unos muy populares, que casi no han tenido modificaciones desde el principio, son los paneles de seguridad con código de acceso.

En el presente documento se hablará sobre un prototipo para mejorar dichos dispositivos de seguridad, utilizando como base el estudio de NEUROQWERTY.

Se tomarán en cuenta puntos de vista tanto técnicos como operativos; se dará un vistazo a la parte económica para lograr la implementación del proyecto, mostrando sus objetivos principales, generales y específicos. Se darán a conocer ventajas y desventajas que puedan surgir durante la creación del proyecto y la visión / misión de este.

Capítulo 1

La propuesta

1.1 Generalidades

Este proyecto nace tras analizar y estudiar la vulnerabilidad que tienen los paneles físicos actuales, sumado a un estudio médico del MIT publicado en una revista científica en el año 2014 llamado NEUROQWERTY. Este estudio plantea que al observar la interacción diaria de una persona con un teclado es posible cuantificar el potencial deterioro psicomotor de una persona.

Esta primera publicación explica cómo hacer una detección temprana de las enfermedades degenerativas como el Parkinson.

Este estudio tiene como base teórica el uso de fuerza, constancia y velocidad de interacción del usuario con su dispositivo, donde se utiliza la presión de las teclas o pantalla de los dispositivos de uso cotidiano. He aquí el principio base que permite el nacimiento de este proyecto.

1.2 Antecedentes del problema

Dado que los paneles físicos de seguridad con código de acceso son los preferidos por muchas personas para resguardar diferentes activos, se tomaron estos como objetos de estudios.

En la actualidad, la mayoría de los paneles constan de una clave que se introduce con un teclado o con la tecnología de proximidad, la cual por medio de un receptor colocado en el panel pueda autentificar tarjetas que son entregadas a los usuarios. Estos controles son preferidos por gran parte de las organizaciones debido a su sencillez, facilidad de uso y mantenibilidad. Sin embargo, estas características son las que crean ciertas brechas que pueden llegar a ser explotadas por personas no autorizadas, poniendo en peligro la seguridad de los datos resguardados.

Dentro de las últimas actualizaciones que se han agregado a dichos paneles están los controles biométricos, pero estos llegan a ser más costosos que sus contrapartes mecánicas; el mantenimiento y la administración no son tarea sencilla.

Con la innovación tecnológica nace la vulnerabilidad; por ello, todos los controles mencionados anteriormente son altamente atacados por personas que desean acceder a esta información. La problemática nace en la alta vulnerabilidad que poseen estos dispositivos y el deseo de mejorar su seguridad para evitar así toda fuga no deseada de información.

1.3 Definición y descripción del problema

Tras revisar varios resultados de estudios sobre las problemáticas, fortalezas y debilidades de los paneles físicos, se llega a la conclusión de que los controles mencionados (los que usan un teclado para la introducción de claves) son los que presentan más vulnerabilidades.

Tras analizar la situación actual, se descubrió que estas claves son tan seguras como el portador que las guarda. Esto nos entrega dos escenarios:

1. Al usuario se le olvida la contraseña con frecuencia.
2. Para evitar que se le olvide la contraseña la guarda por escrito. En casi el 90% de los casos, esta es la razón por la cual una contraseña cae en las manos equivocadas, comprometiendo la seguridad del activo que se estaba protegiendo.

Una problemática existente en dichos paneles es la cantidad de claves que se pueden guardar en memoria; a saber, un número limitado.

1.4 Justificación

Teniendo en cuenta que los controles pueden presentar esta brecha de seguridad, donde el factor humano es el causante y da como resultado que la mitigación sea una tarea casi imposible, se justifica la implementación de este proyecto de investigación.

Este estudio científico-médico permite la creación de un prototipo funcional que puede llegar a mejorar el nivel de seguridad de los controles actuales; se puede traducir en una reducción del costo.

Tras la aplicación de este nuevo *hardware*, se llega a la siguiente premisa: "una clave comprometida ya no sería una brecha de seguridad", lo que nos da como resultado una disminución en el impacto económico, que se traduce en la protección integral de la imagen de una organización.

1.5 Viabilidad

1.5.1 Punto de vista técnico

Gracias al amplio conocimiento técnico y analítico adquirido a lo largo de la carrera de Maestría en Ciberseguridad, se puede afirmar que para llevar a cabo este prototipo necesitamos los siguientes componentes:

- ***Machine learning***: capacidad de un sistema de aprender del usuario sobre la marcha. Esto se va a obtener por medio de un algoritmo creado para el proyecto y un código que permite recolectar los datos de forma precisa; además, permitirá que el prototipo "evolucione" día a día para evitar que un usuario y contraseña correctos no sean reconocidos por el sistema.

- **Teoría del NEUROQWERTY**: teoría que define la posibilidad de estudiar el deterioro psicomotor de una persona con un dispositivo electrónico, tomando

como base que dicha interacción se puede traducir como una huella biométrica única por usuario.

- **Encriptación**: como el objetivo principal del proyecto es mejorar la seguridad en un panel físico, debemos tener la capacidad de asegurar cada sector de dicho control, y esto incluye la información; por lo tanto, se va a utilizar un algoritmo para la protección de datos sensibles.

- **Panel físico de entrada de datos**: dispositivo que se utiliza para permitir o denegar el acceso de las personas a sistemas de información. Entre sus características está que debe ser mecánico.

- **Base de datos**: lugar de almacenamiento del conjunto de información que se registrara sobre los usuarios; además, puede ser extendido para la creación de métricas y alertas tempranas.

- **Huella biométrica**: es una huella que permite que una persona pueda ser identificada con alguna característica de su cuerpo. Esta nueva huella biométrica se obtendrá con la teoría del NEUROQWERTY.

1.5.2 Punto de vista operativo

La implementación de este proyecto se visualizó sin necesidad de estar ligado a una compañía. Se puede decir que está planeado para aplicarlo a cualquier organización que se encuentre en marcha, ya que se puede hacer en horario no ordinario creando un impacto mínimo o nulo en el costo operativo.

1.5.3 Punto de vista económico

El costo de la creación de un prototipo de este nuevo control de seguridad perimetral es bastante bajo. Entre los costos podemos nombrar:

- El panel físico. Esta sería la parte más costosa del prototipo debido a la característica mecánica necesaria para funcionar.
- Computadora para procesamiento y almacenamiento. Este apartado puede variar según lo que se llegue a adquirir. En este caso, se está usando un Arduino por panel; el costo de este es bastante accesible.

Los otros componentes que se van a necesitar para el prototipo son:

- Una base de datos para el registro de los usuarios; esta puede ser de distribución libre.
- El algoritmo para el manejo de la huella biométrica.

Sobre la información de los componentes se va a ahondar de forma más detallada en el apartado 2.4.5.

1.6 Objetivos

Para este proyecto se va a utilizar como taxonomía la propuesta de Churches, dado que se apega bastante al objetivo que se quiere lograr, ya que es una mejora que se le está dando a la taxonomía original de Bloom de 1956.

Tomando en cuenta los puntos descritos con anterioridad, se propone una nueva alternativa para el control de acceso físico, programando un sistema de aprendizaje de comportamiento humano que medirá la velocidad, fuerza y presión al interactuar con un dispositivo. Esta combinación es lo que llamaremos la nueva huella biométrica, la cual es única e intransferible y está estrictamente enlazada a un usuario. Tras obtenerse por medio del algoritmo propuesto, esta debe procesarse para ser verificada o almacenada. A través de ella se verificará la identidad de un usuario y se determinará si tiene o no acceso.

Este prototipo tiene como objetivo incrementar la función básica de los paneles físicos con teclado; se espera que sea el inicio del punto de inflexión positivo para la evolución de dichos controles, permitiendo de una forma económica mejorar la seguridad de los activos.

1.6.1 Objetivo general

Identificar los puntos débiles de los paneles físicos actuales para minimizar las fallas más comunes utilizando un nuevo dispositivo que incrementa la seguridad, otorgando las herramientas necesarias para la creación de un prototipo funcional por medio de documentación, diagramas y especificaciones, además del algoritmo base para autentificación.

1.6.2 Objetivos específicos

1. Incrementar la función básica de los paneles físicos con teclado para mejorar su seguridad por medio de un nuevo *hardware*.
2. Aumentar la seguridad perimetral con el fin de prevenir el ingreso de personal no autorizado mediante la nueva huella biométrica.
3. Evitar las vulnerabilidades que se pueden presentar en el almacenamiento de contraseñas mediante la implementación de un nuevo algoritmo para autentificación.
4. Extender las funcionalidades de un panel físico convencional, utilizando tecnologías de fácil acceso, para generar bitácoras de visitas automáticas mediante el registro de cada ingreso y egreso del personal (que utilice dicho control).
5. Crear alertas tempranas, notificando en tiempo real posibles brechas de seguridad por medio de correo electrónico.
6. Analizar los resultados de la propuesta en un ambiente controlado para ver la factibilidad de su uso comercial.

1.7 Alcances y limitaciones

1.7.1 Alcances

Objetivamente, se desea crear toda la investigación y documentación asociadas al proyecto.

Entre los objetivos a alcanzar son:

1. Creación y entrega del nuevo algoritmo para la generación de la huella biométrica.
2. Documentación necesaria para la puesta en marcha de la base de datos.
    a. Se incluyen requerimientos para la instalación del motor de base de datos.
    b. *Scripts* necesarios para generar la estructura de la base de datos.
    c. *Scripts* con *store procedures* para el funcionamiento correcto de la base de datos.
    d. Algunos datos de prueba.
    e. Casos de pruebas.
3. Análisis de factibilidad.
4. Cualquier otra información necesaria para poder hacer un prototipo en el futuro.

1.7.2 Limitaciones

Tras el proceso de planeamiento y creación de este proyecto, se dio a conocer que la limitación más grande es el panel de seguridad con teclado mecánico.

Este tipo de dispositivo no es muy común en el mercado; aunque existen variaciones de dispositivos que se pueden utilizar, se presentan restricciones tecnológicas que hacen que el manejo de los vectores necesarios sea difícil de capturar.

1.8 Marco de referencia organizacional y socioeconómico

Como se mencionó en las secciones anteriores, este proyecto se visualizó para ser aplicado en cualquier organización sin importar su nivel de madurez. A partir de esto, se tomó la decisión de no enlazarse a una organización específica a la cual se le aplique el resultado de este trabajo de investigación.

Esta perspectiva genera ventajas en el costo operativo, el costo de implementación y el tiempo de personal asociado a la seguridad informática. Sin embargo, también nos muestra desventajas como el tiempo de pruebas, además de que ciertas secciones de este apartado no se podrán rellenar en su totalidad.

1.8.1 Historia

Casi desde el inicio de la humanidad, el uso de controles de seguridad física para la protección de activos (sean organizacionales o personales) ha sido de las principales armas de protección contra hurtos y fugas de información.

Si hacemos un viaje a través del tiempo, podemos notar que al principio se utilizaban las cerraduras como mecanismo de protección; estas se incorporan a puertas, cajones de armarios, cofres, arcones y básicamente a cualquier lugar que se quisiera proteger contra el acceso no autorizado, ya que impedía que dicho activo abriera sin la llave, cumpliendo con el objetivo de proteger su contenido.

El mecanismo normalmente se acciona mediante una llave de metal, antiguamente de hierro y bronce. La clave de la seguridad se da por la forma única de cada llave que encaja en la cerradura.

Con el paso de los años, dichas cerraduras fueron mejoradas para crear combinaciones que garanticen que el patrón de una llave con su llavín sea único. Otras mejoras se dieron al agregar dispositivos electromecánicos o electrónicos, donde la llave se ha sustituido por una tarjeta o dispositivos de entrada de datos como paneles alfanuméricos.

Pero por cada "actualización" que nos brinda mejoras, hay un grupo de personas que se dedican a encontrar la forma de corromper la tecnología. En la actualidad, dada la difusión por internet, estas técnicas son más fáciles de conseguir y crean amenazas que se pueden materializar en cualquier organización. Los creadores de *hardware* siempre están investigando y en las últimas actualizaciones para evitar dichas vulnerabilidades; se agrega el uso de cilindros electrónicos que llegan a sustituir a los cilindros mecánicos.

Cabe mencionar que los paneles físicos son un complemento a la cerradura y que la seguridad que puede otorgar dicho componente se puede ver afectada por la calidad de la cerradura a la cual se le agrega.

Una variación interesante de estos controles se da con paneles de interacción humana donde había palancas secretas que, si se empleaban en el orden correcto, activaban cerrojos que permitían el acceso al activo. Otros ejemplos son los candados con clave para puertas y cadenas, cajas de seguridad o paneles para la protección de habitaciones.

Notamos que estos dispositivos han estado presentes en casi todas las civilizaciones, han prevenido robos, pero sin importar el esfuerzo del encargado de velar por la

información, en ocasiones el fraude se ha presentado, llegando a materializar la amenaza.

1.8.2 Tipo de negocio y mercado meta

Gracias a la versatilidad del control de seguridad que estamos planteando, el mercado meta de esta investigación se aplicaría a cualquier compañía que necesite resguardar activos por medio de una barrera física, que permita el acceso a dicha información solo si se accede con el usuario y contraseña correctos.

1.8.3 Misión

Generar confianza y seguridad extra a las organizaciones, colaboradores y cualesquiera personas físicas que necesiten un sistema de seguridad perimetral inteligente.

1.8.4 Visión

Que, en un futuro cercano, esta investigación abra las puertas a la nueva generación de controles perimetrales físicos, convirtiéndose en un estándar para el mercado.

1.8.5 Valores

Como cualquier otro proyecto, se quieren dar a conocer diferentes valores necesarios para la creación y puesta en marcha de dicho prototipo.

- **Responsabilidad:** se debe comprometer a velar por los activos que el dispositivo va a proteger, esto incluye también los datos personales de los colaboradores y actividades que sean registradas en el sistema.

- **Equidad:** es un proyecto que pretende tener un trato justo y equilibrado entre nuestros colaboradores, al igual que la relación laboral, comercial y cívica con la sociedad, nuestros clientes y sus empleados.

1.8.6 Políticas institucionales

En el momento del desarrollo de este documento no se tiene elaborada ninguna política institucional que afecte al proyecto o a las empresas que puedan a futuro conseguir el prototipo descrito en el documento.

Capítulo 2

Definiendo la seguridad

2 Definiendo la seguridad

Para poder definir la seguridad debemos conocer las variables que afectan el sector donde vamos a trabajar.

2.1 Riesgos

Si empezamos por la parte de posibles riesgos, debemos verificar los niveles en los cuales nos podemos ver afectados.

2.1.1 Riesgos organizacionales

Hay que recordar que cada organización es un mundo aparte. No podemos pretender que el prototipo se acople al 100%, de primera entrada, a cualquier organización. Tomando en cuenta que el dispositivo tiene varios pasos de configuración y una variación en el modelo, se debe planear la forma en que se va a implementar el dispositivo.

