7. PROTOTIPO DE SEGURIDAD PARA EL RESGUARDO DE LA INFORMACIÓN FÍSICA

HELBER BÁEZ-RODRÍGUEZ | helbert.baez@cetcolsubsidio.edu.co

Corporación de Educación Tecnológica COLSUBSIDIO – AIRBUS GROUP, Bogotá – Colombia.

Palabras clave: Seguridad, Infraestructura, Tecnologías de la Información y la Comunicación.

Resumen: Hoy en día, la seguridad de la información en las empresas se está convirtiendo en una gran necesidad, debido a los constantes ataques a los que se enfrentan a nivel informático. Las intrusiones se ven reflejadas a nivel lógico, pero también se encuentran vulnerabilidades a nivel físico que han perdido notoriedad por el auge de la atención de los especialistas en los ciberataques.

El acceso de personal no autorizado a los sitios donde se encuentran los equipos de infraestructura tecnológica de alto valor económico, por ejemplo, es un elemento de la seguridad poco trabajado en las compañías. Esta ponencia está enfocada en la exposición del diseño e implementación de un prototipo de protección del hardware mediante un sistema de alerta de personas que acceden sin autorización a ciertos espacios.

El mecanismo trabaja con Arduino y como medio de enlace utiliza Bluetooth y Wifi, generando comunicación con una aplicación móvil que registra los ingresos no permitidos en una base de datos, protegiendo en tiempo real y alertando a los responsables de la seguridad de las injerencias irregulares.

PROTOTIPO DE SEGURIDAD PARA EL RESGUARDO DE LA INFORMACIÓN FÍSICA

1.Introducción

La seguridad de la información y de equipos que hacen parte de la infraestructura de las tecnologías de la información y la Comunicación (TIC) se está convirtiendo en una necesidad y prioridad actual de las empresas. En las organizaciones encontramos que se presentan ataques a nivel de red donde los ciberdelincuentes encuentran vulnerabilidades para ingresar a los sistemas de información. Sin embargo, los ataques también se pueden presentar de forma física. Por ello, autores como Marrero han acuñado el término de seguridad física, el cual se emplea para referirse a las medidas que tengan que ver con la protección externa de los datos [1].
Álvaro Gómez clasifica la intrusión física en dos tipos: Amenazas del personal interno, donde se ven involucrados de manera voluntaria o involuntaria en incidentes de seguridad informática; y amenazas de exempleados, que pueden actuar contra su antigua organización provocando activación de "Bombas Lógicas, las cuales son programas que se activan después de un periodo de tiempo para un fin específico como dañar impresoras, discos duros, robar información" y cuyo medio de infección es el correo electrónico [2]. Inclusive, los intrusos pueden ingresar a un equipo por medio de la suplantación o engaños, entre otros procedimientos.
Por lo anterior, se debe reforzar la seguridad tanto con el personal interno (insiders) como con usuarios externos (outsiders) [3] y se requieren sistemas de apoyo automatizados mediante sistemas informáticos o herramientas de hardware [4] que permitan resguardar la información y protegerla, así como a los equipos tecnológicos que permiten su distribución y manejo. Este proyecto permite proporcionar una nueva alternativa para las empresas ante los grandes cambios en la seguridad de la información, los delitos informáticos, la privacidad, la protección de los datos personales y accesos a la información [5], generando confianza sobre la protección de su información a nivel físico, teniendo un control y seguimiento constante sobre el personal que ingresa a los centros de cableado u oficinas donde se encuentren equipos con información sensible.
A continuación, se expone el proceso para el diseño y la construcción de un prototipo de seguridad para apoyar la seguridad física en las empresas mejorando la productividad de sus procesos [6], al detectar el ingreso no autorizado de las personas a los diferentes ambientes o espacios donde reposan equipos informáticos de alto costo (tecnológicos o de resguardo de la información). El dispositivo funcional detecta un acceso no autorizado y generaría una alerta a través de una aplicación móvil, la cual queda registrada en una base de datos. De esta manera, se implementa un control y registro de acceso, brindando una oportunidad a las organizaciones para resguardar la seguridad de la información, siendo un valor agregado que el prototipo actúa como complemento de otros dispositivos como cámaras, sensores de movimiento y demás controles físicos.

