UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistemas

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

Estudio de la Interconectividad y la Seguridad de los Datos en los InfoCentros de la Ciudad de Babahoyo

EGRESADO:

Hugo Alexander Chonillo Montece

TUTORA:

Ing. Narcisa María Crespo Torres. Msc.

AÑO 2017

Tema

ESTUDIO DE LA INTERCONECTIVIDAD Y LA SEGURIDAD DE LOS DATOS EN LOS INFOCENTROS DE LA CIUDAD DE BABAHOYO

I. Introducción

Los InfoCentros comunitarios son lugares públicos donde acuden diversos usuarios con la finalidad de aprender de los avances de la tecnología, también resulta útil para realizar tareas o trabajos. Al mantener este espacio abierto al público se vuelve vulnerable para que sufra de ataques hacia los servidores. Los servidores están a cargo por facilitadores contratados, además de ser los encargados de los InfoCentros ellos imparten clases de computación, entre otros cursos.

En los InfoCentros se obtiene información de todos los datos de los ciudadanos que acuden al lugar a capacitarse, debido a que los datos de las inscripciones en los cursos se guardan en el servidor y este se encuentra vulnerable, porque manejan correo electrónico para comunicarse con frecuencia, esta sería la brecha para extraer cualquier tipo de información almacenada en el servidor.

La manera de reducir riesgos que involucran datos de los usuarios es la implementación de normas y medidas para la protección de la información de los InfoCentros.

La norma ISO27001:2013, “Sistema de Gestión de Seguridad de la Información, resultado para mejorar de forma apropiada y lograr determinar varias amenazas, fijando estrategias y controles necesarios resguardar la información.” (ISOTools Excellence, 2015)

Los correos electrónicos que tienen los InfoCentros, no mantienen ningún tipo de seguridad aparte de la del propio correo, la comunicación que realiza los InfoCentros son por medio de los correos electrónicos públicos, no cuenta con correos institucionales, lo que hace posible hackear la cuenta del correo y tener acceso a los datos con facilidad.

Frente a este problema se plantean las siguientes preguntas:

- ¿Cuáles son las medidas de seguridad que tiene su correo electrónico en los InfoCentros de Babahoyo?
- ¿Cómo evitan los riesgos que hay al utilizar los correos electrónicos en los InfoCentros de Babahoyo?
- ¿Qué papel cumple la norma ISO 27001 en la protección de la información que tienen los InfoCentros?
- ¿Cuál es el problema con la comunicación entre los InfoCentros?
- ¿De qué manera brindan seguridad a los correos electrónicos del InfoCentro los encargados del servidor?
- ¿De qué manera mantienen protegidos sus datos en el servidor?

Este caso de estudio se realiza para dar a conocer cuáles son los problemas que hay en los InfoCentros de la ciudad de Babahoyo y en cuanto a la seguridad de sus datos e interconectividad, estos serán estudiados desde los puntos de vista informáticos, obteniendo así un objetivo general, al igual sus respectivos objetivos específicos: Analizar la interconectividad y la seguridad de los datos en los InfoCentros de la ciudad de Babahoyo. Examinar la medida de seguridad que ofrezca mantener un buen nivel de integridad de los datos los ciudadanos en los InfoCentros. Averiguar qué seguridad tiene el servidor con los correos electrónicos. Comprobar que la interconectividad de la red este estable que permitirá al servidor desarrollarse sin problema.

Las limitaciones del presente caso determinan que su objeto de estudio es: el alcance de medidas de seguridad de los datos en los InfoCentros, en el control de acceso a los equipos y correo electrónico, análisis de interconectividad entre los InfoCentros de la ciudad de Babahoyo.

II. Desarrollo

Las organizaciones y sus sistemas de información y redes se enfrentan a amenazas de seguridad de una amplia gama de fuentes, incluyendo fraude informático, espionaje, sabotaje, vandalismo, incendio o inundación. Los causantes de daños, tales como código malicioso, piratería informática y ataques de servicio están siendo frecuentes, complicados y ambiciosos. La seguridad de la información resulta valiosa para entidades públicas y privadas, porque actuara como ayudante, por ejemplo, para obtener la administración electrónica o e-business, y evitar o reducir los riesgos relevantes.(Columba, 2016)

Este trabajo mantiene una sublínea de investigación que se ubica en procesos de transmisión de datos y telecomunicaciones dentro de la línea de investigación de desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos.

Como afirma Hoyos (2016) "El estudio de caso es una estrategia cualitativa que busca documentar, interpretar y valorar, en el contexto de su desarrollo, la particularidad y complejidad de un objeto de estudio que es concreto, contemporáneo y no controlable por el investigador."

La metodología cualitativa fue utilizada en este estudio de caso, debido a que la información que se ha obtenido ha sido de fuentes primarias y directas. Las herramientas utilizadas en este caso de estudio fueron: la Entrevista en profundidad es la técnica más empleada en las distintas áreas del conocimiento y también la de Observación que es una técnica para la recogida de datos sobre comportamiento no verbal.

Primero es importarte saber que: "Los InfoCentros están dispuestos para los habitantes de las parroquias urbanas como rurales separadas de las ciudades del Ecuador. El ciudadano podrá tener entendimiento de las Tecnologías de la Información y Comunicación (TIC), para disminuir la

ignorancia digital.” Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL, s.f.)

La ciudad de Babahoyo cuenta con un InfoCentros ubicado en la Calle transversal entre Simón Bolívar y Camino Real – parroquia Barreiro y el Mega InfoCentros ubicado en la vía Guaranda Babahoyo y Calle Q – parroquia Clemente Baquerizo dentro de la misma ciudad. Son lugares que mantienen las comodidades debidas para los usuarios que asisten a realizar diversas tareas.

El MINTEL maneja los InfoCentros en conjunto con el Gobierno Autónomo Descentralizado de Los Ríos (Prefectura), dan oportunidad para la enseñanza a todos los ciudadanos que quieran aprender, a los estudiantes para que realicen tareas, capacitan al personal de la empresa de limpieza en primeros auxilios y limpieza hospitalaria, personas con discapacidad auditiva los capacitan en herramientas y servicios ofimáticas e instalación y configuración de las redes informáticas, niños becados por la prefectura reciben clases de inglés por el Centro Ecuatoriano De Norteamérica (CEN), a mujeres emprendedoras les dan clases de cosmetología.

Capacitan con cursos de Primeros Auxilios a ciudadanos de la Provincia de Los Ríos, cursos de computación a niños, jóvenes y adultos de la Provincia de Los Ríos y parte de la Provincia del Guayas, cursos de pastillaje, belleza, manualidades a mujeres y hombres que emprenden para formar sus propias empresas.