Este plan debe contemplar las reglas de negocio de la organización, los procesos y hasta el lugar donde se va a colocar dicho dispositivo.

2.1.2 Riesgos personas

Sabemos que las personas siempre son el eslabón más débil en un ecosistema seguro; este dispositivo viene a corregir en parte este factor, pero solo en parte.

El dispositivo está pensado para evitar la fuga de información, previniendo en caso de que un usuario o contraseña se vea comprometido; esto da como resultado que dicha pérdida no cause una brecha en la seguridad.

Debemos mencionar que el dispositivo no está a salvo de malintencionados que intenten hacer un daño físico. Aunque se siga el esquema presentado en el documento sobre la forma óptima para la colocación del dispositivo, este quedará parcialmente expuesto y acá

se pueden generar daños graves (en el teclado); sin embargo, esta situación se minimiza al separar el *hardware* encargado del procesamiento, lo cual evitaría pérdidas mayores.

2.1.3 Riesgos de sistemas

El sistema, aunque puede ser bastante robusto, no está exento de fallos por mal uso, intento de vandalismo o desgaste normal de los activos. Aun así, el estar creado en tecnologías populares permite que su mantenimiento sea sencillo.

El sistema estará en constante crecimiento, debido a los perfeccionamientos tecnológicos, actualización de componentes o mejoras en la lógica inicial.

2.1.4 Riesgos en las características del lugar que vamos a proteger

Es importante revisar los requerimientos del lugar a proteger. Estas características especiales son importantes para determinar el tipo de dispositivo (modelo) que mejor se acople.

Para sectores que ocupan una validación no solo de entrada, sino que deben tener un control de salida, se debe modificar la capa de *FrontEnd* del dispositivo para así incluir otro panel físico; esto también ocasionará que el *software* en dicha capa deba ser actualizado.

Otra característica que no está contemplada en este momento es el tipo de cierre que tendría la puerta donde se colocaría el dispositivo. Para los casos prácticos siempre se pensó en llavines con un seguro incluido, pero a futuro se puede pensar en llavines separados e imanes en las puertas.

2.2 Controles

Como parte de los requisitos del proyecto, los teclados deben ser mecánicos; esta será la interfaz para controlar el acceso y brindar protección. Fácilmente, podemos darnos cuenta de que el dispositivo en sí es un control de seguridad perimetral.

Ya que el dispositivo se encontrará de cara al mundo velando por la protección de la información que estará resguardando, debemos crear ciertos lineamientos para asegurar la disponibilidad e integridad de los datos a proteger.

2.2.1 Políticas de mantenimiento

Todo sistema debe estar en constante mantenimiento para asegurarse de que esté siempre en óptimas condiciones. El mantenimiento no solo debe contemplar el dispositivo, sino que también debemos incluir los otros componentes (puerta, bisagras, tornillos, etc.).

Se debe generar un plan para comprobar la integridad de los datos, limpieza de datos antiguos, copias de seguridad y pruebas en el panel de control para corroboración de la captura del vector que forma la huella biométrica; además, este deberá actualizarse cuando sea necesario.

Los usuarios también deben tener un mantenimiento programado, donde se llevarán a cabo el cambio de contraseña y la actualización de datos.

2.2.2 Acciones ante bloqueo y fallos del sistema

El administrador o encargado que se coloque para el sistema debe ser capaz de solventar cualquier bloqueo inesperado de usuarios, posibles errores o fallos en la autentificación.

El administrador debe tener una solución alterna para poder acceder sin el uso de su usuario. Se pensó en una llave física o una tarjeta de proximidad; esta alternativa estará para nuevas entregas.

Capítulo 3

Marco metodológico

Tras conocer el enfoque inicial del proyecto, debemos analizar y definir el tema, el tipo de investigación que se va a efectuar y el alcance planeado. En esta sección del documento se determina el enfoque y varias técnicas que ayudarán a entender el estudio hecho en esta investigación.

3 Estado de la cuestión

Para llevar a cabo el estado de la cuestión se hizo una búsqueda de documentos que permitieran decidir el tipo de tecnología en el área perimetral.

Las búsquedas relacionadas con el tema se hicieron en fuentes especializadas, como la *European Journal of Operational Research* y el sitio oficial de la IEEE Software, con un resultado de cero artículos publicados.

Por otro lado, la búsqueda en Google lleva al sitio del proyecto original y uno que otro sitio donde se habla de forma muy escueta sobre el tema. De los hallazgos, el 100% de las publicaciones hablaban sobre la tecnología aplicada en el área de la medicina.

Por lo tanto, tras la implementación de una revisión sistemática de Ingeniería de *Software*, se puede asegurar que en este momento no existe nada parecido en el mercado actual, aspecto que crea una ventaja competitiva.
Como este prototipo pretende extender la funcionalidad de los paneles de control, se puede traducir como una mejora en la seguridad perimetral actual. Esto es lo que permite asegurar de forma teórica que se verá una mejora exponencial en la seguridad perimetral actual.

El uso de este prototipo, unido a la forma única de interacción humana propuesta, demuestra que el manejo o control en el caso de usuario y contraseña va a ser más seguro. Aquí nace la hipótesis de un nuevo método de seguridad más robusto con ayuda de la nueva huella biométrica para evitar vulnerabilidades que se lleguen a presentar en el manejo de la dupla mencionada.

Como un bono adicional al usar un sistema de *software* con persistencia de datos que respalde a los nuevos paneles, la creación de bitácora de visitas es totalmente viable al igual que la creación de métricas y alertas tempranas.

Tras la elaboración de un prototipo funcional, se llevará a cabo un periodo de pruebas. Transcurrido este periodo, empezaremos a obtener datos reales que posteriormente van a ser analizados. Esto nos ayudará a mejorar la propuesta y ver la usabilidad en un ambiente controlado, permitiendo determinar si el proyecto es o no factible en su uso comercial.

3.1 Tipo de investigación

Dado que existen varias categorías y subcategorías para llevar a cabo una investigación, y conociendo la magnitud y el alcance del proyecto, se decidió hacer una investigación del tipo exploratorio.

Esta decisión se toma pensando en las ventajas, desventajas y limitaciones que presenta el proyecto, ya que los resultados finales nos podrán brindar una visión más determinante con respecto a la realidad, sabiendo que el material de investigación sobre el campo es escaso y el *hardware* es casi inexistente.

3.2 Alcance investigativo

El alcance de este proyecto es generar la documentación necesaria para entender lo que es la tecnología NEUROQWERTY, lo cual incluye ventajas y desventajas que se puedan presentar al aplicar dicha tecnología a un control físico perimetral de tipo panel.

Como parte del contenido, se incorporará el campo de la tecnología relacionada con la ciberseguridad; algunos de los temas que podemos citar son criptografía, implementación de la seguridad de aplicaciones, protocolos de seguridad y seguridad en datos almacenados.

3.3 Enfoque

Como este proyecto vanguardista desea integrar dos mundos, al unir un sistema de uso cotidiano como es el panel de seguridad físico con la teoría novedosa del estudio médico para la detección temprana de algunas enfermedades degenerativas (NEUROQWERTY), se debe exponer a fondo para un mayor entendimiento.

3.3.1 ¿Qué es el NEUROQWERTY y cómo funciona?

Es un proyecto multidisciplinario e internacional concebido por profesionales de la salud, que tiene como objetivo la identificación prematura de enfermedades degenerativas, principalmente el mal de Parkinson.

Este proyecto lleva a cabo su objetivo por medio del registro de la interacción humana con dispositivos electrónicos. El *hardware* para el cual fue concebido es el teclado de una computadora, pero se piensa hacer una evolución de este al integrar la interacción con dispositivos móviles (celulares y tabletas).

El registro de los datos se hace por medio del *hardware* seleccionado, el cual se asigna a una computadora que tiene un *software* especializado que se encarga de llevar el registro y el análisis por sujeto de prueba.

Dicho *software* es de distribución libre y puede ser descargado de la página oficial del proyecto en el MIT. El *software* registra el patrón del vector fuerza-presión ejercido por un teclado; intenta analizar la habilidad motriz de una persona al momento de la interacción, notando cambios significativos en dicho patrón. El análisis se envía a un servidor y los resultados se envían a los encargados del proyecto.

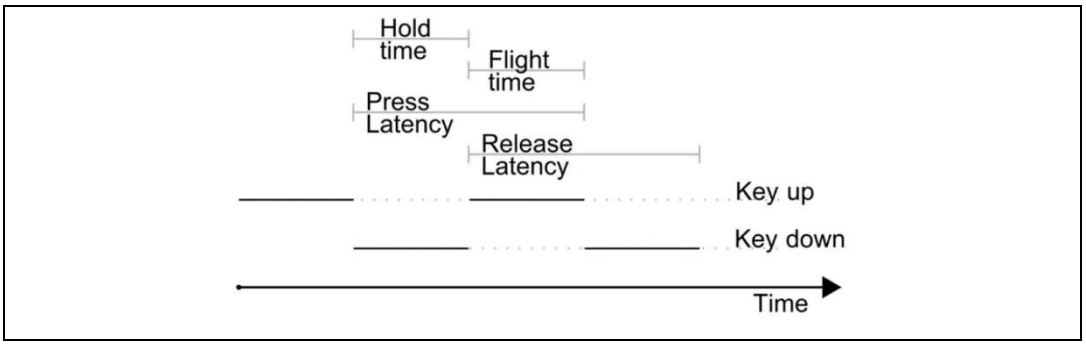


Figura 1. Representación gráfica de las dinámicas de pulsación de teclas
Fuente: https://www.nature.com/articles/srep09678

La teoría afirma que toda persona mantiene una firma biométrica única, la cual está compuesta por presión y fuerza; en estos casos, el *software* es el encargado del registro en línea.

Los resultados del estudio permiten determinar si existe un deterioro psicomotor y con esto evaluar la posibilidad de que el usuario pueda padecer Parkinson.

La enfermedad de Parkinson afecta a más de cinco millones de personas en el mundo y se cree que los casos se duplicarán en tan solo veinte años por el envejecimiento de la sociedad. Esta enfermedad es un enemigo terrible, teniendo en cuenta que desde diez años antes de un diagnóstico seguro las neuronas empiezan a morir. Estilísticamente hablando, solo al 70% de los casos se les da una identificación correcta y temprana.

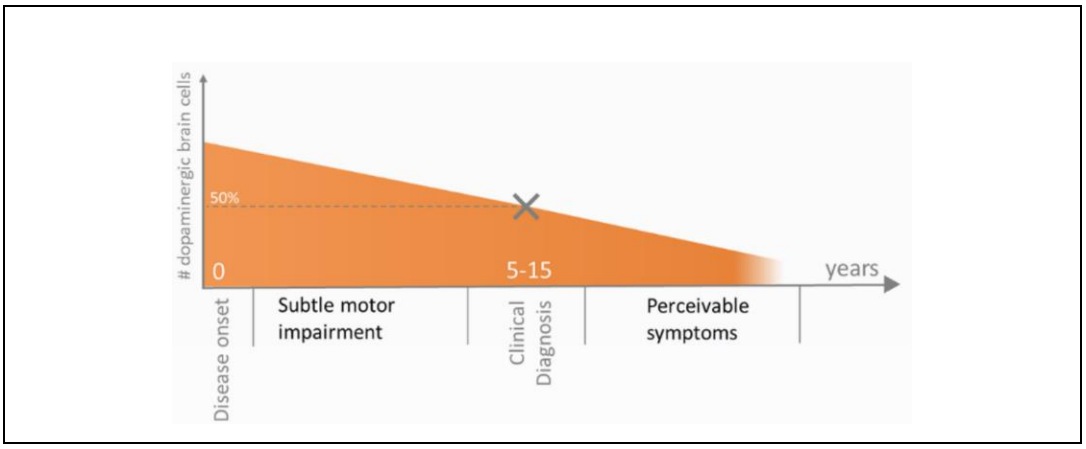


Figura 2. Gráfica de porcentaje-tiempo de la afectación de la enfermedad
Fuente: https://neuroqwerty.mit.edu/

El proyecto se dio gracias al apoyo financiero de la Comunidad de Madrid, la Fundación Ramón Areces y la Fundación Michael J. Fox para la investigación del Parkinson (número de subvención 10860).

Tras la ejecución de la primera etapa, la cual se encuentra cerrada, se dio a conocer un conjunto de datos de la enfermedad de Parkinson temprana, la cual se conoce como MIT-CS1PD; posteriormente, se presentó el segundo conjunto de datos de la enfermedad de Parkinson que se conoce como MIT-CS2PD.

3.3.1.1 Sobre MIT-CS1PD

Estos son los datos recolectados en la primera oleada de investigación del proyecto NEUROQWERTY. Este conjunto de datos incluye la información recopilada de una muestra de población con un total de 31 sujetos. Se tomó una muestra de control conformada por 13 sujetos; es decir, pacientes sanos, y en contraparte se reclutaron 18 pacientes con enfermedad de Parkinson (PD). Todos ellos fueron reclutados en dos unidades de trastornos del movimiento en Madrid (España), siguiendo los protocolos institucionales aprobados por el Instituto Tecnológico de Massachusetts, EE. UU. (Comité sobre el uso de seres humanos como aprobación experimental N.º 1402006203), Hospital

12 de octubre, España (N.º CEIC: 14/090) y Hospital Clínico San Carlos, España (N.º 14/136-E).

Los archivos muestran la información que se logra recabar durante las sesiones, donde se presentaban actividades de escritura en un procesador de texto. Se les daba libertad para corrección de errores de mecanografía y todos los participantes utilizaron un equipo Lenovo G50-70 i3-4005U con 4 MB de memoria y una pantalla de 15 pulgadas con Manjaro Linux.

Tras la primera sesión, se les pidió a los mismos sujetos asistir tiempo después a ejecutar una prueba similar, lo que permitió comparar los datos y obtener resultados bastantes positivos.