2. Procedimiento Experimental

Mediante los diagramas siguientes, se describen los elementos tecnológicos que interactúan para el diseño del prototipo para el resguardo de la información física y digital y las fases del desarrollo del dispositivo, con el fin de llevar a cabo un procedimiento adecuado e identificar los componentes y los resultados esperados.
Para empezar, el proceso de creación del prototipo se da en seis fases, a saber:

Tabla 1. Fases del Proyecto

ACTIVIDAD	DESCRIPCIÓN
Analizar	Identificar las necesidades de los centros de acopio de equipos que representan un gran valor para la compañía y requieran ser asegurados de manera física.
Planear	Generación y verificación de componentes específicos del prototipo.
Diseñar	Bosquejo del funcionamiento del prototipo.
Pruebas	Experimentación para garantizar la funcionalidad del prototipo.
Evaluar	Medición de la efectividad y recopilación de información mediante registros en la base de datos.
Ejecución y verificación para nuevas pruebas	Corrección de los posibles errores hallados en la fase de evaluación para garantizar un proceso de registro y de alarmas eficiente.

PROTOTIPO DE SEGURIDAD PARA EL RESGUARDO DE LA INFORMACIÓN FÍSICA

Como se describió anteriormente, el primer paso en el diseño del prototipo para el resguardo de la información física y digital es un análisis de las necesidades a las que atiende el dispositivo y sus posibles aplicaciones.

Se identificó que este tipo de sistemas aportan a la seguridad informática en las empresas al evitar amenazas que pongan en riesgo la información y los equipos que la resguardan, fortaleciendo la productividad de las empresas. [7] Las TIC han sido un elemento fundamental en los sistemas para la seguridad y defensa, por lo que estos dispositivos de detección de intrusos vía láser garantizan rapidez, integración, interoperabilidad y seguridad. Estos hallazgos se resumen en la figura 1.

En la segunda etapa, de planeación, se definen los componentes necesarios para la creación del prototipo.

Arduino 1.0: Placa usada como medio para la ejecución de diferentes proyectos, la cual contiene componentes de hardware y software libre para interactuar y hacer uso de recursos electrónicos de bajo costo (Figura 2).

Módulo Emisor Infrarrojo:

Cumple la función de emitir el haz de luz para generar la barrerá en la entrada del área a proteger.

Módulo Receptor:

Se cambia por el Módulo Sensor con Fotocelda, el cual recibe el haz de luz con el fin de limitar la barrera y, de este modo, mediante las configuraciones se generen las alertas en el momento de la interrupción del haz de luz infrarrojo.

Módulo Bluetooth:

Permite la comunicación entre el dispositivo y la aplicación de celular para la interacción y comunicación de los diferentes comandos programados.

Módulo Wifi:

Alternativa de ampliación de cobertura en caso de requerir ampliar el alcance de la señal (actualmente no hace parte del proyecto ya que se tiene una comunicación vía bluetooth). [9]

Realizando las respectivas cotizaciones se adquieren los elementos con los valores descritos en la Tabla No 2.

En cuanto a los módulos receptores, se usó un módulo sensor de fotocelda que cumple con la función de receptor de señal (Figura 3.)