Se prestan las instalaciones del Mega InfoCentro al Ministerio de Agricultura, Ganadería, Acuacultura y Pesca (MAGAP) y CNT para realizar capacitaciones a sus funcionarios, al Ministerio de Salud Pública (MSP) para el concurso de Méritos y Oposición de profesionales de la salud en etapas de pruebas técnicas y psicométricas a 50 postulantes, también las Cárceles del

Ecuador prestan las instalaciones para llevar a cabo concurso de Méritos y Oposición en etapas de pruebas técnicas y psicométricas a 20 postulantes para guías de las cárceles.

Los facilitadores encargado de los InfoCentros ellos reciben capacitaciones de 4 a 5 veces al mes y son también evaluados, por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL, s.f.), "este tiene la obligación de contestar a las acciones de asesoría y apoyo, asegurando que el acceso a los servicios del área de telecomunicación se mantega de forma igualitaria, para que la Sociedad de la Información avance de manera garantizada y la comunidad tenga un buen vivir."

"La utilización de servidores Unix y Linux son conocidas por ser de plataformas más duraderas, estos servidores son de gama alta y media, los usuarios corporativos confían en Unix y Linux porque presiden ataques a los servidores que resulta difícil asegurar la seguridad total hacia el servidor, por lo que el encargado de sistemas tiene que estar capacitado. Por lo general los ataques se realizan en días no laborables o cuando el encargado no accede con frecuencia." (Trejo, 2014)

"Refiriéndose a un servidor como un equipo, resultan siendo computadoras que tienen programas servidores, estos terminan siendo más grandes y con características superiores que las computadoras habituales." (Plataforma academica para pregrado y posgrado, 2016)

El servidor de cada InfoCentro es el que controla el manejo de todos los Thin client "estos son usuarios agiles, resultando en la informática habitual una cliente ligero, una alternativa segura para las aplicaciones y datos que se encuentran en el servidor." (Soluciones para la movilidad empresarial, 2014).

Los sistemas operativos que tienen en los servidores de los InfoCentros son Ubuntu y Windows Server-2012 R2. Tienen un procesador Intel Xeon de x64, una memoria de 16 Gb. El sistema

operativo solo necesita estar instalado en el servidor, debido a que los Thin client se conecta al servidor para abrir sesión de trabajo en él. Si el servidor se encuentra en Ubuntu los Thin client inicia sesión en Ubuntu y si está en Windows iniciara sesión en Windows mismo.

Entre todos los InfoCentros mantienen comunicación sobre sus actividades diarias, informan de problemas que haya a su jefe, para ello es necesario la interconectividad que según lo publicado en SlideShare "es la conexión de dos o más redes. Resulta fundamental para entrar a las bases de datos compartidas de manera veloz y compartir recursos y tener acceso a las en forma rápida, también el encargado tendrá permitido manejar la red en forma centralizada." (SlideShare, 2012)

Para que se produzca intercambio de información entre entidades (sean del tipo que fuera), es necesario un proceso que involucra la interconexión de dispositivos, es decir la conexión de computadores personales, teléfonos, cableados y medios o dispositivos especiales de interconexión de redes. Por lo tanto, una red de comunicaciones no es más que un conjunto de dispositivos autónomos con capacidad de interconexión. El proceso de intercambio de datos o información se denomina transmisión de datos. Y además, cualquier sistema de transmisión de datos está formado por cinco componentes básicos: emisor, mensaje, receptor, medio y protocolo. (Gil, Pomares, & Candelas, 2010)

Se encuentra que existen dispositivos de interconectividad que permite su intercomunicación. Esta el Conmutador o Swicth "un artefacto de interconexión de redes para computadoras o dispositivos para una red. El uso de un conmutador es la unión de redes y datos a transmitir. Este realiza un filtro en la red, maximizando la seguridad y el rendimiento de las conexiones al provocar una fusión de éstas." (DefiniciónABC, s.f.)

Servidor de acceso remoto “la función de hardware y software que permite acceder de manera remota a herramientas o información que se encuentra en una red de dispositivos usualmente.” (Plataforma academica para pregrado y posgrado, 2016)

Router de igual forma renombrado como enrutador, encaminador o rúter este “dispositivo se utiliza para enlazar una red local, realiza la función de emitir datos tanto dentro o fuera de la red local actividad de enviar los datos fuera o dentro de la red local, como corresponda. De hecho, dentro del router hay una pequeña computadora especializada. Generalmente se puede acceder a la configuración del mismo router a través de una página web interna, que suele establecerse en números seguidos de puntos.” (MAQUINARIApro, s.f.) “Un router distribuye el acceso a Internet de dos formas: por cables llamados cables de red Ethernet o de forma inalámbrica.” (Worcester, s.f.)

En los dos InfoCentros ubicados en la ciudad de Babahoyo se procedió a realizar una entrevista, a los facilitadores (Anexo 5, 6, 7, 8): Marcos Segura del InfoCentro Barreiro, Andrea Freire y Juan Carlos Montalvo del Mega InfoCentro de Babahoyo, en la cual se obtuvo la información y se observó que estos mantienen dispositivos de interconectividad. En el InfoCentros de Barreiro hay dos conmutadores, un servidor que controla a 10 máquinas para los usuarios, no tienen router porque el lugar es pequeño en comparación con el mega InfoCentros que al ser más grande el mega tiene 4 conmutadores, un servidor que controla a 50 máquinas para los usuarios, un router inalámbrico con la red abierta, este mantiene restricciones que solo puede acceder una vez al día y solo será por dos horas a cada usuario.

Para la Interconectividad, se han adaptado muchos protocolos para usarse en redes, para los autores, Ramírez, Rojas y Baleón “Se conoce como la familia de protocolos TCP/IP de Internet

más destaca y utilizada en la interconectividad; casi todos los expertos en informática la llaman TCP/IP.” (Ramírez, Rojas, & Baleón, 2012) Protocolo que utilizan los InfoCentros.

El tipo de conexión a internet que mantienen los InfoCentros es por medio de cable de fibra óptica que les provee la “CORPORACIÓN NACIONAL DE TELECOMUNICACIONES, CNT S.A esta es una es una empresa pública en el mercado de las telecomunicaciones del Ecuador, el servicio que ofrece a los ecuatorianos, para unir al país es un buen servicio en redes de telecomunicaciones.” (CNT, s.f.)

Como asegura Hayes “La fibra óptica es una tecnología de transmisión de luz a través de finos hilos de fibra óptica sumamente transparente, generalmente son fibras de vidrio pero a veces los son de plástico. La fibra óptica se utiliza en las comunicaciones, la iluminación, la medicina, los controles ópticos y en la fabricación de sensores. La asociación de fibra óptica (FOA, por sus siglas en inglés tiene como principal interés la utilización de fibra óptica en las comunicaciones.” (Hayes, 2014)

Para el autor (Castellano, 2015), “La tecnología informática desarrollada en los últimos tiempos ha convertido al computador en una herramienta indispensable en las organizaciones de hoy en día, ya que proporciona los medíos para un control efectivo sobre los recursos que maneja y las operaciones que realiza. Pero esa situación también presenta otras consecuencias, como son: fácil acceso a la información, creciente dependencia al computador, creciente número de personas con estudios en computación, entre otras, que hacen vulnerables a las organizaciones desde el punto de vista informático.”