El resultado se puede ver en el gráfico 1, donde el valor GT crea la diferencia entre el tipo de población que ejecutó la prueba. Se lleva control también de resultados de la evaluación clínica, UPDRS-III, pulsaciones alternativas de los dedos, pulsación de una sola tecla, puntuación NEUROQWERTY y velocidad de escritura, además de los datos recolectados en cada sesión (archivo 1 y 2).

	gt	updrs108	afTap	sTap	nqScore	digitando rapido
pID						
11	Cierto	14.25	Yaya	162.25	0.117543	189,372549
60 60	Falso	2,00	Yaya	162.25	0,070350	60.533333
67	Cierto	25.25	Yaya	133,75	0.223411	54,333333
68	Falso	6.00	Yaya	159,00	0,074973	71.800000
70	Cierto	26.25	Yaya	113,50	0.175751	39,614035

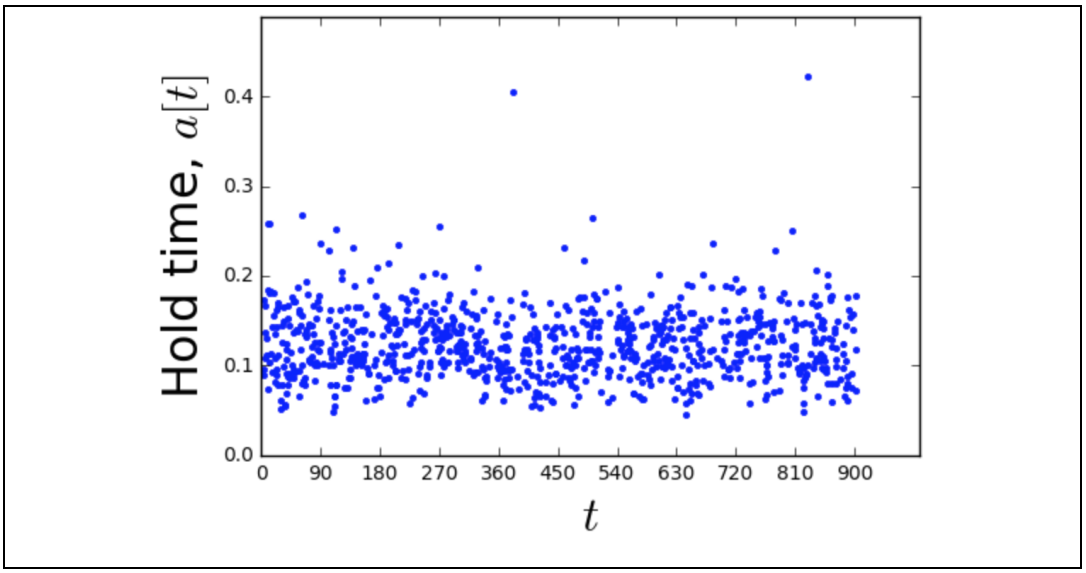


Figura 3. Resultado de las pruebas 1

Fuente: https://neuroqwerty.mit.edu/sites/default/files/images/readme.html

3.3.1.2 Sobre PD_MIT-CS2PD

Al igual que el conjunto de datos anterior, se hace la recolección de información de varios sujetos de prueba. En este caso, se sometió a 54 pacientes, de los cuales 30 corresponden a sujetos sanos (es decir, los sujetos de control) con una contraparte de 24 pacientes que presentaban la enfermedad de Parkinson.

Al igual que el grupo anterior, los sujetos fueron reclutados de dos unidades de trastornos del movimiento en Madrid (España) siguiendo los protocolos institucionales aprobados por el Instituto Tecnológico de Massachusetts, EE. UU. (Comité sobre el uso de seres humanos como aprobación experimental N.º 1402006203), Hospital 12 de octubre, España (N.º CEIC: 14/090) y Hospital Clínico San Carlos, España (N.º 14/136-E).

Dicho grupo utilizó el mismo modelo de computadora, con las mismas características de memoria y *software*, para efectuar la misma actividad de escritura en un procesador de

texto. Al igual que con el grupo anterior, se hizo una segunda sesión para corroborar los datos.

En este caso, los datos arrojados se detallan en el gráfico 2.

	gt	updrs108	afTap	sTap	nqScore	digitando rapido
pID						
1000	Cierto	27	79,0	184,5	0.107179	56.866667
1001	Cierto	dieciséis	96,5	189,0	0,056286	118,000000
1002	Falso	5 5	140,0	158,0	0,039519	119.037037
1004	Cierto	22	83,5	191,5	0,034853	74.266667
1005	Cierto	17	68,0	150,0	0,048307	74.969697

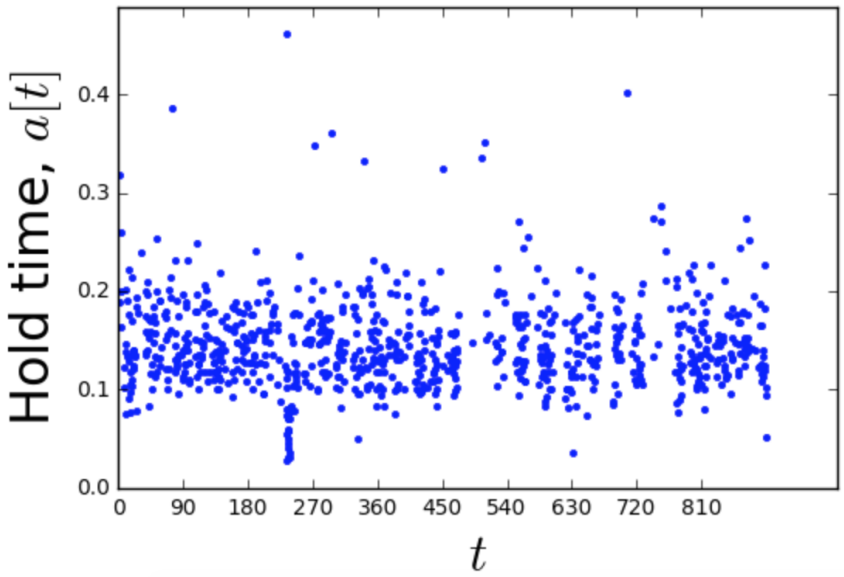
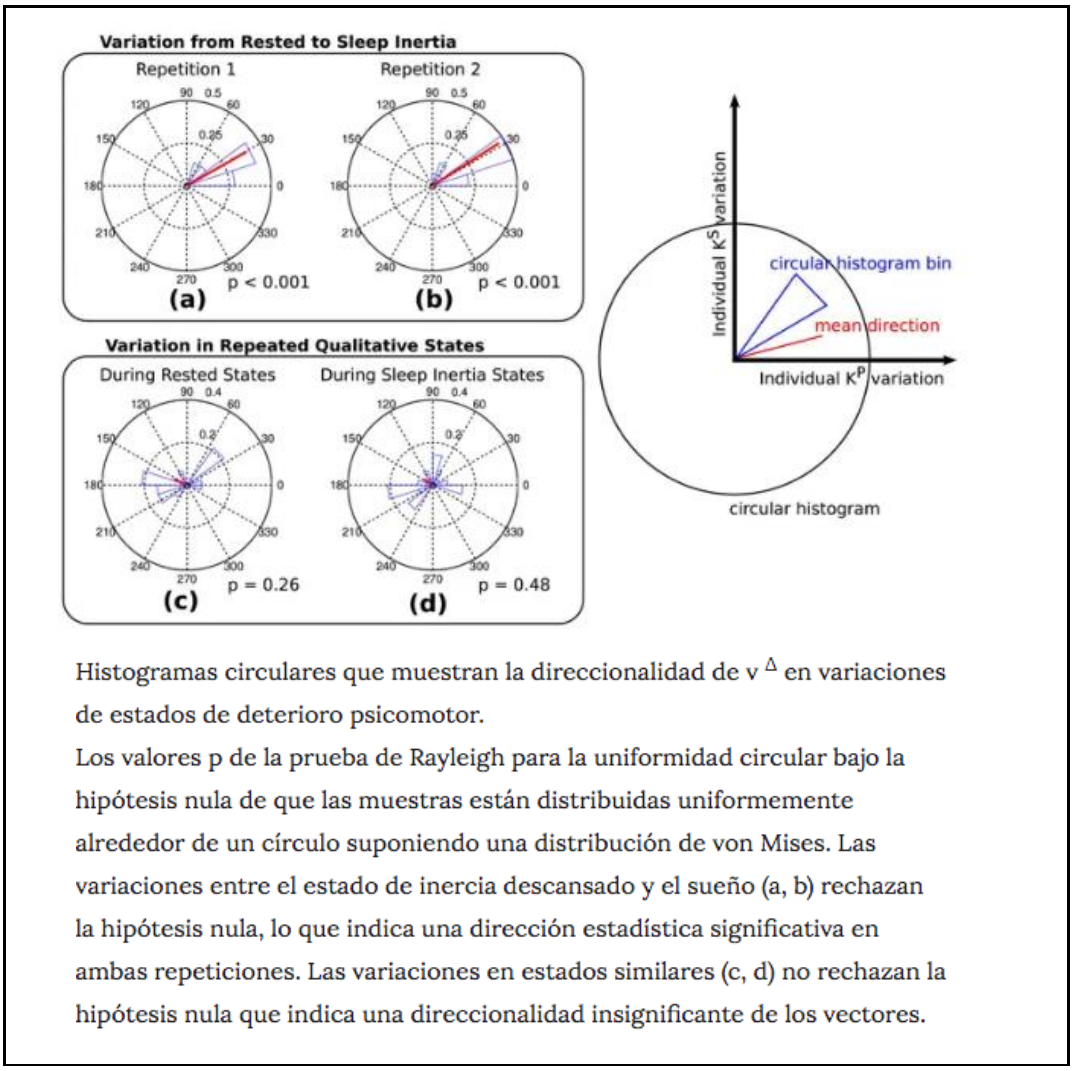


Figura 4. Resultado de las pruebas 2

Fuente: https://neuroqwerty.mit.edu/sites/default/files/images/readme.html

3.3.1.3 Los resultados

Tal como muestra la publicación de Giancardo, Sánchez-Ferro, Butterworth, Mendoza y Hooker (2015), la evaluación del conjunto de datos muestra cambios importantes en los estados psicomotores de los pacientes con la enfermedad (PD) que no presentaban los sujetos de control. Dicho cambio se representa en el vector de dirección vΔ y los resultados publicados se realizaron mediante una prueba *Rayleigth*, tal como lo muestra la figura 3.



Histogramas circulares que muestran la direccionalidad de v^{Δ} en variaciones de estados de deterioro psicomotor.
Los valores p de la prueba de Rayleigh para la uniformidad circular bajo la hipótesis nula de que las muestras están distribuidas uniformemente alrededor de un círculo suponiendo una distribución de von Mises. Las variaciones entre el estado de inercia descansado y el sueño (a, b) rechazan la hipótesis nula, lo que indica una dirección estadística significativa en ambas repeticiones. Las variaciones en estados similares (c, d) no rechazan la hipótesis nula que indica una direccionalidad insignificante de los vectores.

Figura 5. Histograma circular del estado de deterioro psicomotor
Fuente: https://www.nature.com/articles/srep09678

Al final, el resultado sugiere que la interacción del dedo con dispositivos electrónicos es capaz de proporcionar datos informativos sobre el estado psicomotor sin cambiar el flujo de trabajo diario del sujeto o la funcionalidad del dispositivo utilizado.

Las ventajas de poder cuantificar la función psicomotora podrían mejorar la atención médica futura, lo que da como resultado alterno la capacidad de generar seguridad en *software* para la toma de decisiones importantes. También se espera que los hallazgos se puedan utilizar en otras ramas de la medicina donde se vea afectada el área psicomotora de una persona.

3.3.2 El nuevo dispositivo de control

En la actualidad, hemos visto cómo los temas de ciberseguridad se han vuelto pan de cada día; el aseguramiento de los activos es un tema primordial. Todos desean que lo que están protegiendo se mantenga seguro en el lugar de resguardo.

En el momento en que la humanidad ha necesitado de la seguridad informática para resguardar información, se ha percatado de que sus controles también deben evolucionar; sin embargo, debido a esto se puede presentar alguno de estos problemas: los atacantes van a la misma velocidad de evolución (o hasta más avanzados) que los controles de protección o que los dispositivos que se escogieron para proteger activos no reciben ningún tipo de actualización.

El segundo caso es en el que caen los controles físicos tipo panel, ya que las últimas actualizaciones dejan más de lado la interacción física delegando dicha funcionalidad a terceros (tarjetas de proximidad, *Bluetooth*, NFS, etc.).

Por esta razón, se escogió un dispositivo tan útil, pero tan olvidado (en caso de actualizaciones), para amplificarlo con estudio del Dr. Mayol y su equipo. El nacimiento de esta idea podría revolucionar la historia de los controles para seguridad perimetral y

abrirá muchas puertas que a futuro pueden ser utilizadas para seguir mejorando controles; esto puede incluir no solo *hardware*, sino también *software* que pueda revolucionar la protección de la información.

Viendo las limitaciones del mercado actual, se optó por el uso de varias tecnologías que son de fácil acceso y que puedan permitir la creación de un prototipo. Sí se debe mencionar que al ser creado con este tipo de dispositivos la calidad del producto no es la óptima, al igual que su diseño.

El prototipo ideal del nuevo panel físico estará compuesto por un Arduino como la placa base, un conjunto de sensores de fuerza que servirán de teclado, esto como reemplazo para el teclado numérico mecánico. Este prototipo debe estar conectado a una computadora; en este caso, se usa un *Raspberry* para abaratar costos. En este es donde se encuentran la base de datos y el código para revisar si el usuario que está frente al panel es el correcto.

También se pensó en un prototipo donde la interfaz fuera un teclado mecánico que remplazara los sensores de fuerza. Este cambio haría que el prototipo fuera más económico, pero sacrificaría la precisión de la recolección de datos.

3.3.2.1 El Arduino

El *hardware* seleccionado fue Arduino, ya que es una plataforma de creación electrónica de código abierto; está basado en *hardware* y *software* libre. Se puede decir que este dispositivo permite crear microcomputadoras en una sola placa.

Esta placa posee un microcontrolador de tipo ATMEL, los cuales son circuitos integrados que le permiten a la gente grabar instrucciones para poder ser utilizadas en programas que interactúen con los componentes de la placa o periféricos externos.

Una gran ventaja del Arduino es que tiene varios modelos que se pueden comprar por valores bajos y que se acoplan a varios proyectos.