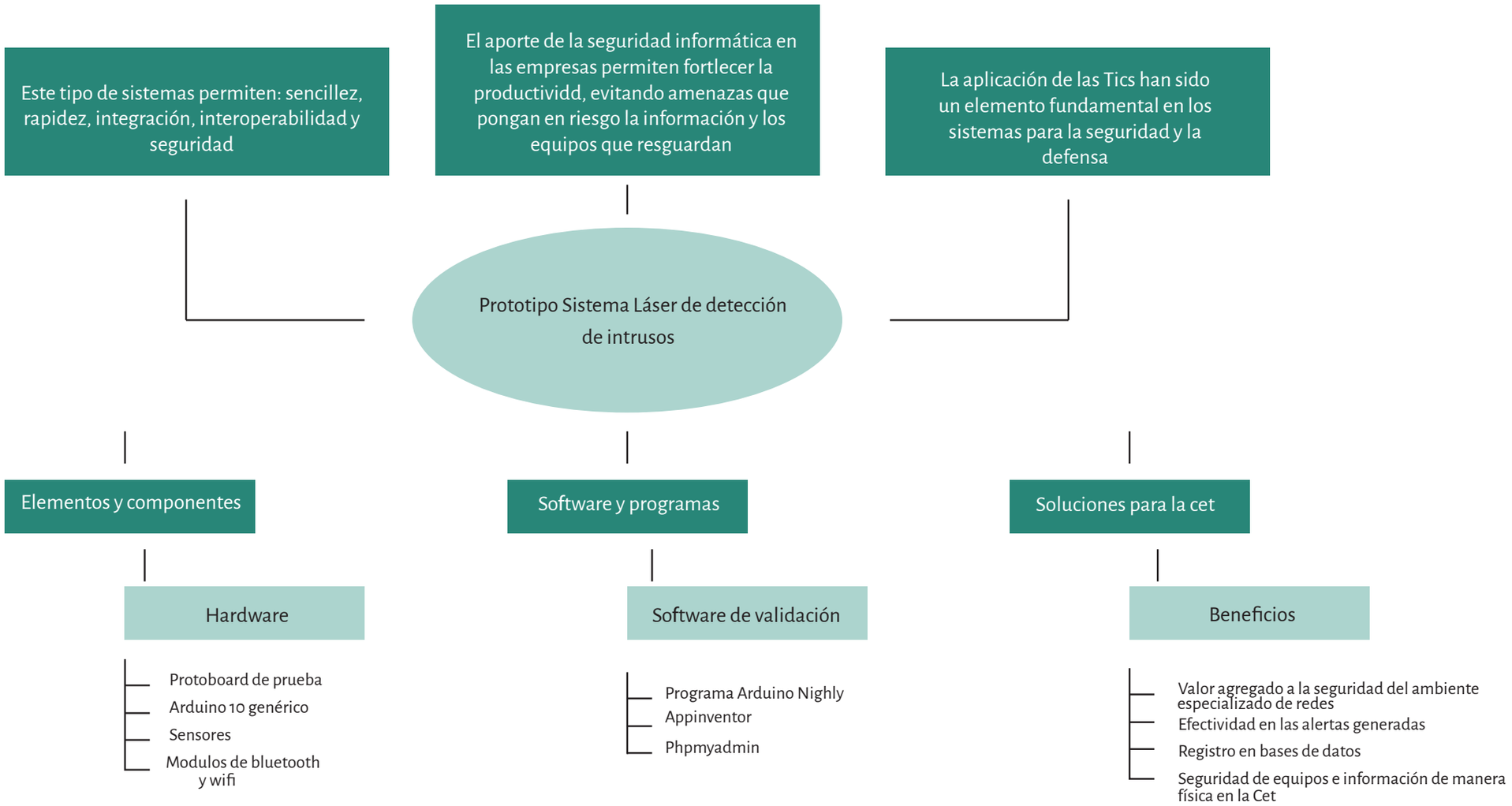

Figura 1. Marco Tecnológico Desarrollo del Proyecto. Tomado de descubrearduino [8]

Tabla No 2. Tabla de Recursos de Hardware y Software

HADWARE	COSTO	SOFTWARE	COSTO
Arduino 1.0	24.000	**Programa Arduino Nighly**	(Software Libre)
Sensor Laser Emisor	20.000	**Appinventor**	(Software Libre)
Sensor Receptor (se cambia por modulo fotocelda)	12.000	**phpmyadmin**	(Software Libre)
Módulo de Bluetooth HC05	15.000	X	X
Modulo Wifi ESP 8266	20.000	X	X
Protoboard y Consumibles generales	35.000	X	X