La norma ISO 27001: 2013 conforme la (ISOTools Excellence, 2015) “la finalidad de esta norma es gestionar y estudiar los peligros basados en los procesos. Este proporciona seguridad

ante cualquier riesgo que ponga en amenaza a las entidades públicas y privadas, por lo cual podrían ocasionar daños en la entidad. Las entidades enfrentan a diario riesgos e inseguridades que vienen de distintas maneras.”

Todos los InfoCentros manipulan información, los datos de todos los usuarios que llegan a capacitarse o a realizar otras actividades, el autor (Tejada, 2014) dice que los, “datos de carácter personal: son cualquier tipo de dato que concierna a las personas físicas identificadas o identificables.” Por ello hay que tener seguridad en toda la información que contenga datos de los usuarios que acuden y laboran en los InfoCentros.

Como alega Tejada(2014) “Las medidas de seguridad para evitar alteraciones y accesos no autorizados a datos personales se tomarán siempre atendiendo a la naturaleza de los datos almacenados, los riesgos a los que están expuestos y la tecnología disponible.”.

“Existen medidas de seguridad, implementación y mantenimiento para la protección de la información, para que cualquier tipo de empresa obtenga sus objetivos y garantizar que cumplan el aumento del prestigio, la legislación y la imagen de la empresa.” (ISOTools Excellence, 2015)

La ISO 27001:2013 SGSI en el anexo A.15 Conformidad de la ISO 27001 se centra en el A.15.1.3 Protección de los registros de la organización: Registros importantes deben ser protegidos de pérdida, destrucción y falsificación, de acuerdo con estatutos, reglamentaciones, contractuales, y requerimientos del negocio. Y el A.15.1.4 Protección de los datos y privacidad de la información personal: Protección de los datos y privacidad debe ser asegurada como requerimiento en la legislación relevante, regulaciones, y, si es aplicable, cláusulas contractuales. Los facilitadores encargado de los InfoCentros deben aplicar esta norma ISO para mantener protegidos los datos de los usuarios.

SGSI preserva los pilares de la seguridad (confidencialidad, integridad y disponibilidad) mediante la gestión de riesgos. Dicho por el autor Medina, "confidencialidad es el poder que no permite divulgar ningún tipo de información personal a terceras personas. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización." Al igual "la integridad, por su parte, es el poder que mantiene los datos libres de modificaciones sin autorización alguna. El objetivo es de mantener la información tal cual fue producida con exactitud, sin manipulaciones o alteraciones por personas ajenas sin autorización." (Medina, 2014)

"La disponibilidad es mantener la información a disposición de quienes requieran acceder a ella siendo estas personas, procesos o aplicaciones en cualquier momento deseado." (Medina, 2014)

Según lo investigado en (Gestión de Riesgo en la Seguridad Informática, s.f.) "En la Seguridad Informática se debe diferenciar dos ideas de protección, la Protección de Datos y la Seguridad de la Información.

Figura 1. *"Seguridad-de-la-información"*

Fuente: *(Gestión de Riesgo en la Seguridad Informática, s.f.)*

"En la Seguridad de la Información como se muestra en la (Figura 1), el propósito de la protección son los datos mismos, se asegura primero la confidencialidad, integridad y disponibilidad de los datos, también la autenticidad entre otros.

La razón para aplicar medidas de protección, es el mismo interés que tiene el lugar o la persona que se encarga de los datos, debido que la modificación o pérdida de los datos provocaría un daño." (Gestión de Riesgo en la Seguridad Informática, s.f.)

Figura 2. *"Protección-de-datos"*

Fuente: *(Gestión de Riesgo en la Seguridad Informática, s.f.)*

"En el caso de la Protección de Datos como se muestra en la (Figura 2), el interés de la protección no son los datos, sino la información referente a las personas. Ahora, la razón para aplicar medidas de protección, por parte de la persona o establecimiento que manipula los datos, es por ética personal o por responsabilidad legal, previniendo resultados negativos de la información de las personas se trata." (Gestión de Riesgo en la Seguridad Informática, s.f.)

En muchos Estados hay leyes que regulan el tratamiento de los datos personales, en el caso de la Constitución Política del Ecuador 2008, en su artículo 23, inciso 8, se considera el derecho a la "honra, a la buena reputación y a la intimidad personal y familiar…"(Carballo, 2012), esta ley protege el nombre, la voz y la imagen de la persona.

Como afirma Rouse “la seguridad es un proceso para que los datos no sean manipulados ni existan perdidas de la misma por lo cual es importante el respaldo operativo de datos y la recuperación de desastres/continuidad del negocio.” (Rouse, 2016)

Los datos de los usuarios que realizan diversos cursos, y toda información que se recepta para realizar los cursos están en el correo del facilitador encargado del InfoCentro. Esta información se envía mediante el correo electrónico y también mantienen comunicación por este mismo medio, el correo electrónico que utilizan es Gmail, el MINTEL les proporciona un correo electrónico a cada InfoCentro dándoles una dirección de correo que identifica el lugar donde están ubicados y ellos mismo le dan la contraseña.

El autor López(2011) dice, “El personal directivo debe ser responsable de los documentos que redacta y envía a otras empresas y organismos públicos. Además, la mayoría serán enviados por e-mail. El acceso a muchos equipos sensibles debe ser controlado de: alguna forma, sobre todo una vez encendidos, para garantizar que nadie aproveche un descanso del personal para usarlos.”

Como asegura Meza “el uso del correo electrónico por medio del internet que no tengas las seguridades correspondiente son vulnerables a tener amenazas en las seguridades de su sistema. Se tiene que saber las amenazas para garantizar que su política de seguridad sugiera cómo disminuirlos. El correo electrónico es otra manera de comunicarse. Hay que ser discreto al momento de enviar por correo electrónico información reservada. El correo electrónico es probable que lo intercepte y lo lea, por lo que viaja entre numerosos sistemas y luego llega a su destino. Conviene que para conservar la confidencialidad del correo electrónico se apliquen medidas de seguridad necesarias” (Meza, 2016)

Gmail tiene millones de usuarios activos al mes según el autor (Sernis Laleona, 2016) por, Sencillez de uso, Funcionalidades que se adaptan a las necesidades y Buena gestión del correo no deseado. También muchos móviles usan Android (que lleva integrado Gmail y obliga a tener una cuenta de Google para usarlo) ha ayudado.