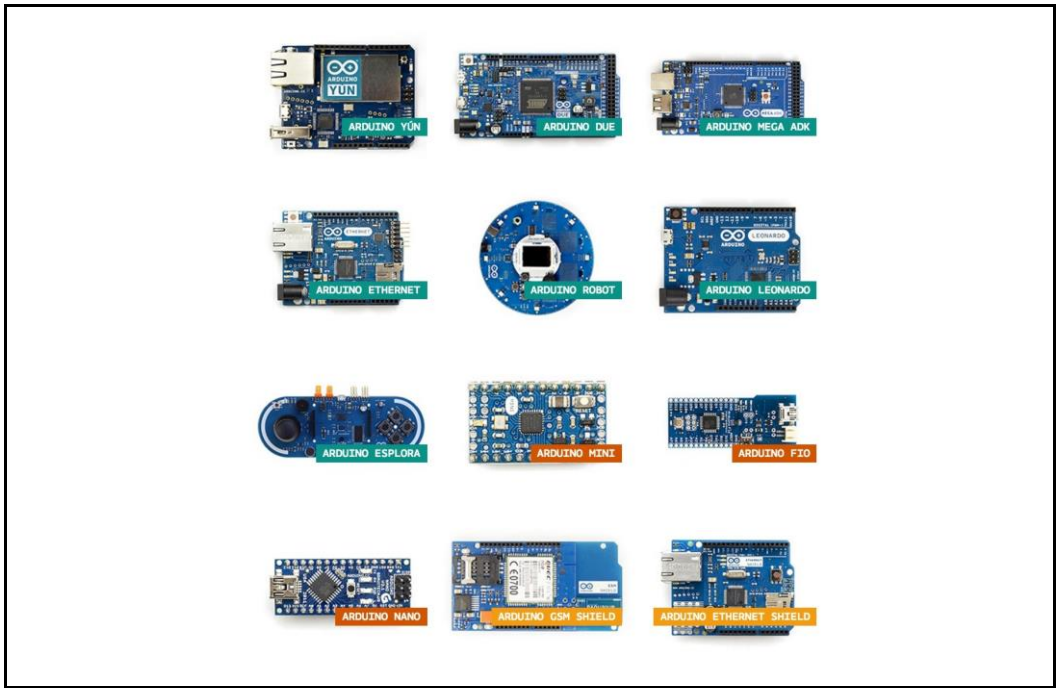


Figura 6. Diferentes modelos dentro de la gama de los Arduino

Fuente: https://www.xataka.com/makers/empezar-con-arduino-genuino-como-elegir-la-placa-modelos-compatibles-y-kits-de-iniciacion

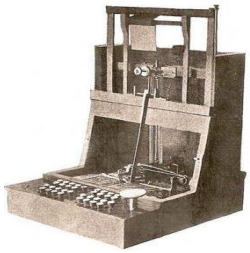
Existen unos componentes llamados SHIELDS que se unen al Arduino para poder agregarle más características a la placa base.

3.3.2.2 Los sensores de fuerza

Estos componentes, también conocidos como células de carga, son dispositivos que nos permiten obtener por medio de una señal eléctrica la fuerza proporcional que se ejerce sobre ellos. Estos sensores se pueden clasificar entre dinamómetros y células de carga.

Ambas categorías tienen varios tipos de componentes que llegan a cumplir la misma función, pero son utilizados en diferentes sectores. Mientras los dinamómetros son usados

para aplicaciones en máquinas de ensayo o instrumentos para calibración, porque son más precisos y estables que su contraparte, las células de carga están concebidas pensando en aplicaciones de pesaje o de verificación, muy utilizados en el sector industrial.



3.3.2.3 Teclados mecánicos

Estos periféricos, que son buscados en la actualidad por la precisión de sus funcionalidades, tienen ya décadas de historia. Hay ciertas maquinarias que tenían teclados integrados, entre ellas se rescatan dos: uno creado en 1575 por Francesco Rampazero y otro creado en 1714 por Henry Mill. Aunque no tenían un procesador de fondo, estaban pensados para una escritura "mecánica" y para facilitar la vida a las personas no videntes; aun así, los prototipos funcionales que llegaron al mercado se dieron hasta el siglo XIX.

Fue en la década de los 80 cuando una computadora redujo en gran medida tanto su precio como su tamaño, lo que permitió a los ciudadanos adquirir una y tener un dispositivo de estos en casa. Para ese momento los teclados eran estrictamente mecánicos. Una peculiaridad de estos modelos de computadoras era que los teclados venían integrados en el *hardware*, eran construidos como una sola placa.

Tras la evolución de las computadoras, donde la producción en masa creció, se dio la baja en los costos, algo que ciertas compañías aprovecharon para aventurarse a variar sus modelos, ya que tomaron la decisión de crear periféricos compatibles con sus computadoras.

3.3.2.3.1 *Spring Switch*

Una de las empresas pioneras que siguieron esta línea fue IBM. En su historia llegaron a tener varios modelos de teclados y uno de los más populares fue el IBM PX XT, que utilizaba la tecnología patentada de esta empresa para teclas mecánicas llamada Spring Switch.

	
IBM PC 5150 con teclado y monitor monocromático verde (5151)	Teclado *IBM PX XT*

Figura 7. IBM PC 5150 con teclado
Fuente: https://en.wikipedia.org/wiki/IBM_Personal_Computer

El *Spring Switch* era un diseño que tenía cada tecla dentro de los teclados mecánicos; estas teclas usaban un resorte que se doblaba hasta pulsar la tecla. En el momento en que este muelle pegaba en lado lateral de la tecla producía un clic, sonido que informaba que la tecla se había presionado correctamente.

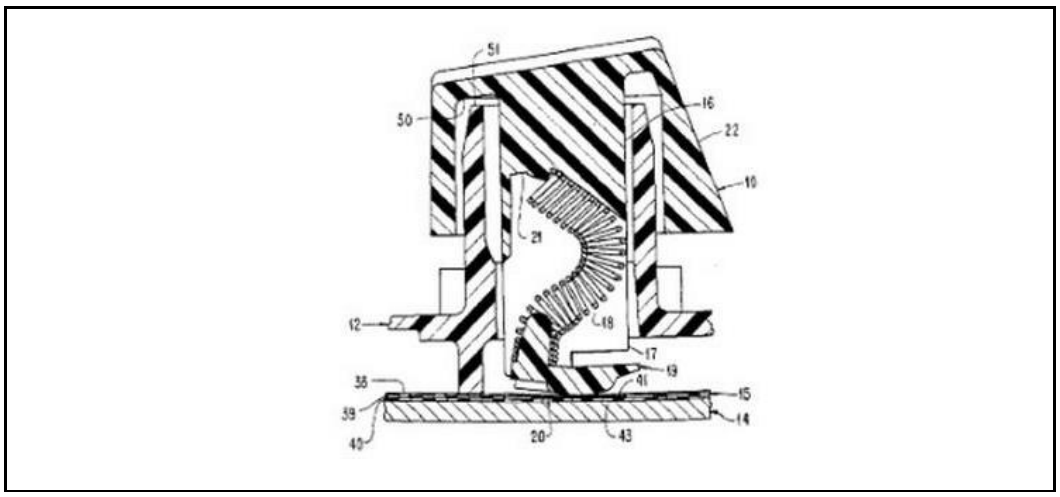


Figura 8. Diseño del modelo *Spring Switch*

Fuente: https://hothardware.com/news/ibms-legendary-model-f-buckling-spring-keyboard-reinvented

3.3.2.3.2 Tecnología ALPS

En Japón, tras el mercado emergente, crearon su propio diseño de teclas y en 1983 ven la luz los ALPS. Este mecanismo era mucho más complejo, pero con mayor posición, más que cualquiera existente en ese momento.

En este diseño, cada tecla llegaba a tener 10 componentes, razón por la cual se les conoció como ALPS complicados. Cada conjunto agregaba contactos electrónicos. A este tipo de interruptores se les hizo muchas copias, pero también mejoras que agregan un componente más a los 10 antes mencionados; este era la hoja del clic.



Figura 9. Los 11 componentes para crear una tecla ALPS
Fuente: https://deskthority.net/wiki/Alps_SKCM_Orange

Compañías como Apple, Acer y Dell vieron la ventaja de usar esta tecnología japonesa y la utilizaron en sus modelos por muchos años, hasta que dejaron de fabricarse en el 2012. En la actualidad, existen clones que son tan funcionales como los originales y compatibles tanto como los *switches* Mattias.

3.3.2.3.3 *Switches* Mattias

Este diseño es un clon modificado de los ALPS. *Mattias Corporation* introdujo dichos componentes cuando *Forward Electronics* vio una oportunidad de mercado, ya que la compañía había dejado de producir y distribuir los originales en el año 2012. La modificación del diseño duró aproximadamente dos años y desde la fecha (aproximadamente en el 2014) son de los más vendidos.

Aunque el diseño es una copia de los ALPS, se diferencian en ciertos aspectos:

- El clic silencioso: se incorporan elementos de amortiguado; por lo tanto, el interruptor baja el ruido producido, y aunque se le llama clic silencioso, el interruptor en ningún momento hace clic.
- Interruptor lineal silencioso: el diseño se modifica agregando un control deslizante (normalmente de color rojo) al que se le agregan piezas de goma que sirven para amortiguar los interruptores (aplicados tanto para la carrera hacia arriba como hacia abajo), y se le agrega un resorte extra para la hoja de clic en los interruptores táctiles, lo que omite cualquier golpe.

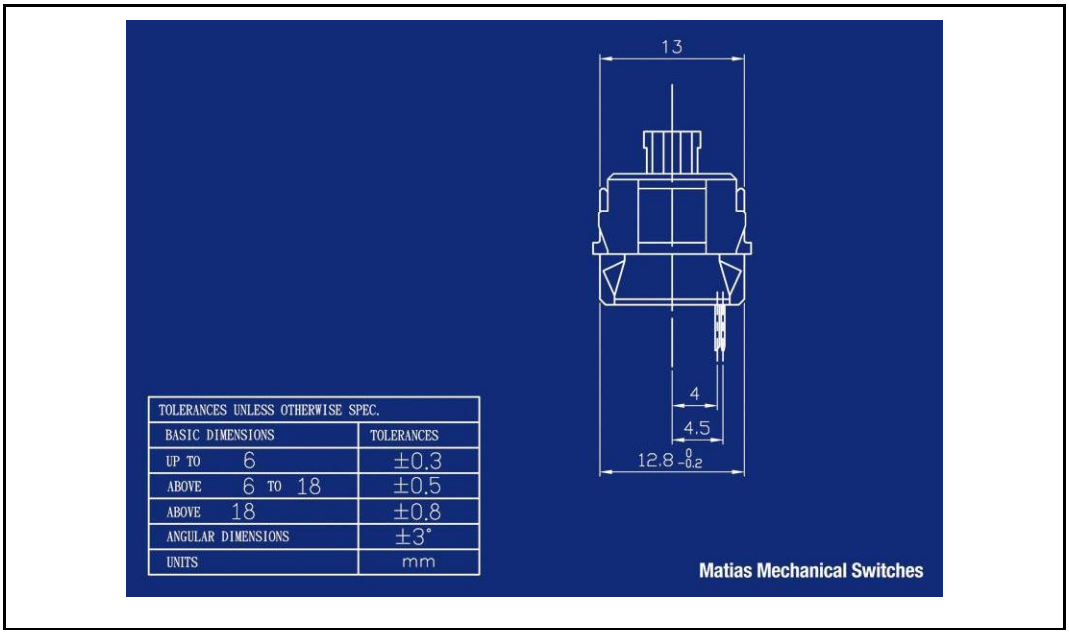


Figura 10. Plano de un interruptor para switches Mattias
Fuente: https://matias.ca/switches/click/blueprints

3.3.2.3.4 *Cherry MX Switches*

Este diseño de teclas mecánicas son las más populares y vendidas en la última década. Aunque su primer interruptor aparece en 1983, su producción sigue dándose como desde el principio. Se han convertido en referencia para los interruptores mecánicos. Tienen cuatro modelos disponibles para el público que son muy parecidos entre sí, pero varían en el tipo de componentes.

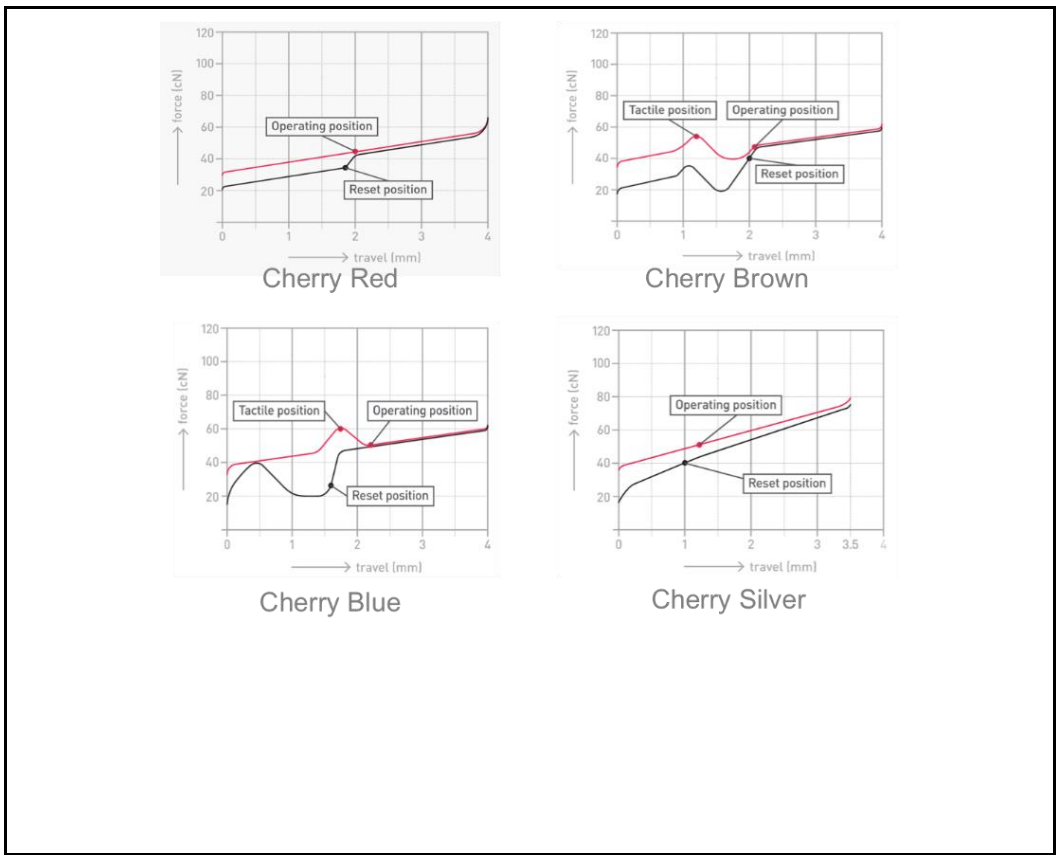


Figura 11. Comparación de pulsaciones de los Cherry
Fuente: https://www.cherrymx.de/en/mx-original

3.3.2.3.4.1 *Cherry MX RED*

Este tipo de *switch* es el más popular del mercado debido a su extrema comodidad; su actuación lineal es bastante efectiva y silenciosa, pero tiene una desventaja en el momento de teclear, ya que al ser tan silencioso se puede errar en la tecla que se está presionando.

Este diseño tiene un resorte con resistencia mínima que le permite tener un tiempo de respuesta bastante alto. Se usa mucho para mecanografía y juegos.