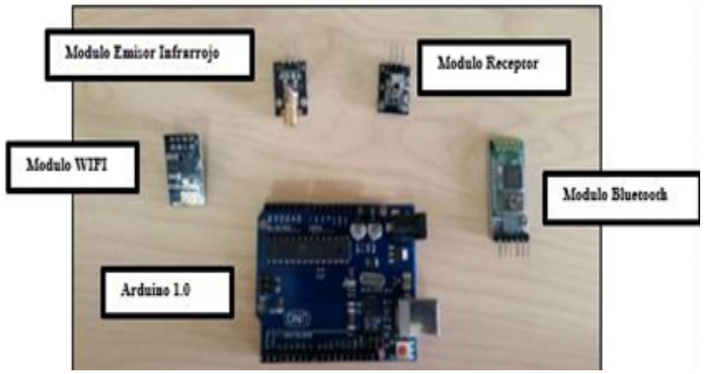

Figura 2. Componentes de trabajo del Proyecto. Fuente propia.

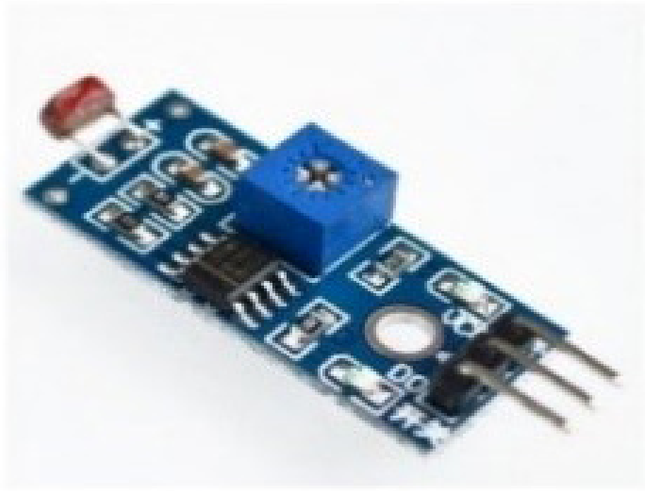

Figura 3. Modulo Sensor con Fotocelda. Tomado de Dualtronica [10]

3. Resultados y Discusión

Al determinar las características y arquitectura de cada componente del prototipo con el fin de validar el tipo de conexión y la ubicación en el Arduino, se pasa del circuito a la baquela y, de esta forma, es posible ejecutar las pruebas iniciales donde por medio de la protoboard se verifica el funcionamiento de cada componente. Posteriormente, se realizan las pruebas de encendido y apagado del sistema mediante la aplicación móvil y, por último, las pruebas de intrusión y análisis de datos del prototipo en la ubicación correspondiente (Salón 1201 CET Colsubsidio-Airbus, con único acceso, donde se resguardan equipos de cómputo y de telecomunicaciones de alto costo).

Estas pruebas permiten determinar la configuración del módulo sensor de fotocelda sobre la intensidad de luz para la generación de la alerta, y el funcionamiento de la aplicación en la parte de gestión del dispositivo con respecto a la programación de hardware realizada o si se requiere realizar cambios en la opción de sensibilidad del sensor en el momento de recepción del haz de luz emitida por el módulo emisor láser.

Al realizar las pruebas de detección entre el módulo emisor láser y el módulo receptor de fotocelda, se estudia si el láser emite el haz de luz. Asimismo, se verifica si al bloquear el haz de luz se genera algún tipo de resultado en el programa Arduino Nightly, el cual es el programa de configuración y gestión de la placa Arduino que además de las herramientas de programación y configuración, permite simular los eventos para verificación y muestra de resultados, por medio de un código. Al bloquear el código, el Arduino Nightly genera un mensaje de acceso y, en caso contrario, genera un mensaje de denegación.

En la fase de evaluación (Figura 4) se encontró que los resultados fueron los esperados y los componentes que intervienen en la construcción del prototipo funcionan de manera correcta, generando que el emisor se encuentre en el funcionamiento óptimo sobre las pruebas realizadas. Al interrumpir el paso del láser entre el módulo emisor y el receptor, se enciende y se apaga el led y se identifican las diferentes intrusiones, programando el Arduino con el fin de generar los mensajes de alerta, obteniendo que al bloquear el láser muestra el mensaje “alerta, intrusión detectada” y al dar el paso muestra “ok”.