Tabla 1. *"Proveedores-de-correos-electronicos-corporativos-o-institucionales"*

Proveedor	Tecnología libre o privada	Documentos en la Nube	Calendario y Eventos	Tareas	Espacio en Gb	Costo en USD por cuenta
Gmail	Tecnología Privada	si	si	si	30	50/año[2]
Office 365	Tecnología Privada	si	si	si	50	50/año[3]
Zoho	Tecnología Privada	si	si	si	5	24/año[4]
Open-Xchange App Suite	Tecnología Libre	no	si	si	5	9.12/año[5]
Zimbra	Tecnología Privada	si	si	si	25	54/año[6]

Fuentes: *(gsuite, s.f.) (ESP office 365, s.f.) (zoho, s.f.) (open-xchange, s.f.) (Manual_ZIMBRA, s.f.)*

Utilizar un correo institucional tiene ventajas (unjfsc, 2013) como: "Seguridad y privacidad, Sigue conectado desde cualquier lugar, Acerca a alumnos, docentes, egresados y personal, Agiliza tus trabajos, Cuida el medio ambiente." Como se visualiza en la (Tabla 1), hay muchos proveedores que ofrecen correos electrónicos institucionales o corporativos en diversos precios y características importantes sobre su servicio.

El Correo Institucional tiene importancia usarlo según (Carmona, s.f.), "es el medio de comunicación principal entre los individuos de la comunidad educativa. Señala un sentido de institucionalidad, la visualizar el dominio "@g.upn.mx" señala que forman parte de una

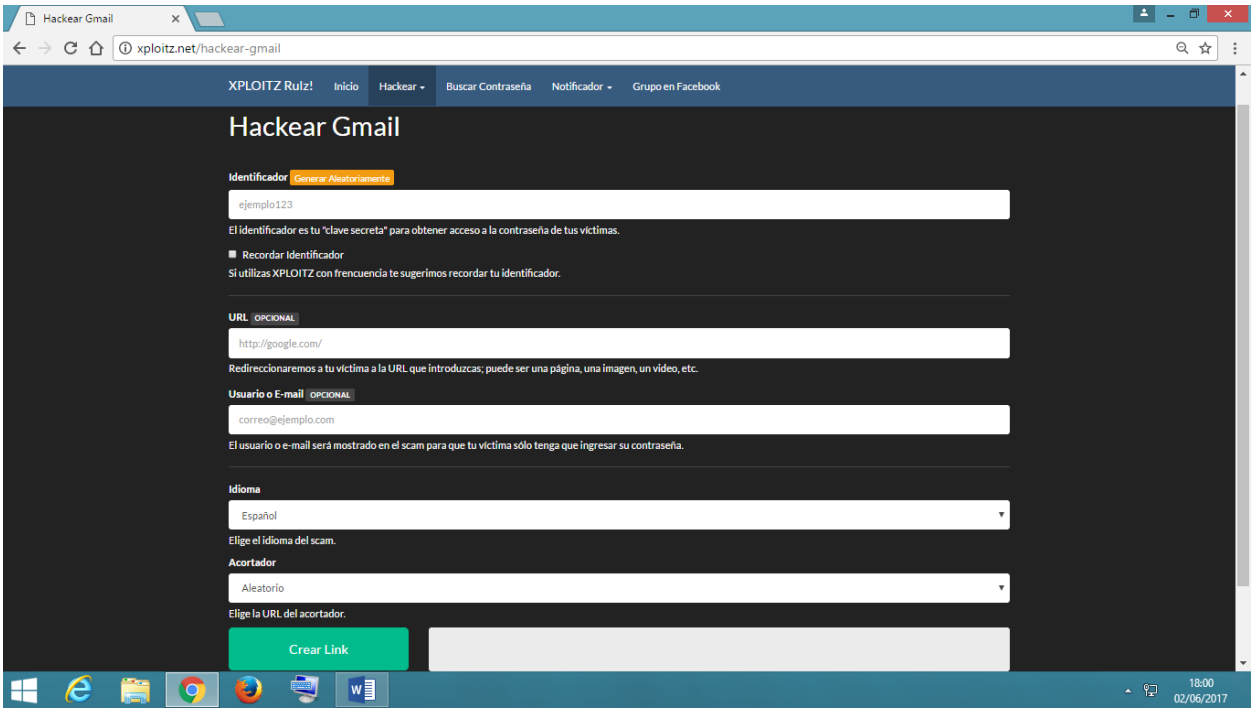
institución, dándole un entorno de formalidad en todas las comunicaciones. Impide que nuestro correo personal al utilizarlo, los mensajes de compañeros y docentes se extravíen entre los otros que se reciben (spam, cadenas, asuntos personales, etc.). Este servicio al tener será exclusivamente para los asuntos vinculados con la institución."

La agencia creativa dice que la razón más obvia de utilizar correo institucional, "es porque brindan MÁS SEGURIDAD a las cuentas de correo electrónico que están alojadas en su servidor privado, permitiendo impedir posibles ataques de virus, malware, o inclusive fraudes de correos." (agencia creativa, 2013)

"El servicio de correo gratuito incluye accesorios que pueden ser inadecuados o sobrantes para un negocio, como la publicidad constante, el chat, o Google +. En el caso del servicio de correo profesional, se caracteriza por la compatibilidad y su seriedad con todos los programas de correo para PC, este es compatible inclusive con el acceso web gratuito que brinda Google (Gmail)." (agencia creativa, 2013)

Después de una búsqueda para acceder o conseguir información que tiene los correos electrónicos de los InfoCentros, en la (Figura 3), se encuentra XPLOITZ Rulz! que según Lozano(2016) "es una plataforma en que su principal objetivo es estafar, confundir; en lo cual se puede crear un "Login" semejante a las páginas de cualquier red social (Facebook, Twitter, Instagram y Snapchat) o correo electrónico (Hotmail, Gmail y Yahoo) y engañar al individuo para que ingrese los datos de su cuenta y asi en estafador obtendrá por medio de esta plataforma los datos requeridos.". En los anexos (anexo1, anexo2 y anexo3), está detallado paso a paso como se puede obtener el usuario y la clave de un correo electrónico de Gmail.

Figura 3. *"Página-web-de-Xploitz"*



Fuente: *(XPLOITZ Rulz!, s.f.)*

Se encontró una publicación del diario EL COMERCIO donde se da a conocer de los ataques que han tenido empresas dentro del país por medio de correo electrónico, Javier Ortega el que publica esta información dice cuántas empresas han sido atacadas, como fue el ataque y que lo produjo.