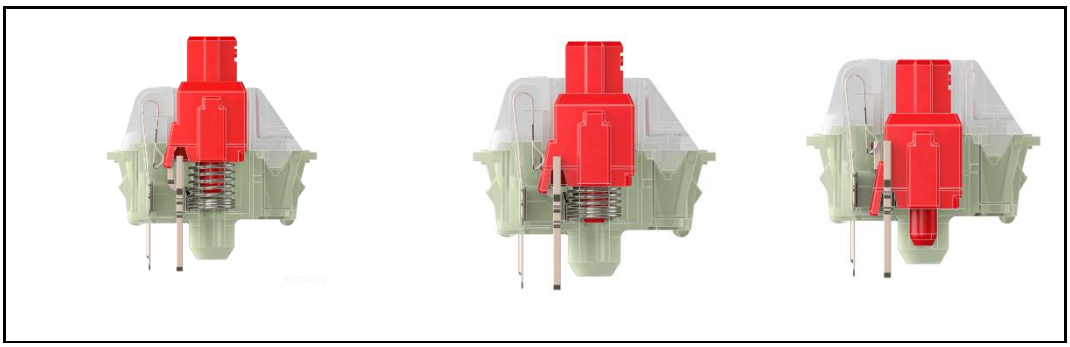


Figura 12. Visualización gráfica del funcionamiento del Cherry MX Red
Fuente: https://www.cherrymx.de/en/mx-original

3.3.2.3.4.2 Cherry MX Blue

Este es el interruptor más utilizado para la escritura, debido a la suavidad y el sonido (semejante a una máquina de escribir). Este tipo de *switch* no se aconseja para juegos por su mecanismo para pulsarlo de forma continua y rápida. Estas teclas tienden a tener posiciones de reinicio más altas y requieren una mayor fuerza de actuación, por lo que pueden funcionar un poco más lento en situaciones de toque rápido.

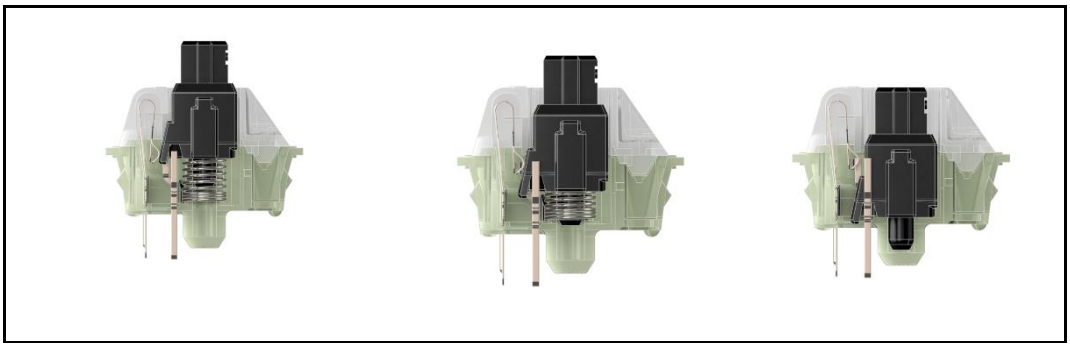


Figura 13. Visualización gráfica del funcionamiento del Cherry MX Black
Fuente: https://www.cherrymx.de/en/mx-original

3.3.2.3.4.3 Cherry MX Brown

Este es el interruptor intermedio, son de gran calidad para la escritura y juego. Son sumamente suaves y con un clic en el medio; esto permite que la pulsación no necesite llegar al fondo de la tecla, lo que la hace más rápida, pero sin errores.

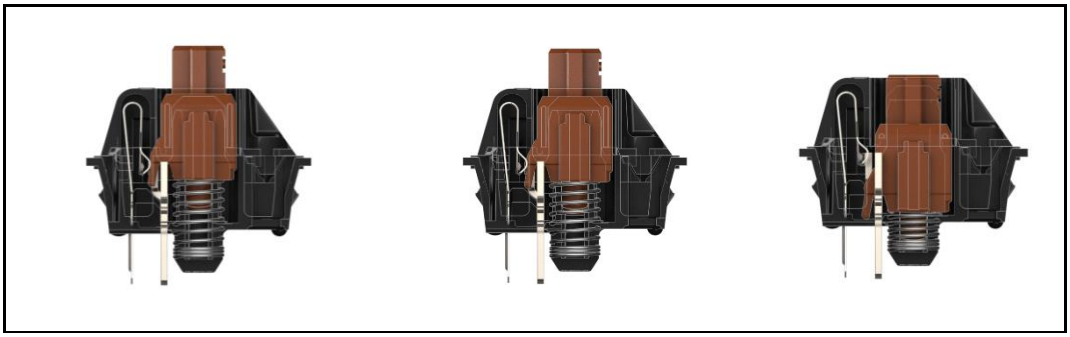


Figura 14. Visualización gráfica del funcionamiento del Cherry MX Brown
Fuente: https://www.cherrymx.de/en/mx-original

3.3.2.4 Teclados de membrana

Con el paso del tiempo, la evolución de los periféricos ha crecido a pasos de gigantes; las compañías entran en guerra para hacer periféricos que sean más fáciles de transportar, ergonómicos y hasta baratos. Esto hizo que en los 90 la creación y puesta en marcha de teclados de membrana se pusieran de moda.

Sumado al costo de producción, este tipo de teclado muestra numerosas ventajas en varias áreas como la técnica, operativa y hasta su estética; se convirtieron en fuertes competidores en el mercado. Muchos de estos teclados se pueden someter a condiciones particulares que los hacen sobresalir a los mecánicos, entre estas altas temperaturas y humedad.

El diseño de un teclado de membrana está compuesto por dos láminas (membranas) plásticas y delgadas. En la parte interna se graban pistas conductoras en la cara interior; además, se agrega una tercera membrana de separación, agujereada en las zonas en las que va una tecla. La capa superior se llama carátula y a la capa inferior se le llama circuito. Ambas capas se ensamblan mediante un adhesivo de doble cara.

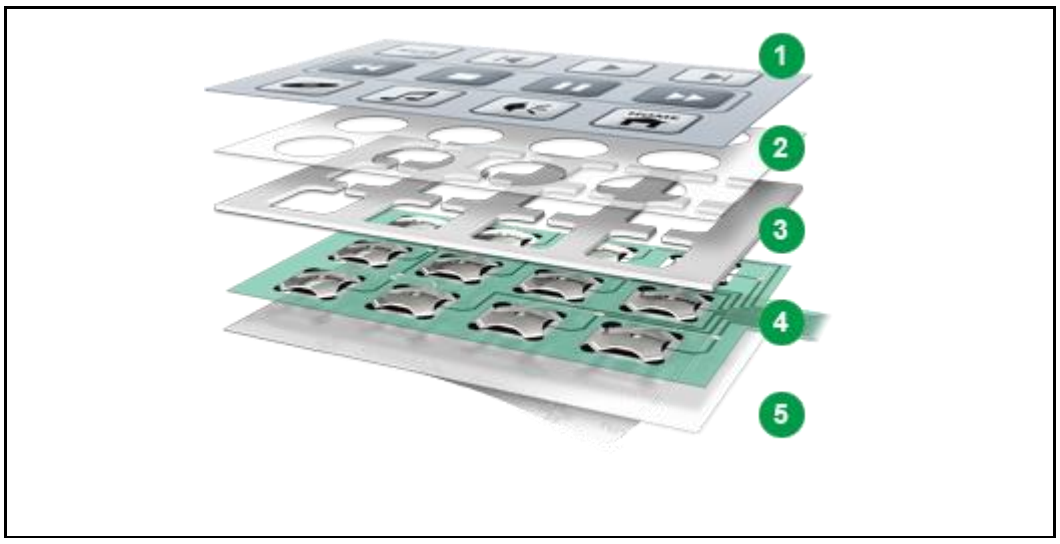


Figura 15. Modelo de estándar de un diseño de teclado de membrana
Fuente: http://www.teclaplast.com/index.php/pages/teclado-membrana

El funcionamiento de estos teclados es por medio de electricidad; cuando se hace presión sobre una tecla en específico, se hace un contacto entre las membranas dando paso a la electricidad entre cada capa; esta lectura permite saber con exactitud cuál es la tecla presionada.

Entre las características más importantes de la mayoría de los teclados de membrana se encuentran:

- Un grosor total entre 0,8 y 1,5 mm.
- Un precio competitivo debido a la tecnología económica.
- Resistencia excelente a condiciones climáticas, químicas y mecánicas extremas.
- Mejorar la suciedad entre teclas a comparación de sus contrapartes mecánicas.
- Aumento en el tiempo de vida de las teclas mecánicas mudas (3×107 usos).
- Aumento en el tiempo de vida de las teclas mecánicas sonoras (5×106 usos).

3.3.3 Los prototipos

Para llegar al prototipo final se llevaron a cabo varios productos que se fueron descartando por prueba y error.

En etapas primerizas, se intentó hacer un prototipo con dispositivos de tipo dinamómetro, pero no pasó de la etapa de planeación. Al ver las dificultades para tratar de usar este dispositivo, se llevó la problemática al tutor, quien aconsejó el uso de controles de consolas. Por lo tanto, se hizo la prueba con varios tipos de controles de varias marcas.

Todos dieron como resultado una limitante: aunque los controles tienen botones con sensor de presión, no son todos los que tienen esta característica. En resumen, los botones que tenían las características eran los de las flechas de movimiento, que son bastante imprecisos y de difícil manejo en un prototipo funcional.

3.3.3.1 Prototipo con sensores

Para este momento donde el proyecto se había quedado estancado se necesitó generar algunas ideas alternas. Tras una investigación se encontró una posible solución utilizando sensores de presión; teóricamente, es el producto más factible para cumplir con los requisitos del nuevo panel de seguridad.

Dado que los sensores son transductores, convierten una fuerza de tensión, compresión o presión en señales eléctricas, lo que permite obtener valores medibles que se pueden llegar a estandarizar. Es decir, en el momento en que se le aplica fuerza a la celda de carga, esta se deforma y dicho cambio manda una señal eléctrica proporcional a la fuerza ejercida.

El prototipo está compuesto por diez sensores de fuerza de 10 kg que funcionan como entrada de datos al interactuar con los usuarios, son las teclas del panel. Estos sensores están conectados a módulos amplificadores de energía (HZ711), los cuales se conectan al *protoboard*. Esta tableta acopla todos los componentes para poder sacar un único cable que

se conecta al Arduino uno. Este último permite obtener los datos de cada celda para ser almacenados y analizados.

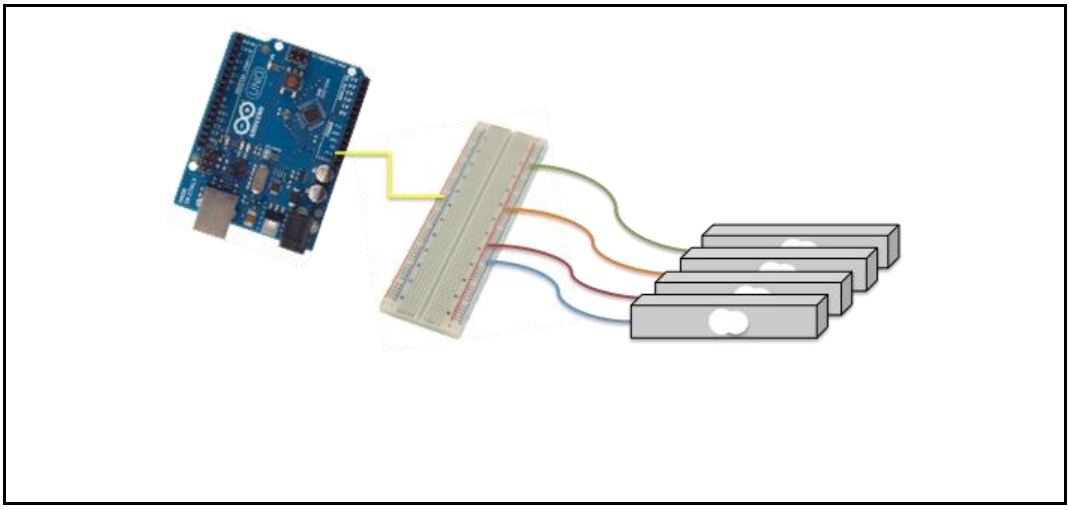


Figura 16. Diseño del prototipo con sensores
Fuente: imagen propia.

Los sensores de fuerza llegan a presentar ciertas dificultades que pueden complicar el prototipo:

- El primero era la conexión del sensor, ya que necesitaba un amplificador de poder.
- La segunda limitante es la cantidad de sensores que se pueden conectar directamente al Arduino; para esto se diseñó un circuito que por el momento está usando una *protoboard*. La conexión óptima es de máximo dos sensores; tras un cambio en el circuito se lograron conectar cinco conectores.
- El tercero es el *protoboard*, ya que este componente es para hacer pruebas; este detalle hace que los cables conectados se separen fácilmente y causan fallos en la lectura de datos. En futuras entregas, se debe diseñar una placa para que sea más portátil y menos frágil.

El último problema va directamente con el prototipo, debido a que el tamaño es bastante grande y las conexiones son frágiles, ya que se pueden desconectar en cualquier momento,

aunque se agreguen a una “caja” para poder ser transportados. Cada sensor debe estar unido a dos superficies, una como base y otra donde el usuario ejercerá la presión. Cada sensor debe estar separado para que las lecturas sean precisas y cuando se ejerza la presión en una tecla no interfiera como una falsa lectura de las “teclas” que estén a su alrededor.

Se creó un algoritmo para este prototipo, donde las medidas recolectadas en las entradas del usuario son:

- Fuerza: presión ejercida sobre la tecla. La corriente eléctrica se traduce en valores numéricos decimales.
- Tiempo de presión: medida en milisegundos del tiempo en el que una tecla está siendo presionada.
- Velocidad: es un valor numérico calculado obtenido de los valores anteriores.

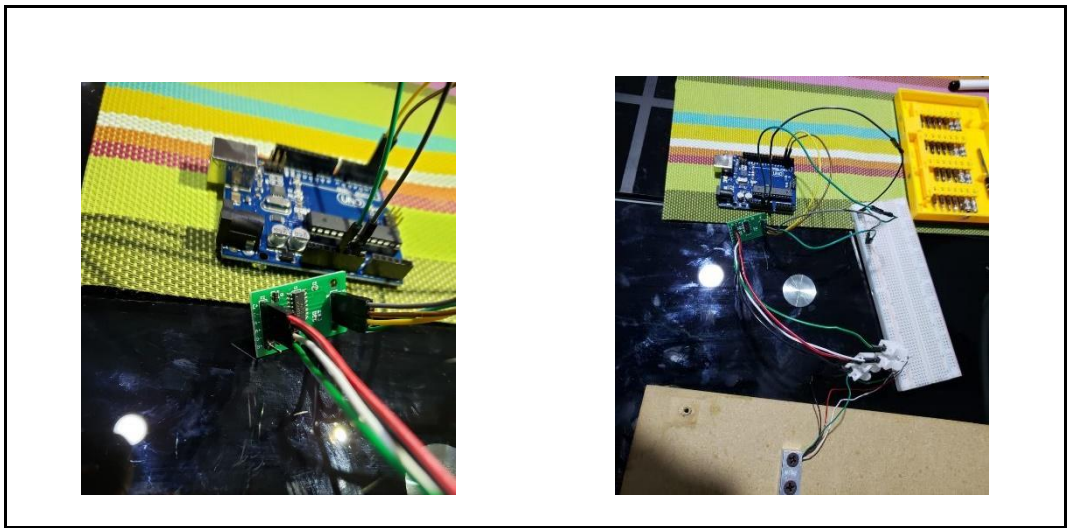


Figura 17. Desarrollo del prototipo con sensores
Fuente: imagen propia.