Por otra parte, la aplicación móvil se configuró para manipular el dispositivo desde el celular por medio del Bluetooth (Figura 5). Se obtuvo la activación y desactivación del módulo laser exitosamente, por medio de los botones “activar sistema”, que al ser presionado enciende el módulo emisor láser emitiendo el haz de luz hacia el módulo de receptor de fotocelda, y “desactivar sistema”, que al ser presionado apaga el módulo emisor láser dejando de emitir el haz de luz. Cuando la aplicación interactúa con el prototipo se evidencian los resultados sobre los mensajes de alerta de igual modo que en el aparte anterior.

Tabla 3. Valores adquiridos sobre las pruebas en sitio

Pruebas ejecutadas entre las 17:00 y 18:00 horas (Salón 1201)	**Luz Encendida**	**Luz Apagada**	**Puerta Cerrada (Sin Luz)**
	426	483	744 – 762
	Datos análogos de código binario detectado por el módulo sensor de fotocelda sobre la cantidad de luz recibida.		
Pruebas ejecutadas entre las 17:00 y 18:00 horas (Salón 1201)	**Luz Encendida**	**Luz Apagada**	**Puerta Cerrada (Sin Luz)**
	527	615	790 – 815
	Entre menor intensidad de luz exterior, mayor sensibilidad del módulo sensor de fotocelda.		

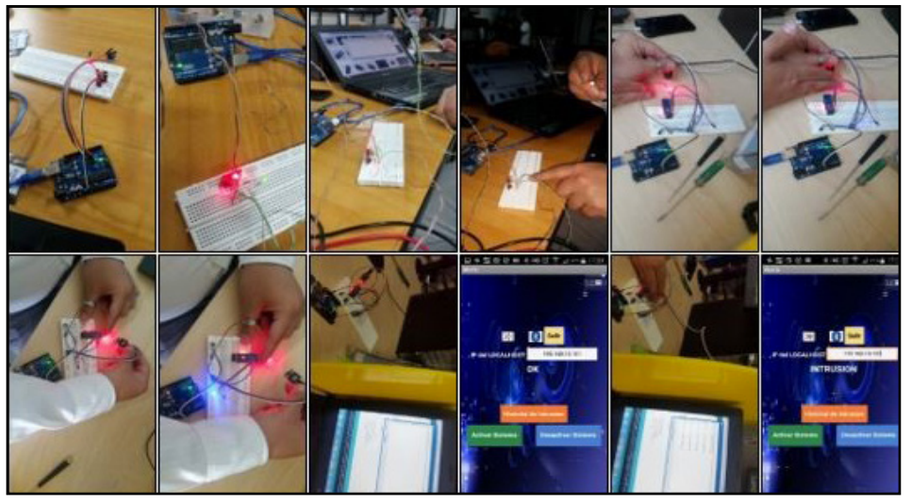

Figura 4. Pruebas del Módulo Emisor y Receptor de Fotocelda Láser.
Fuente Propia

Figura 5. Pruebas de resultados interacción aplicación.

Figura 6. Pruebas de resultados prototipo instalado.
Fuente Propia

Por último, se realizaron las pruebas necesarias para verificar el funcionamiento en el sitio donde enciende y se apaga el led y se identifican las diferentes intrusiones, programando el Arduino con el fin de generar los mensajes de alerta, obteniendo que al bloquear el láser muestra el mensaje “alerta, intrusión detectada” y al dar el paso muestra “ok”.

Por otra parte, la aplicación móvil se configuró para manipular el dispositivo desde el celular por medio del Bluetooth (Figura 5). Se obtuvo la activación y desactivación del módulo laser exitosamente, por medio de los botones “activar sistema”, que al ser presionado enciende el módulo emisor láser emitiendo el haz de luz hacia el módulo de receptor de fotocelda, y “desactivar sistema”, que al ser presionado apaga el módulo emisor láser dejando de emitir el haz de luz.