Como comenta Ortega, en Cibermafias atacaron a 17 empresas ecuatorianas. "Un virus se dispersó un 19 de enero del 2015. Expertos en seguridad informática conocieron las primeras infecciones. El 'malware' avanzó y en cinco días accedió a las computadoras de unas 17 empresas privadas e instituciones públicas de Quito, Guayaquil y Cuenca." (Ortega, 2015)

"El programa maligno penetró en las computadoras para encriptar archivos sensibles: documentos subidos en Excel, Word, AutoCAD. Una de las empresas que sufrió el ataque se le extravió carpetas que almacenaban datos del departamento de contabilidad. Debido al contagio,

las compañías notificaron los daños a GMS, una de las cinco empresas de Ecuador que oculta mega plataformas informáticas. El especialista en seguridad de la información de esa firma Xavier Almeida, dijo que no había visto algo parecido en el país." (Ortega, 2015)

"Técnicos analizaron las computadoras infectados y descubrieron que se trataba del virus denominado *cryptolocker*, un poderoso 'malware' llega a los usuarios por medio de correos electrónicos con información supuestamente valiosa. Las empresas afectadas notificaron que el programa uso una fachada falsa de asunto 'facturación electrónica'. Técnicos no descartan que el 'malware' se propago en Ecuador por la circunstancia que desde el 1 de enero del 2015, se pide la emisión de estos documentos digitales." (Ortega, 2015)

Lo que menciono (Ortega, 2015), "En Ecuador lo más usual en delitos informáticos era hasta el momento, las estafas, extorsiones, la clonación de tarjetas, acceso a correos electrónicos."

III. Conclusiones

El estudio de la interconectividad y la seguridad de los datos en los InfoCentros de la ciudad de Babahoyo, aporta al facilitador del InfoCentro con técnicas para evitar pérdida de información de sus usuarios, a evitar ataques en contra de su correo electrónico, conocer si mantienen una conexión eficiente en su comunicación, mejorar las medidas de seguridad de los datos que están en el servidor y en el correo electrónico.

En los InfoCentros ingresa muchos usuarios a realizar diversas actividades, los datos o información que se obtiene se ellos, son requeridos por el MINTEL para llevar un reporte de cómo se están administrando cada InfoCentro.

Él envió de información por correo electrónico público o privado, resulta inseguro debido a que se puede obtener su usuario y su clave de manera ágil, o infectar el servidor y obtener cualquier información, esto a medida que avanza la tecnología, se conocen nuevas formas de sustraer cualquier dato que desee el usurpador. Por lo que habría mayor seguridad en los datos si estos se enviaran por un correo electrónico institucional o corporativo, en lo cual solo abrirá correos que tenga el dominio del mismo lugar, así se estará seguro que ese correo no es sospechoso o malicioso.

Los InfoCentros mantenían problemas en la interconectividad, su conexión no era estable tenían problemas con el internet, fallaba en ocasiones, hoy en día ya cuentan con conexión de fibra óptica, que es lo que la corporación CNT están proporcionando a los InfoCentros, debido a que es la socia tecnológica del Estado, además de ser la fibra el medio de transmisión que es inmune a las interferencias electromagnéticas.

Bibliografía

Castellano, L. R. (2015). *Seguridad en Informática* (Segunda Ampliada ed.). Veneuela: IE. Obtenido de https://www.amazon.com/Seguridad-Informatica-Edici%C3%B3n-ampliada-Spanish-ebook/dp/B017EA7BXW/ref=pd_rhf_se_s_cp_7?_encoding=UTF8&pd_rd_i=B017EA7BXW&pd_rd_r=MB73AV53A5ZFV5C6FTCE&pd_rd_w=bjWJU&pd_rd_wg=ZHiXa&psc=1&refRID=MB73AV53A5ZFV5C6FTCE

Columba, E. S. (2016). *Guía de Referencia de Fundmentos de Seguridad de la Información basado en ISO 27001 e ISO 27002* (primera ed.). Obtenido de https://www.amazon.com/Fundamentos-Seguridad-Informaci%C3%B3n-basados-27001-ebook/dp/B01EDKIIEW/ref=sr_1_1?s=books&ie=UTF8&qid=1493395729&sr=1-1&keywords=Fundamentos+de+Seguridad+de+la+Informaci%C3%B3n+basados+en+ISO+27001%2F27002%3A+Gu%C3%ADa+de+referenc

Gil Vázquez, P., Pomares Baeza, J., & Candelas Herías, F. (2010). *Redes y transmisión de datos.* San Vicente de Alicante. Obtenido de https://books.google.es/books?hl=es&lr=&id=On6y2SEaWyMC&oi=fnd&pg=PA11&dq=medios+f%C3%ADsicos+de+cableado+de+redes&ots=Lcdn6tMlKI&sig=cF5AiIGvUnuZiW2cdSnDFpGXXGs#v=onepage&q=medios%20f%C3%ADsicos%20de%20cableado%20de%20redes&f=false

Hayes, J. (2014). *Guía de Referencia de la Asociación de Fibra Óptica (FOA) Sobre Fibra Óptica: Guía de estudio para la certificación de la FOA.* Copyright. Obtenido de https://www.amazon.com/Referencia-Asociaci%C3%B3n-Fibra-%C3%93ptica-Sobre/dp/1495990184/ref=sr_1_1?s=books&ie=UTF8&qid=1493692344&sr=1-1&keywords=Gu%C3%ADa+de+Referencia+de+la+Asociaci%C3%B3n+de+Fibra+%C3%93ptica+%28FOA%29+Sobre+Fibra+%C3%93ptica%3A+Gu%C3

Hoyos, Ó. I. (2016). *Metodología para la elaboración de estudios de caso en responsabilidad social.* Colombia. Obtenido de https://books.google.com.ec/books?id=TlUeDQAAQBAJ&pg=PP7&dq=metodologia+cualitativa+de+un+caso+de+estudio&hl=es&sa=X&ved=0ahUKEwjWzvrX_JPUAhWI6yYKHeOvD0YQ6AEIQjAH#v=onepage&q=metodologia%20cualitativa%20de%20un%20caso%20de%20estudio&f=false

López, A. (2011). *Redes seguras (Seguridad informática).* Obtenido de https://books.google.es/books?hl=es&lr=&id=15PTAwAAQBAJ&oi=fnd&pg=PA143&dq=medios+f%C3%ADsicos+de+cableado+de+redes&ots=J5jCcMaWLh&sig=yf-hChpwyMSxOK1DvLxWoFvsoXA#v=onepage&q=medios%20f%C3%ADsicos%20de%20cableado%20de%20redes&f=false

Medina, J. (2014). *Evaluación de Vulnerabilidades TIC* (Primera ed.). Laderas del Campillo (Murcia): klindle. Obtenido de https://www.amazon.com/Evaluaci%C3%B3n-Vulnerabilidades-Spanish-Javier-Medina-ebook/dp/B00QGPIQHW/ref=pd_rhf_se_s_cp_1?_encoding=UTF8&pd_rd_i=B00QGPIQHW&pd_rd_r=MB73AV53A5ZFV5C6FTCE&pd_rd_w=bjWJU&pd_rd_wg=ZHiXa&psc=1&refRID=MB73AV53A5ZFV5C6FTCE