3.3.3.2 Prototipo con teclado mecánico

Este prototipo consta de un teclado mecánico que se une por medio de un cable USB al Arduino uno. El teclado es de la marca Corsair y tiene teclas tipo Cherry MX Red.

Sin embargo, al igual que el otro diseño, este producto presenta dificultades que también pueden complicar la construcción del prototipo:

- Falsas lectura de los vectores de presión ejercidos con las teclas: el problema principal es que, en las últimas cuatro décadas de existencia de teclados mecánicos, no se han creado códigos para la lectura de dichos vectores, lo cual representa el problema principal.
- El costo de los teclados mecánicos: estos dispositivos pueden llegar a ser bastante caros, dependiendo de la calidad de los sensores que contengan y la marca.

Sin embargo, también hay ventajas. Como se mencionó anteriormente, estos dispositivos tienen mucho tiempo en el mercado y esto ha permitido la creación de varios modelos de teclados y varios componentes, lo que facilita que, en el caso de un fallo, pueda ser reemplazado en partes o por completo.

Tomando en cuenta estas características, se creó un algoritmo para este prototipo donde las medidas recolectadas en las entradas del usuario son:

- Tiempo de presión: medida en milisegundos del tiempo en el que una tecla está siendo presionada.
- Velocidad: es un valor numérico calculado por el intervalo de tiempo desde que se presiona la primera tecla hasta que se presione la última. La mayor dificultad con este punto era determinar en qué momento el usuario deja de presionar teclas, por lo que se crea un tiempo máximo existente entre la presión de las teclas; pasado dicho tiempo sin presionar una tecla, se considerará que el usuario terminó de escribir en el periférico.



Figura 18. Desarrollo del prototipo con teclado mecánico.
Fuente: imagen propia.

3.3.4 Mejorando el prototipo con la seguridad informática

El objetivo del proyecto es generar un nuevo dispositivo de *hardware* que mejorará los paneles existentes. Si a esto le sumamos lo aprendido a lo largo de la maestría, permite la integración de controles para mejorar la seguridad.

3.3.4.1 El proceso del sistema

Para poder explicar la unión del dispositivo a la seguridad informática debemos ver el proceso global del sistema (definiendo el sistema como el conjunto de *software* y *hardware* necesario para lograr el objetivo).

En la figura 17 podemos observar el diagrama de procesos global del sistema:

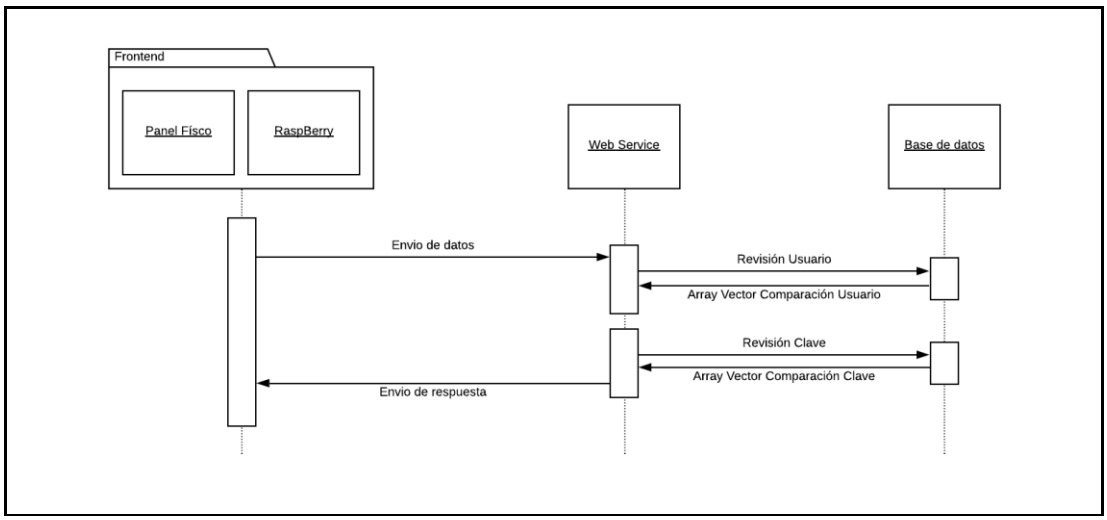


Figura 19. Diseño de procesos

Fuente: imagen propia.

Podemos ver que el sistema estará dividido en tres capas principales. La primera capa es llamada *FrontEnd*, compuesta por el teclado mecánico y un sistema de procesamiento (puede ser un *Raspberry* o un Arduino). Esta capa se encarga de la captura de los datos de usuario y de mostrar la respuesta, correcta o errónea, de las validaciones efectuadas en el sistema.

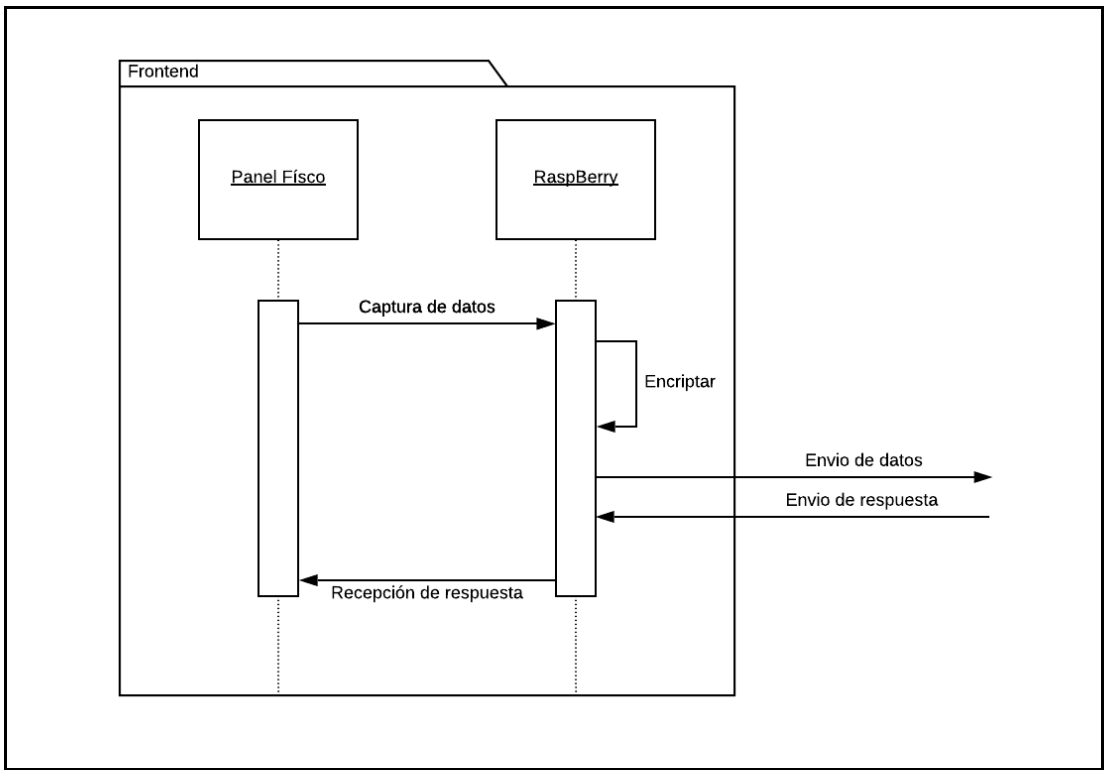


Figura 20. Capa de presentación
Fuente: imagen propia.

La segunda capa del sistema es un *Web Service*. Este es el *Core* de la aplicación, ya que es el que tiene el algoritmo de comparación. Además, es en esta capa donde se reciben los datos encriptados de las otras capas; por lo tanto, debe tener la capacidad de desencriptarlos para poder procesarlos.

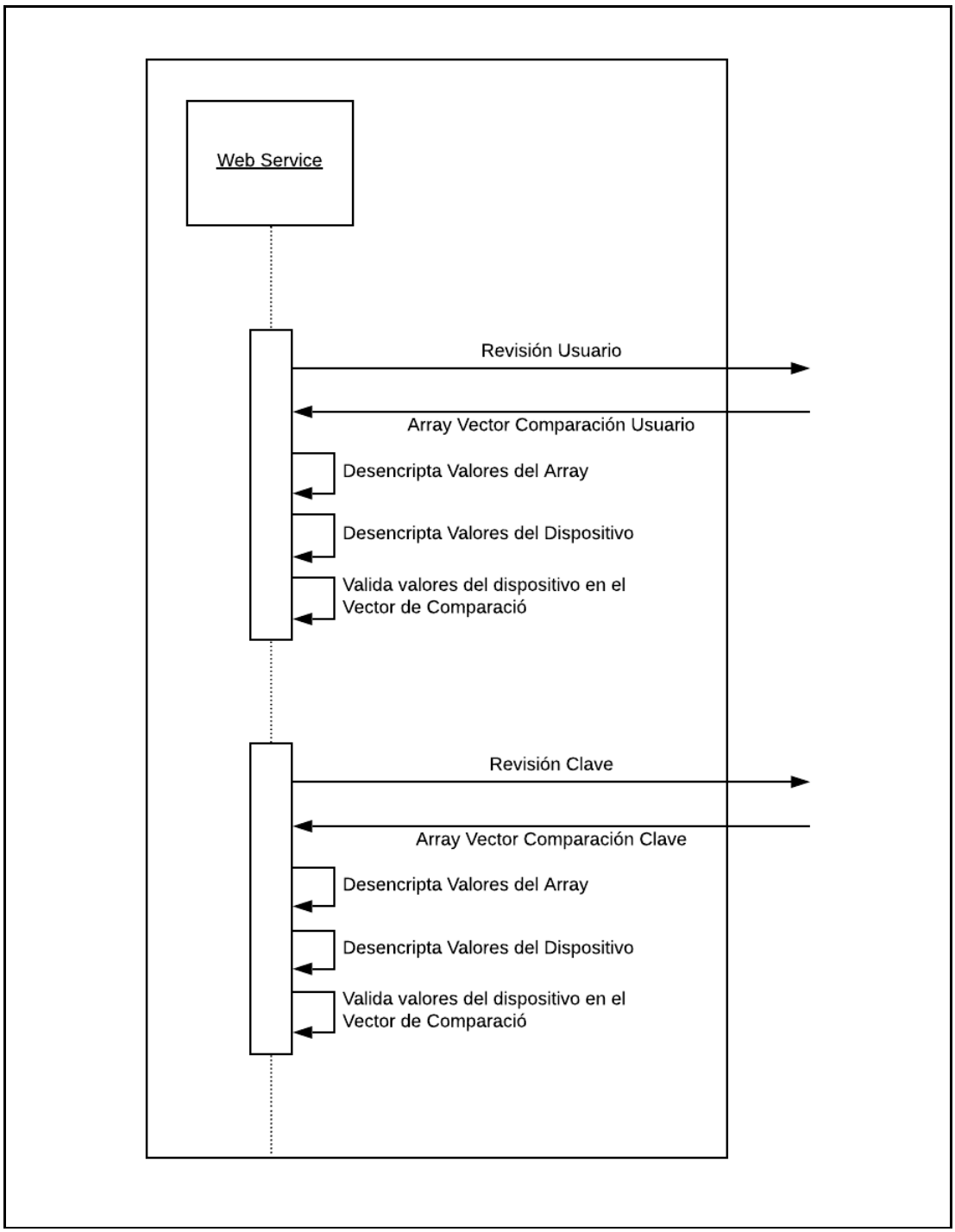


Figura 21. Capa de Lógica (*Web Services*)

Fuente: imagen propia.

La última capa es donde se encuentra la *base de datos*. En ella vamos a almacenar todos los datos tanto de los usuarios como de los dispositivos, además de otros datos como una bitácora de errores y otra de incidentes, las cuales pueden servir para el mejoramiento del sistema y el monitoreo de los activos que están siendo resguardados.

La comunicación entre las capas *FrontEnd* y *Web Services* estará completamente encriptada.

Esta división de capas está pensada para un sistema que esté 100% conectado a una red. Una variación que se le puede hacer a este sistema es unificar todas las capas en el panel físico, lo que puede eliminar la conexión a la red. Esto tiene ventajas y desventajas, ya que hay ciertas características extra que no se podrían utilizar.

3.3.4.2 La base de datos

En el momento de la proyección inicial, se planteó la importancia de preservar los datos, desde el almacenamiento de bitácoras hasta la información relacionada a cada usuario. Debido a este detalle, se toma la decisión de crear la implementación de una base de datos.

Una de las aristas importantes en la creación del sistema es cubrir la necesidad de que llegue a ser de bajo costo, permitiendo la competencia con productos que existen en el mercado. Dada esta premisa, se optó por una base de datos relacional soportada en un sistema gestor de libre distribución como es MySQL.

3.3.4.2.1 Los controles en la base de datos

En esta sección se va a hablar un poco de los mecanismos que se utilizarán para asegurarnos de contemplar y mantener la seguridad en el sistema, específicamente en el área de la base de datos.

3.3.4.2.1.1 Inventario de tablas

La información es el activo más importante de una empresa. Como estamos manejando dicho activo en un solo lugar, debemos tener un mapa para saber exactamente dónde guardamos cada dato.