Cuando la aplicación interactúa con el prototipo se evidencian los resultados sobre los mensajes de alerta de igual modo que en el aparte anterior.

Por último, se realizaron las pruebas necesarias para verificar el funcionamiento en el sitio donde va a quedar instalado el dispositivo de resguardo de la información física y digital, con el fin de determinar los valores generados por el sensor receptor fotocelda con respecto a la cantidad de luz recibida por la distancia entre el módulo emisor y receptor (Figura 6).

Los valores obtenidos se muestran en la Tabla 3, los cuales permitieron ajustar, con datos específicos, la programación de los módulos con respecto a la intensidad de luz y sensibilidad del sensor para la detección de la intrusión.

En el proceso de verificación y pruebas finales se encuentran varias dificultades sobre cómo enlazar la aplicación con la base de datos en php myadmin (Gestor de bases de datos a través de la web) y adicionalmente que, cuando se genere la alerta, este registro quede enlazado en la base de datos, teniendo en cuenta como medio la aplicación y la transferencia desde el dispositivo. Aún se están generando las pruebas de enlace para solucionar este inconveniente y se espera que estas alertas puedan ser registradas en una base de datos, para que de este modo se tenga un consolidado de los eventos de las intrusiones no autorizadas.

4. Conclusiones

Este proyecto describe el procedimiento, desde el análisis hasta la ejecución, para la construcción y puesta en funcionamiento de un Prototipo de seguridad para el resguardo de la información física y digital. En el transcurso de la búsqueda de componentes, uno de los componentes requeridos (Sensor receptor de laser) no estaba disponible en Colombia, por lo tanto, se cambió por un sensor receptor con fotocelda, pero, en general, se mantuvo la propuesta con el enfoque y la idea inicial. Los resultados fueron los esperados en cuanto a las alertas mostradas sobre la interrupción del haz de luz del láser.

La interacción de la aplicación móvil permite un servicio adicional: la activación y desactivación del láser. Este se aplicó durante el desarrollo de la aplicación logrando facilitar el manejo del prototipo y obteniendo una administración eficiente.

El módulo Wifi debe emplearse a futuro con el fin de obtener un mayor alcance en cuanto a la interacción entre la aplicación y el dispositivo. En este momento el dispositivo mediante bluetooth tiene un alcance no mayor a 12 metros, con el módulo wifi esa cifra puede aumentar.

Los componentes son ensamblados en la baquela con el sistema embebido, configurado y adaptado a la necesidad del proyecto, mostrando el funcionamiento de los diferentes componentes los cuales quedaron evidenciados, es decir que, a nivel de hardware, el prototipo cumple con el objetivo planteado. Aún quedan varias pruebas por realizar, sin embargo, para ser prototipo, tiene una gran expectativa, lo que va a permitir el funcionamiento adecuado con lo requerido para generar un dispositivo de seguridad estable.

5. Referencias

[1] Marrero Y, 2003 La Criptografía como elemento de la seguridad informática ACIMED (2003) 11.
[2] Proyecto Malware 2009 Bombas lógicas o bombas de tiempo
[3] Gómez A 2014 Seguridad en Equipos Informático (Madrid: Ediciones de la U) p 40.
[4] Montesino R, Baluja, W and Porvén J 2013 Gestión automatizada e integrada de controles de seguridad informática Ingeniería Electrónica, Automática y Comunicaciones (2013) 34 1.
[5] Argüelles M, 2016 Retos De La Legislación Informática En México Computación y Sistemas (2016) 20 4.
[6] Pérez F, 2006 El Papel de las TIC en los Sistemas para la Seguridad y la Defensa Seguridad y Defensa (2006) 154 42.
[7] Segu.Info. Seguridad Física.
[8] Descubrearduino. Construye un sistema de seguridad con láser con Arduino.
[9] Aprendiendo Arduino. Sensores.
[10] Dualtronica. modulo Sensor con Fotocelda.