Sernis Laleona, C. (2016). *Gmail - mucho más que el e-mail: Guía paso a paso para conocer todas sus posibilidades* (Primera ed.). Copyright. Obtenido de https://www.amazon.com/Gmail-e-mail-conocer-posibilidades-Spanish/dp/1530625637/ref=sr_1_25?s=books&ie=UTF8&qid=1493328991&sr=1-25&keywords=correo+electronico

Tejada, E. C. (2014). *Auditoría de seguridad informática. IFCT0109* (Primera ed.). (I. Editorial, Ed.) Cueva de Viera, 2, Local 3 Centro Negocios CADl ANTEQUERA, Málaga: IC Editorial. Obtenido de https://books.google.com.ec/books?id=8a3KCQAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Trejo, J. E. (2014). *Metologia de Contingencia En Servidores DNS, DHCP, Web, Correo y FTP En Sistemas Operativos Unix y Linux.* Alemania: Copyright. Obtenido de https://www.amazon.com/Metologia-Contingencia-Servidores-Sistemas-Operativos/dp/3656645639/ref=sr_1_2?s=books&ie=UTF8&qid=1493324079&sr=1-2&keywords=servidores+de+correo

Linkografía

agencia creativa. (2013). Obtenido de http://www.agenciacreativa.net/noticias/correo-gratuito-vs-correo-profesional-no-es-oro-todo-lo-que-reluce

Carballo, D. L. (19 de enero de 2012). *Daniel López Carballo*. Obtenido de http://dlcarballo.com/2012/01/19/sobre-la-legislacion-de-proteccion-de-datos-en-ecuador/

Carmona, E. A. (s.f.). *slideshare*. Obtenido de Uso del Correo Institucional: https://es.slideshare.net/eliaca/uso-del-correo-institcional-upn?next_slideshow=1

CNT. (s.f.). Obtenido de http://soy.cnt.com.ec/index.php?option=com_content&view=article&id=251&Itemid=6

DefiniciónABC. (s.f.). Obtenido de Definición de Conmutador: http://www.definicionabc.com/tecnologia/conmutador.php

ESP office 365. (s.f.). Obtenido de http://www.epn.edu.ec/correo-institucional/

Gestión de Riesgo en la Seguridad Informática. (s.f.). Obtenido de https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

gsuite. (s.f.). Obtenido de https://gsuite.google.com/intl/es-419/pricing.html?country=ar&tab_activeEl=tabset-companies

ISOTools Excellence. (23 de abril de 2015). *Blog especializado en Sistemas de Gestión de Seguridad de la Información* . Obtenido de La importancia de la norma ISO 27001: http://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/

Lozano, A. F. (2016). *BLOGGIN RED*. Obtenido de http://www.blogginred.com/2016/10/como-hackear-una-cuenta-de-facebook.html#.WStJSJI1_IU

Manual_ZIMBRA. (s.f.). Obtenido de http://189.203.254.137/paginas/sistemas/documentos/Manual_ZIMBRA.pdf

MAQUINARIApro. (s.f.). Obtenido de Funcion del router: http://www.maquinariapro.com/electronica/router.html

Meza, K. (14 de junio de 2016). *kathy meza porta*. Obtenido de Correo electrónico, bloc y redes sociales: http://kathymezaporta.blogspot.com/2016/06/v-behaviorurldefaultvmlo.html

Ministerio de Telecomunicaciones y Sociedad de la Informacion. (s.f.). Obtenido de https://www.telecomunicaciones.gob.ec/infocentros-comunitarios/

MINTEL. (s.f.). Obtenido de Ministerio de Telecomunicaciones: https://www.telecomunicaciones.gob.ec/valores-mision-vision/

open-xchange. (s.f.). Obtenido de https://www.open-xchange.com/

Ortega, J. (24 de enero de 2015). EL COMERCIO. *Cibermafias atacaron a 17 empresas ecuatorianas*, págs. http://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html.

Plataforma academica para pregrado y posgrado. (30 de abril de 2016). Obtenido de Programa Integración de Tecnologías a la Docencia : http://aprendeenlinea.udea.edu.co/lms/moodle/mod/page/view.php?id=73890

Ramírez Martínez , Z., Rojas Palacios , M. Á., & Baleón Aguilar , G. (16 de julio de 2012). *Intercomunicación y Seguridad en Redes*. Obtenido de Interconectividad: https://lordratita.wordpress.com/2012/07/16/unidad-1-interconectividad/

Rouse, M. (febrero de 2016). *SearchDataCenter*. Obtenido de TechTarget: http://searchdatacenter.techtarget.com/es/definicion/Proteccion-de-datos

SlideShare. (23 de septimbre de 2012). Obtenido de Tecnologia: https://es.slideshare.net/helen1404/interconectividad-14423052

Soluciones para la movilidad empresarial. (18 de diciembre de 2014). Obtenido de http://movilidadempresarial.idg.es/tecnologias/la-virtualizacion-evoluciona-los-thin-client-hacia-terminales-portatiles

unjfsc. (20 de Noviembre de 2013). Obtenido de http://www.med-unjfsc.edu.pe/interes/por_que_tener_correo/

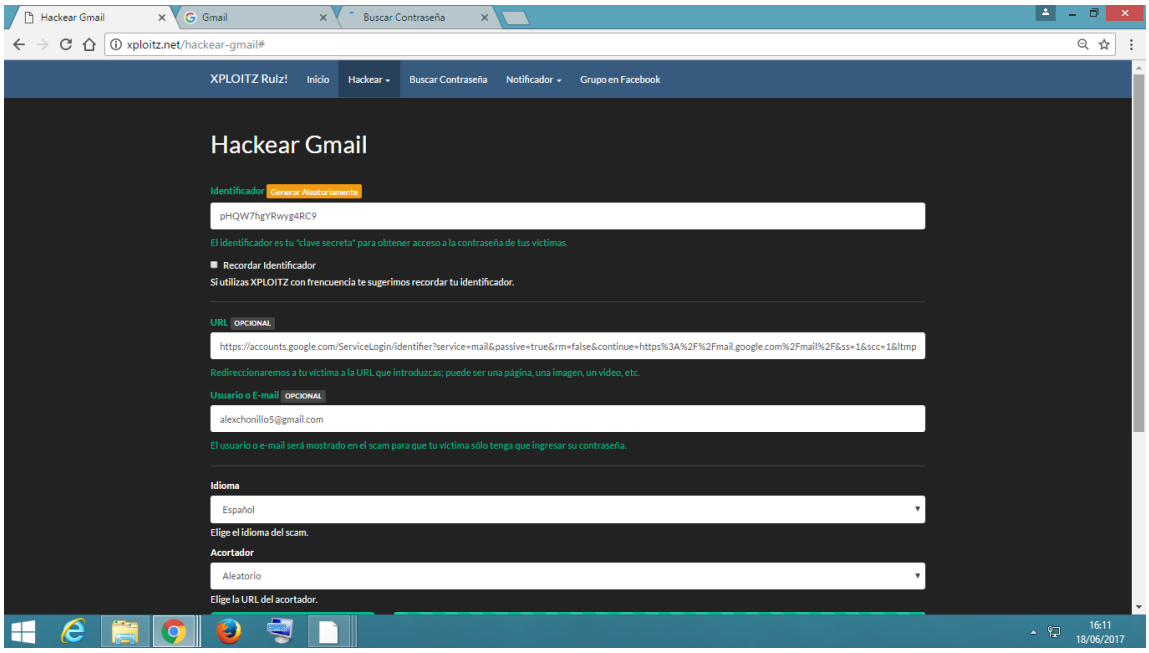
Worcester, M. (s.f.). *eHowenespañol*. Obtenido de Cuales son las funciones de los routers: http://www.ehowenespanol.com/cuales-son-funciones-routers-info_268928/