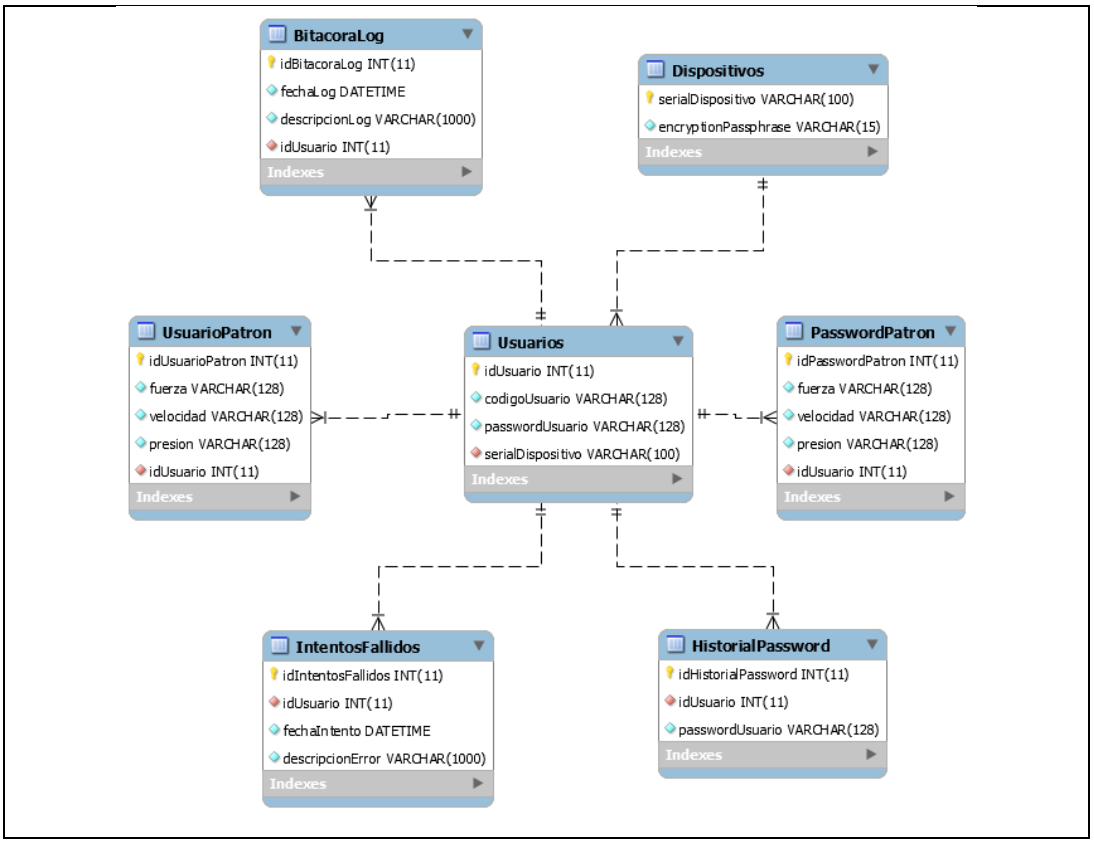


Figura 22. Modelo entidad relación

Fuente: imagen propia.

Como muestra la figura 20, esas son las tablas del sistema y la relación que tiene cada una. A continuación, se explica un poco más sobre ellas.

1. **Dispositivos**: en esta tabla se almacena la información de todos los dispositivos que tenemos en capa de presentación. Esta tabla está pensada para cuando se necesite

más de un dispositivo con esta nueva tecnología en la organización. Todos los dispositivos deben registrar su número de serie y se les debe generar las llaves de encriptación específicas.

2. **Usuarios**: es aquí donde se almacena la información relacionada con cada usuario. Entre los datos más relevantes tenemos nombre de usuario, contraseña y dispositivos asignados.
3. ***PasswordPatron***: esta es una tabla que se encarga de almacenar la nueva huella biométrica del usuario con respecto a las contraseñas ingresadas.
4. ***UsuarioPatron***: tabla que se encarga de almacenar la nueva huella biométrica del usuario con respecto al nombre de usuario ingresado.
5. ***BitacoraLog***: es en esta tabla en donde vamos guardando información que tenga que ver con errores que puedan surgir en el uso de nuestra aplicación; acá también se almacenan incidentes ocasionales.
6. **IntentosFallidos**: en esta tabla almacenamos los intentos fallidos de un usuario para que, en caso de superar el límite de intentos predeterminados por el administrador, se le pueda hacer un bloqueo automático.
7. ***HistorialPassword***: esta es una tabla histórica que nos permite almacenar la información de las contraseñas pasadas utilizadas por un usuario. Esto ayuda a mejorar la seguridad, ya que no permitirá al usuario ingresar contraseñas utilizadas en los últimos N cambios hechos. Este valor será parametrizable y se podrá cambiar solo por el administrador de forma global. Las contraseñas van a estar encriptadas.

3.3.4.2.1.2 Sensibilidad de los datos

Al hablar de la sensibilidad de los datos nos encontramos frente a un término muy subjetivo; este dependerá mucho de la organización con la que se trabaja y las políticas establecidas, aunque muchos pueden alegar que son los datos que la ley establece y protege.

En el caso de esta base de datos, se consideraron tres clasificaciones para los datos a manejar:

- **Estrictamente sensibles:** todo dato que pueda comprometer la seguridad e integridad del sistema completo. Estos se manejan con encriptación.
- **Sensibles**: son datos que no comprometen la seguridad o integridad del sistema, pero pueden dar información de un usuario en específico. En este caso se maneja por enmascaramiento.
- **No sensibles**: cualquier otra información que se guarde en la base de datos. Estos no comprometen la seguridad o integridad del sistema o de los usuarios.

3.3.4.2.1.3 Políticas de respaldos

Un respaldo se puede definir como una copia fidedigna de un dato, la cual es una copia exacta de dicho valor inicial. Estas se realizan con el fin de tener una forma rápida y sencilla de recuperar información en caso de ser necesario.

Estas son algunas características que los respaldos deben tener o cumplir:

- Confiabilidad del respaldo
- Constancia en los respaldos
- Cumplir con las políticas corporativas RPO/RTO

Se debe desarrollar una política que contemple:

- Estrategias de respaldo basadas en las necesidades del negocio
- Definir necesidades de almacenamiento actuales y futuras
- Definir los responsables de cada proceso

Se recomienda la inclusión de los siguientes puntos en las políticas de respaldo para este sistema:

- Mantener consistencia en el plan de respaldo para cada dispositivo con esta huella biométrica que se encuentre en la organización. Al tener un solo proceso "homologado" para todos los dispositivos se asegura que los datos van a ser respaldados correctamente y que estos pueden ser restaurados en el momento que se amerite, manteniendo siempre el mismo formato y reglas de negocio.
- Establecer métricas claras, medibles y con facilidad para corroborar que los respaldos se hagan de forma correcta. En el transcurso del ciclo de vida del dispositivo se mostrarán estadísticas en cada uno que se repetirán con el tiempo.
- Implementar procesos que se cumplan a cabalidad para así tener siempre respaldos íntegros y constantes. Se recomienda a futuro tratar de automatizar dichos procesos.
- El tiempo sugerido para los respaldos es de una semana; se realizarían en el momento de menor afluencia de datos.

3.3.4.2.1.4 Plan de recuperación

En el momento que se está creando un plan de respaldos se debe pensar inmediatamente en un plan de recuperación, proceso que cubre los datos que permiten a una organización comenzar de nuevo sus operaciones en caso de un desastre, pérdida o ataque.

Se deben seguir casi los mismos lineamientos que se utilizan en el plan de respaldos y pensar en reglas de negocios que puedan tener un valor agregado para este punto. Este documento es uno de los que no se espera utilizar, pero no puede faltar entre la documentación fundamental de la organización.

Un plan de recuperación crea una mejora en la imagen de la organización, ya que permite a los usuarios notar que se preocupan por sus datos y que tienen planes alternos para la puesta en marcha de todos los procesos. Por este motivo, el nuevo sistema de huella biométrica debe estar integrado a este plan.

Algunos elementos que se deben tener en cuenta al momento de generar un plan de recuperación son:

- Definir tiempo de recuperación de datos
- Definir estrategias de recuperación de datos
- Definir los responsables de cada proceso
- Definir el lugar de almacenamiento de los respaldos

3.3.4.2.1.5 Plan antirrobos de la información

Para la creación y puesta en marcha de este plan se debe conocer la información que se está protegiendo. Teniendo en cuenta este dato, se puede calcular el impacto que pueda causar su pérdida y el impacto de esfuerzo para crear medidas de protección.

En el caso de la base de datos del dispositivo, se están tomando en cuenta varias medidas:

- **Inventario de base de datos:** se hace un registro de los lugares donde se va a almacenar la información (ver apartado 3.3.4.2.1.1).
- **Sensibilidad de datos**: es una clasificación de los datos que se están guardando. En este se ve también el tratamiento que se le otorga (ver apartado 3.3.4.2.1.2).
- **Codificación segura**: por la forma en que está creado el sistema, solo existe una forma de entrada y salida en la comunicación con la base de datos. Se da gracias a un *Web Service* que se encarga de hacer todas las transacciones pertinentes. Es en este componente donde se llegaron a implementaron varios puntos de control (ver apartado 3.3.4.3).
- **Uso de encriptación y enmascaramiento**: esta es la parte fundamental del aplicativo para evitar el robo de información; los datos más sensibles que se explicaron anteriormente se van a tratar según su clasificación y cada nivel tendrá un método que se usará para el almacenamiento de los datos. El uso de encriptación

se explica en el apartado 3.3.4.2.4 y del enmascaramiento se explica en el apartado 2.3.4.2.3.

3.3.4.2.1.6 Cuentas fuera de uso

Uno de los problemas más grandes de todo sistema es la cantidad de usuarios que son creados y a los que con el tiempo no se les da el mantenimiento adecuado. En muchas ocasiones, estos descuidos se traducen en que seguimos guardando información de usuarios que ya no se encuentran en la organización y, en los peores casos, con los permisos activos.

Teniendo esta problemática real en mente, se dispuso dos formas para evitar que esta amenaza se materialice. La primera es la funcionalidad que permite a un administrador hacer la eliminación "temporal" de permisos (por motivo de salidas, vacaciones o viajes; el estado del usuario cambia a suspendido) o el borrado "permanente" de un usuario en el sistema.

La segunda forma es por medio de una tarea programada que se realiza todos los días; esta va a revisar los usuarios que están bloqueados y si llevan un mes en este estado, se eliminarán permanentemente.

Un administrador puede cambiar el estado de un usuario de bloqueado a suspendido para evitar eliminaciones no deseadas del sistema.

3.3.4.2.1.7 Políticas de parches y actualización

Todo sistema debe cumplir con los ciclos de vida. Parte importante de esto es el mantenimiento y la actualización.

En el caso de la base de datos, ya que el sistema usa MySQL, se debe estar atento a las vulnerabilidades, parches y actualizaciones que surjan con el tiempo. Este motor de base de datos tiene un soporte activo y ocasionalmente se liberan nuevas versiones.

3.3.4.2.2 La nueva huella biométrica

Como se ha mencionado en apartados anteriores, la nueva huella biométrica va a estar compuesta por un vector de tres valores: velocidad, fuerza y presión. Este vector se almacenará en la base de datos en las tablas de patrones que corresponden al usuario y a la contraseña.

Dado que cada persona tiene una huella biométrica única, esta se debe almacenar en nuestra base de datos; para aumentar la seguridad de dicho almacenamiento se utiliza el enmascaramiento de datos por medio de una semilla personalizada.

Esta huella biométrica presenta un problema importante relacionado con el portador. El ser humano es una variable que casi nunca llega a ser constante. La huella puede que varíe en su composición haciendo que una comparación directa cause falsos negativos en el momento de la autentificación. Para solucionar esta problemática se ideó un sistema de control.

Se van a almacenar como mínimo cinco vectores de huella biométrica (por cada valor usuario y contraseña). Estos valores van a dar un rango en el cual un usuario puede ser identificado y autentificado. Este valor no puede ser de un rango muy grande, ya que los usuarios no van a variar tanto al momento de interactuar con el sistema, y esto se debe especificar en el manual de usuario y en cualquier entrenamiento otorgado.

Teniendo esta modificación en la forma tradicional de guardar valores, al almacenar un conjunto de vectores permitimos al sistema tener un aprendizaje constante. Un usuario que

interactúe varias veces con el sistema va a familiarizarse con él. Esto da como resultado que el vector de huella digital aumentará en velocidad. Para lograr que el sistema aprenda debemos reemplazar el valor más antiguo almacenado en el conjunto de vectores. Esta es la clave para lograr que el sistema evolucione junto a sus usuarios.

3.3.4.2.3 La semilla y el enmascaramiento de los datos

Como se mencionó en el apartado anterior, hay ciertos datos que antes de ser guardados van a ser enmascarados para aumentar la seguridad del sistema.

El algoritmo de enmascaramiento es bastante sencillo. Se va a generar una semilla en el momento que se haga el registro de un nuevo dispositivo. Para poder formar la semilla debemos saber:

- La suma de los componentes de la fecha con hora del registro del dispositivo [FRD].
- Cantidad de caracteres en el número de serie [SL].
- Suma del valor numérico de la serie. Este puede estar compuesto por letras y números. En el caso de las letras se obtiene su valor numeral en el alfabeto [SN].

Corresponderá a la siguiente fórmula matemática:

$$Semilla\ = (FRD * SL + SN)\ \%\ 100$$

Esta fórmula da un valor numérico decimal que será utilizado para enmascarar los valores del vector. Este se almacena en la tabla “Dispositivos”.

3.3.4.2.4 Las llaves públicas y privadas

Una de las formas más seguras para mantener en privado la información es por medio de encriptación de datos, claro que la encriptación será tan segura como el método y “el secreto” que usemos para hacer el proceso.

En la actualidad, uno de los métodos más utilizados es la criptografía asimétrica; este método se basa en el uso de un par de claves que se crean en un mismo dispositivo (el que recibe el mensaje). Una de estas será pública (la cual se comparte al mundo) y la otra será privada (que se guarda en un lugar seguro). Este tipo de métodos criptográficos garantizan que esa dupla de claves solo se pueda generar una única vez, lo que hace casi imposible que dos personas hayan obtenido casualmente la misma dupla de claves. Este tipo de encriptación permite que la llave pública se utilice solo para hacer cifrado mientras que la llave privada será utilizada principalmente para descifrar los mensajes. Aunque la llave pública puede hacer cifrado, su uso no es tan relevante.

Debido a esta premisa se decide el uso de llaves públicas y privadas para el cifrado de datos sensibles en el sistema. Este proceso recae en el componente llamado *Web Service*.

En el momento del registro de un nuevo dispositivo, ambas llaves serán generadas; posteriormente, se hará el envío de cada una a su respectivo lugar de almacenamiento, la pública que se guardará en el dispositivo y la privada quedará almacenada en la base de datos.

Para darle un poco más de protección en el sistema, se tomó la decisión de proteger la llave privada en el momento de ser almacenada en la base de datos; para esto se va a hacer uso de la funcionalidad de encriptar que tiene el método AES, utilizando una frase que el administrador registra en el sistema. Esta frase debe ser única por dispositivo.

3.3.4.3 El código dentro del *Web Service*

Esta sección es una de las más importantes en este sistema. Es acá donde se coloca la mayor parte de la lógica de negocio.

La forma de definir un *Web Service* hace que sea óptimo para este trabajo. Al ser un componente cerrado que se comunica con otros sistemas o componentes por medio de interfaces, es posible tener la lógica del negocio encapsulada para evitar fuga de información, pero con funciones tan completas y robustas que permitan a otros componentes poder obtener la información necesaria y cumplir con sus objetivos.

El *Web Service* tiene los siguientes servicios:

- Conexión a base de datos por medio del *singleton*.
- Verificación de usuario y contraseña.
- Corroboración del vector biométrico contra el vector de comparación alojado en la base de datos para los campos de usuario y contraseña.
- Módulo de mantenimiento de usuarios.

Estos son los servicios que se espera que a futuro se implementen:

- Módulo administrativo
- Módulo de valores parametrizables
- Revisión y mantenimiento de bitácoras

3.3.4.4 El algoritmo de encriptación

Tomando como base que un algoritmo es un conjunto de instrucciones definidas y no ambiguas, ordenadas y finitas diseñadas para llegar a la solución de un problema, podemos mencionar que, aunque se utilizan métodos de encriptación populares, este algoritmo fue diseñado específicamente para este dispositivo.

Para la creación de este algoritmo se determinó utilizar RSA. La decisión se dio ya que la seguridad de este algoritmo radica en el problema de la factorización de números enteros. Esto permite que, al obtener dos valores primos al azar y mantenerlos en secreto, la posibilidad de que dos pares de llaves sean idénticas tienda a cero.

Este algoritmo está pensado para prevenir quedarse atrás, ya que su tamaño crece con el aumento de la capacidad de cálculo de las computadoras. Por algo lleva más de cuatro décadas en el mercado, evolucionando con la tecnología.

Las características del algoritmo creado son las siguientes:

- Una longitud parametrizable que se define de forma predeterminada como 2048 bits. Este se puede modificar en cualquier momento.
- Se generan dos llaves por dispositivo, una se guarda en la base de datos (privada) y la otra se almacena en el dispositivo (la llave pública).

3.3.4.5 Las reglas del juego

En esta sección se tratarán ciertas reglas necesarias para el uso óptimo del nuevo sistema biométrico. Es una sección informativa donde se especifican asuntos como el tiempo de vida de la huella biométrica, uso y manejo de los datos de un usuario, datos que se almacenan, entre otros.

3.3.4.5.1 El aprendizaje de la huella biométrica

La huella biométrica, como se ha mencionado, representa datos almacenados directamente en la base de datos. Se obtienen de la interacción del usuario con el sistema.

La huella biométrica es un conjunto de valores que se va a ir recolectando con el tiempo; al ser un conjunto, se le llama vector de comparación biométrico. Al final, es un conjunto de cinco[1] vectores biométricos, estos son los que se usan para la comparación de los patrones. Estas huellas están en constante evolución, ya que en cada ingreso correcto de un usuario se va a reemplazar el valor más viejo de la tabla.

[1] Este valor es el predeterminado, pero el administrador lo puede modificar.

3.3.4.5.2 El tiempo de vida de los datos de usuario

El tiempo definido para los datos de usuario va a ser finito. Se van a eliminar en el momento que no sean necesarios y, en la mayoría de los casos, es cuando el usuario ya no se encuentre colaborando con la organización.

3.3.4.5.3 Bitácora de errores de conexión

Todo sistema debe poder ser auditable, razón por la cual se decide hacer una tabla de bitácora para almacenar todos los errores de conexión que se den en el sistema. Esto permitirá conocer los puntos más vulnerables de una organización y hasta los eslabones más débiles de la compañía, al darnos cuenta cuáles usuarios son a los que se les ha intentado vulnerar.

3.3.4.5.4 Bitácora de incidentes

Ningún sistema de *software* está libre de errores. La mejor forma de encontrarlos y solucionarlos es por medio de una bitácora de incidentes.

Acá se almacenarán los casos atípicos de la ejecución de nuestro sistema, lo que permitirá detectar irregularidades presentadas por mal funcionamiento o ataques efectuados por terceros.

3.3.4.5.5 Reglas de los usuarios

Como cualquier sistema de seguridad, debemos crear una política para los usuarios del sistema. Entre las reglas que los usuarios deben seguir se encuentran las siguientes:

- Todo usuario registrado en el sistema tendrá:
  - Clave: un número compuesto por seis caracteres.
  - Usuario: un número compuesto por cuatro caracteres.
  - Vector de comprobación biométrica:
    - Cinco registros para el código usuario.
    - Cinco registros para la contraseña.

- Un correo electrónico.

- El correo electrónico es el medio por el cual el sistema le informará al usuario eventualidades como: contraseña pronta a vencer, usuario bloqueado, usuario programado a eliminación.
- Las claves de los usuarios tienen un tiempo de vida. Este será determinado por el administrador del sistema, aunque de forma predeterminada es de seis meses.
- En el momento que se debe actualizar la clave, esta no puede ser igual a las últimas cuatro almacenadas o el valor que especifique el administrador.
- El usuario tiene un mes (o el tiempo que sea predeterminado por el administrador en el sistema) para hacer la actualización de la clave, desde el momento que esta expira. Pasado el mes, si no existe una actualización, el usuario se colocará en estado bloqueado.
- El usuario y la contraseña son privados y deben cuidarlos. Aunque este sistema venga a prevenir este tipo de situaciones, el usuario debe ser consciente de que compartir dichos datos es una violación a la seguridad de la organización.
- El usuario quedará bloqueado después de tres intentos fallidos de ingreso al sistema. Deberá comunicarse con el administrador para hacer el proceso de liberación de un usuario.
- Si un usuario queda, en un periodo de un mes, sin hacer ingreso correcto a los sistemas después de ser colocado como bloqueado, el sistema lo eliminará de la base de datos de forma automática.
- El administrador puede suspender a un usuario para darle de baja temporalmente; sus datos permanecerán en el sistema y serán accesibles en el momento que vuelva a estar activo.

3.3.4.6 Módulo de administración

El sistema debe tener un módulo web para la administración de todos los dispositivos. En el caso de este prototipo, el sistema no cuenta con dicho módulo web, pero posee una

versión en consola que permite efectuar las funciones que están creadas para el administrador.

Funciones existentes:

- Registro de usuarios
- Registro de dispositivos
- Desbloqueo de un usuario específico

Funciones por construir:

- Manejo de errores y bitácoras
- Manejo de mantenimiento de datos
- Estadísticas
- Envío respaldos por correo electrónico
- Eliminación de usuarios inactivos
- Reemplazo de dispositivos

3.3.4.6.1 Registro de dispositivos

Considerando el ecosistema de los nuevos dispositivos, se está pensando que cada vez que se agrega un prototipo nuevo, este es registrado en el sistema. Para esto se procede a registrar el número de serie del dispositivo, generar una semilla y un par de llaves.

El número de serie será el identificador del dispositivo. También se va a usar para hacer la semilla uniéndose a la fecha del registro. Esta semilla se va a usar para enmascarar los datos de los vectores (usuario y contraseña). Las llaves van a ser dos, una pública y otra privada. Dichas llaves se van a usar para agregar encriptación al sistema. Ambas se generan en el servidor en el momento del registro del dispositivo; la privada se guarda en base de datos y la pública se envía al dispositivo para poderla almacenar.

3.3.4.6.2 Registro de usuarios

Uno de los insumos más importantes del sistema son los usuarios. Al momento de hacer el registro de uno nuevo, se deben guardar los siguientes valores:

Código de usuario

- Contraseña.
- Dispositivo asignado.
- Registro mínimo de los vectores para usuario y contraseña; por defecto son cinco.
- Fecha de ingreso de contraseña (esta fecha se actualizará cada vez que se cambie la contraseña).

Para el momento de la creación de este prototipo se hizo una versión más pequeña del sistema; se espera que en futuras entregas se pueda hacer el almacenamiento de otros datos del usuario como el correo electrónico, nombre y apellidos.

3.3.4.6.3 Mantenimiento de los usuarios

Como cualquier información que se guarde en la base de datos, esta debe recibir mantenimiento. Es de suma importancia que la clave de cada usuario se actualice en un periodo no mayor a los seis meses. No obstante, este valor de tiempo puede ser configurado por el administrador.

Además, cada vez que se hace un cambio de contraseña se deben agregar los valores de los vectores tanto para el usuario como para la contraseña. Este proceso se debe efectuar por el valor predeterminado por el administrador para la cantidad mínima de vectores (se recomiendan cinco registros). Estos se utilizan para hacer la comparación en los intentos de autorización y autenticación de un usuario.

Los usuarios deben ser retirados del sistema en el momento en que ya no sean necesarios. En caso de que no se lleve a cabo dicha tarea, el sistema contará con un proceso de eliminación de usuarios bloqueados con mucho tiempo de inactividad.

3.3.4.6.4 Manejo de los usuarios bloqueados

El sistema tiene un mecanismo de bloqueo; este mecanismo se puede activar de dos maneras. La primera es cuando un usuario intenta entrar al sistema y falla varias veces por cualquier motivo. Esto coloca al usuario en estado bloqueado y para hacer el desbloqueo de la cuenta debe contactar al administrador.

La segunda forma de que se active este mecanismo es por inactividad de los usuarios. Como se mencionó en el apartado anterior, el periodo de vigencia de una contraseña será designado por el administrador.

Por defecto, el sistema tiene seis meses como tiempo para hacer el cambio de contraseña; pasado ese tiempo, el usuario se coloca en estado bloqueado. Si un usuario no hace la actualización en menos de un mes, será colocado como inactivo y tiene una semana antes de ser eliminado definitivamente del sistema de forma automática.

3.3.4.6.5 Manejo de fallos

Como cualquier sistema, este está creado para funcionar siempre de la mejor manera, pero en el caso de que un fallo o error se genere, se va a tener un sistema de bitácoras donde se guarda información que pueda ayudar a entender su naturaleza.

Se tienen dos tipos de bitácoras. La primera está dirigida a recolectar datos de fallos del sistema y la segunda, a incidentes con las funciones del sistema. La diferencia principal recae en que los incidentes reflejan cualquier anomalía en el manejo de usuarios, contraseñas, registros y administración.

Estos logs podrán ser accedidos por medio del módulo del administrador y podrán ser descargados para su análisis.

De igual manera, el *Web Service* tendrá una función predeterminada para enviar, por correo y cada seis meses, el log de incidentes y de errores. Estos se guardan en un zip y se usa la semilla como contraseña.

3.3.4.6.6 Manejo de datos antiguos

El sistema crecerá con cada dispositivo o usuario que se agregue. Se debe tener en cuenta que los datos quedarán disponibles en la base de datos.

Es responsabilidad del administrador hacer el manejo de datos del sistema, esto incluye el respaldo y eliminación de datos obsoletos.

Como se mencionó, se crearon herramientas dentro del módulo de administración para mejorar dicho proceso, como por ejemplo eliminar usuarios inactivos, enviar respaldos de bitácoras y limpieza de bitácoras.

Conclusiones

Tras el desarrollo de este documento, se puede llegar a concluir que:

1. La falta de innovación en los dispositivos para resguardar la seguridad perimetral ha ocasionado brechas de seguridad, los paneles físicos pueden ser vulnerados fácilmente.
2. El estudio del NEUROQWERTY posee aplicaciones no solo médicas, sino también en el área de la tecnología. El uso de la huella biométrica propuesta en este documento puede ayudar a cambiar la forma de implementar la seguridad actual y mejorarla exponencialmente.
3. El almacenaje de las contraseñas siempre es un problema más en paneles físicos, ya que normalmente solo se puede crear una sola clave y esta se comparte con todos los usuarios.
4. La funcionalidad actual del panel físico es muy básica, consiste únicamente en limitar accesos mediante un código. Introducir nuevas opciones es posible y rentable gracias a los avances tecnológicos actuales.
5. Aunque existen muchos sistemas perimetrales en la actualidad, la mayoría son muy rudimentarios y omiten funciones de notificación en tiempo real. Aunque en el mercado podemos encontrar modelos que efectúen dichas funciones, su precio llega a ser elevado.
6. El análisis de los resultados de la puesta en práctica en un ambiente controlado es de suma importancia, ya que permite obtener información sobre el uso y mejoras que pueda necesitar el proyecto.

Recomendaciones

Las siguientes líneas son algunas recomendaciones que surgieron tras la investigación de esta nueva propuesta.

1. Se recomienda utilizar las especificaciones del prototipo base de esta tesis para crear un nuevo *hardware* que mejore la seguridad de los paneles físicos.
2. Se recomienda el uso de huella biométrica para la protección de activos, debido a que esta funciona como un identificador único e irrepetible para cada usuario.
3. Se recomienda el uso del algoritmo creado en el proyecto para autentificar a los usuarios y así evitar el ingreso de personal no autorizado a los activos que queremos proteger, sin importar si consiguen la clave de algún usuario.
4. Se recomienda aumentar las funcionalidades del dispositivo para tener un valor agregado en comparación con otros productos existentes en el mercado. Como base se pueden utilizar las descritas dentro de este documento; sin embargo, se pueden extender aún más.
5. Se recomienda el uso de funcionalidades para alertas tempranas. Esto permite mitigar y eliminar brechas de seguridad, creando una mayor confianza en el manejo de los activos. Estas funciones pueden ser encontradas en algunos dispositivos (como el prototipo que se presenta en el documento) o por medio de la tecnología actual.
6. Debido a lo ambicioso del proyecto, se recomienda continuar buscando métodos que permitan mejorar el dispositivo planteado, haciendo uso de los últimos avances tecnológicos del mercado y creando siempre pruebas controladas que puedan analizarse, de manera que sean las ideales para mejorar el proyecto.

Bibliografía

Arduino. (2020). *What is Arduino?* Recuperado de https://www.arduino.cc/

Corrales, H., Cilleruelo, C. y Cuevas, A. (2014). *Criptografía y métodos de cifrados*. Recuperado de http://www3.uah.es/libretics/concurso2014/files2014/Trabajos/Criptografia%20y%20Metodos%20de%20Cifrado.pdf

Deskthority Wiki. (2017). *Alps SKCL/SKCM series*. Recuperado de https://deskthority.net/wiki/Alps_SKCL/SKCM_series

García, J. L. (2012). *Tecnología: la historia del teclado convencional de las máquinas de escribir*. Recuperado de https://campus.fundec.org.ar/admin/archivos/MAETIC - QWERTY.pdf

Giancardo, L., Sánchez-Ferro, A., Butterworth, I., Mendoza, C. y Hooker, J. (2015). Psychomotor Impairment Detection via Finger Interactions with a Computer Keyboard During Natural Typing. *Sci Rep* 5, 9678. https://doi.org/10.1038/srep09678

IBM (1983). *Technical reference.* Recuperado de http://ps-2.kev009.com/basil.holloway/ALL PDF/IBM5160TechRef.pdf

Mathias Corporation. (2013). *The world´s quietest mechanical keyswitches*. Recuperado de http://matias.ca/switches/quiet/