XPLOITZ Rulz! (s.f.). Obtenido de http://xploitz.net/hackear-gmail#

zoho. (s.f.). Obtenido de https://www.zoho.com/workplace/pricing.html

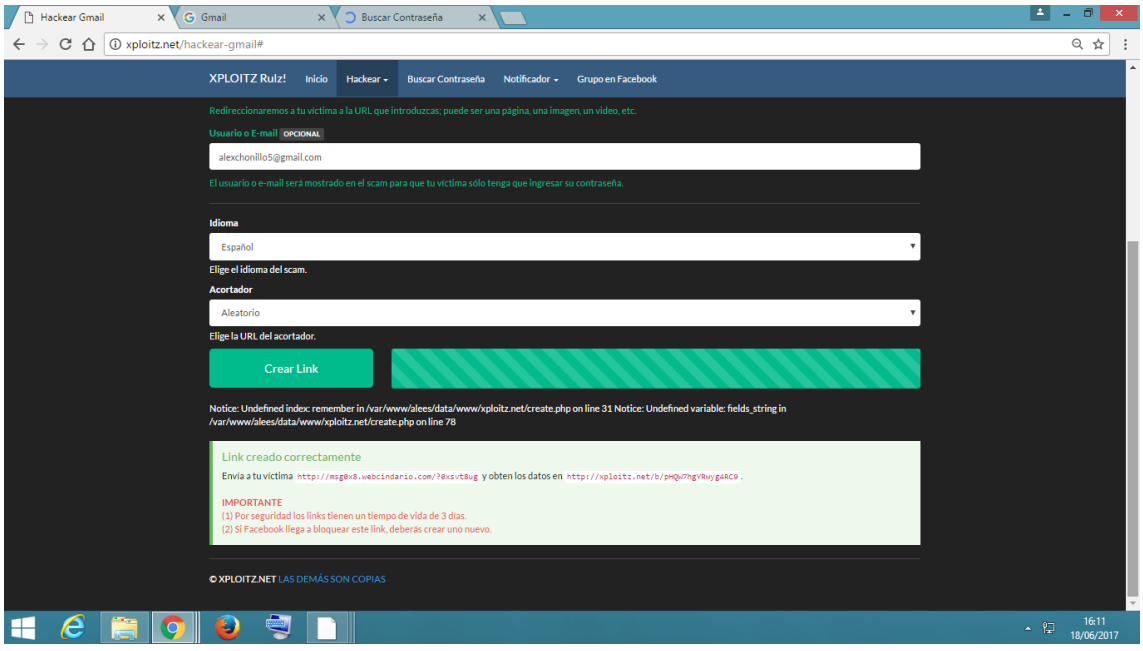
ANEXOS

Anexo 1. *Ingreso de datos*



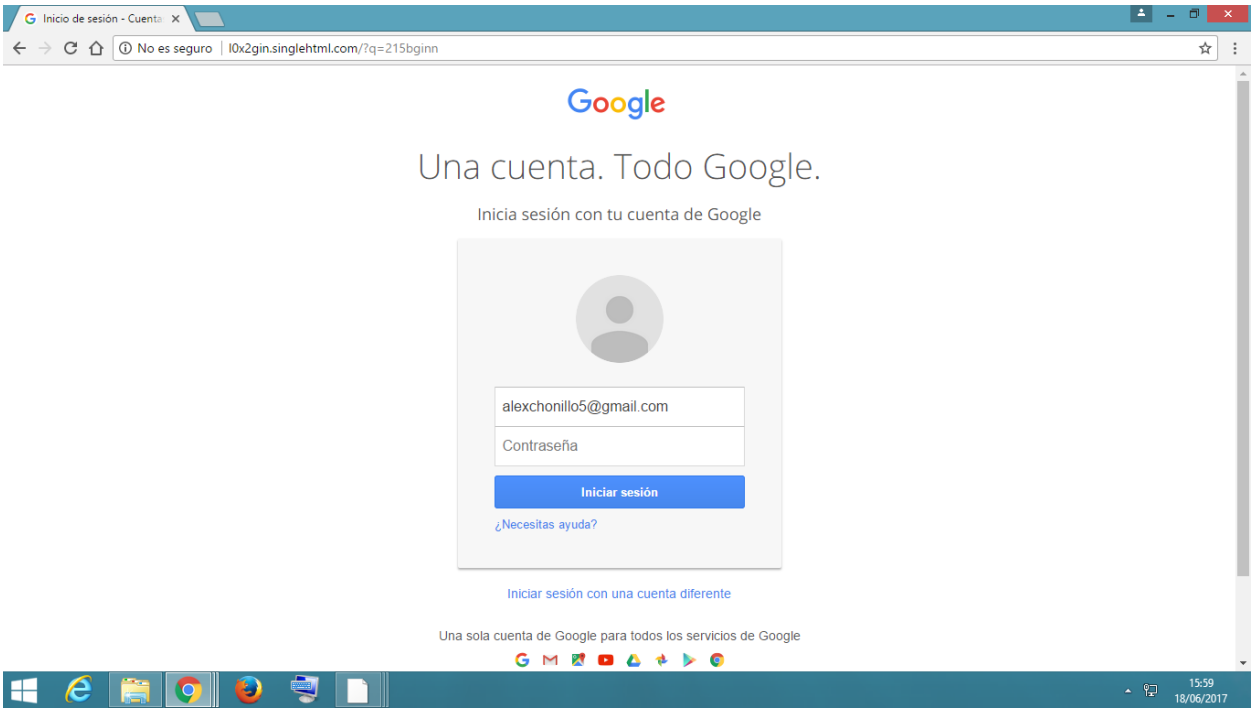
Fuente: *(XPLOITZ Rulz!, s.f.)*

Anexo 2. *Códigos generados*



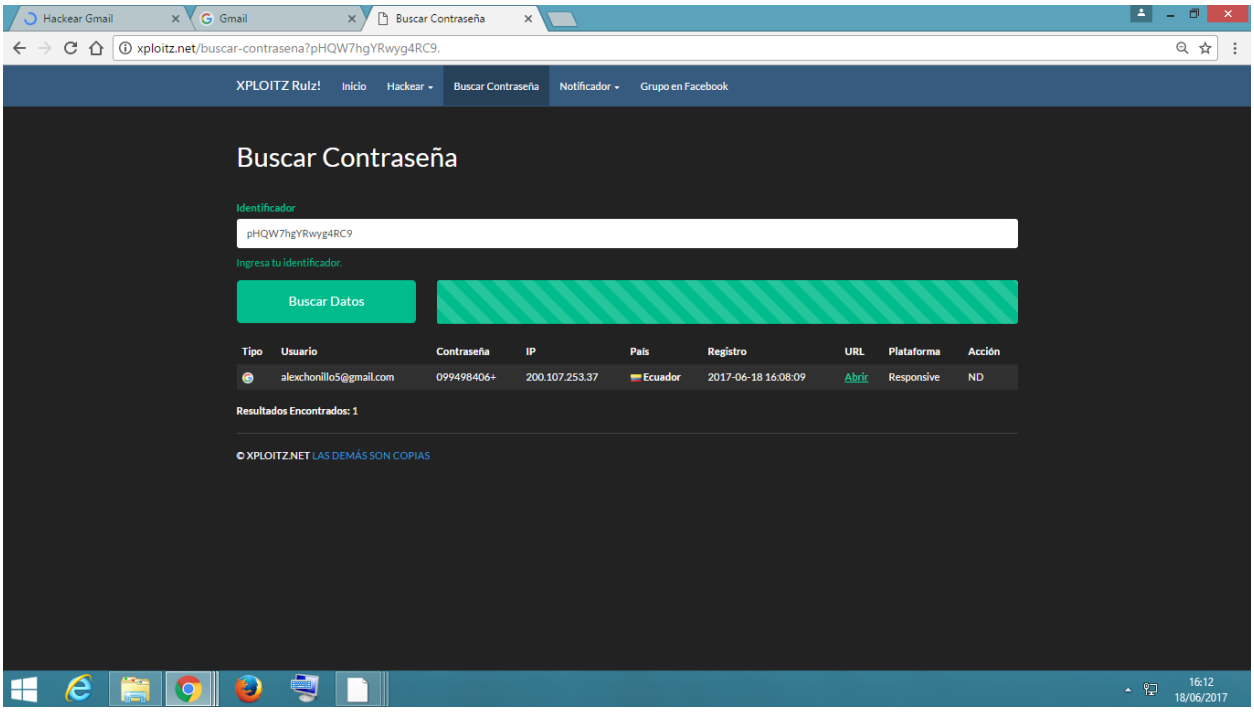
Fuente: *(XPLOITZ Rulz!, s.f.)*

Anexo 3. *Página espía*



Fuente: *(msg0x8 xploitz, s.f.)*

Anexo 4. *Página que muestra el resultado*



Fuente: *(xploitz, s.f.)*

Anexo 5. *Cuestionario utilizado para la entrevista.*

Preguntas

¿Utiliza medidas de seguridad en el correo electrónico del InfoCentros de Babahoyo?

¿Cómo evitan los riesgos que hay al utilizar los correos electrónicos en los InfoCentros de Babahoyo?

¿Utiliza alguna norma para la protección de la información que tiene el InfoCentros?

¿Qué inconveniente tienen con la comunicación entre los InfoCentros?

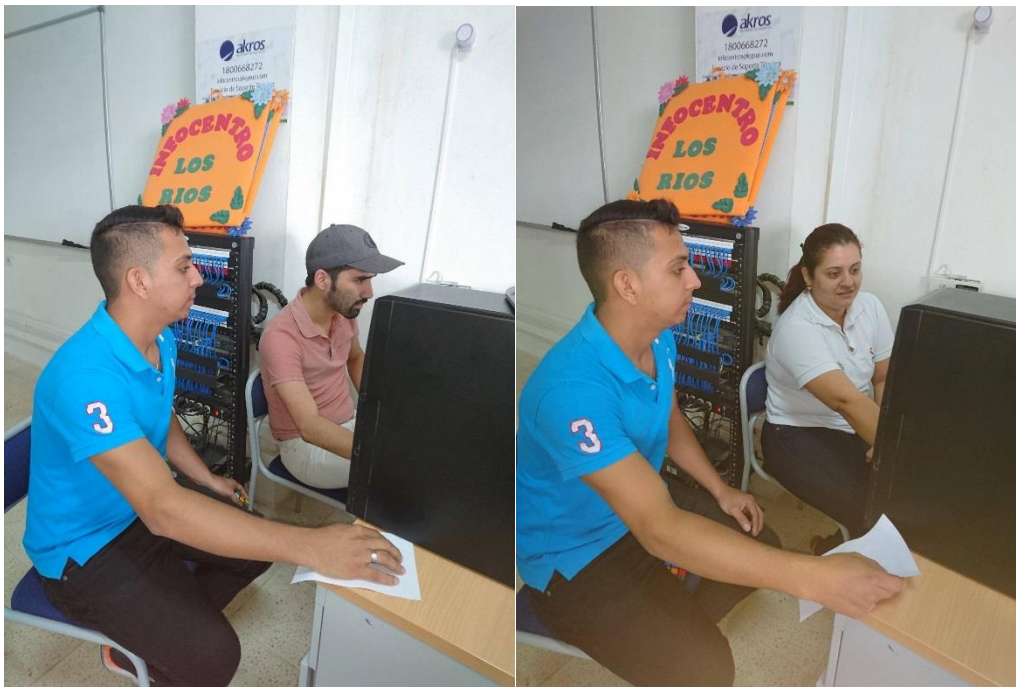
¿Cuál es la seguridad con el correo electrónico del InfoCentro siendo usted el encargado del servidor?

¿Cómo mantienen protegidos sus datos en el servidor?

¿Qué datos manejan los InfoCentros?

Anexo 6. *Entrevista en el InfoCentro Barreiro al facilitador Marcos Segura*

Anexo 7. *Entrevista en el Mega InfoCentro Barreiro al facilitador Juan Carlos Montalvo*



Anexo 8. *Entrevista en el Mega InfoCentro Barreiro a la facilitadora Andrea Freire*

Índice de Contenido

Índice de Tablas

Índice de Figuras

Índice de Anexos