Confiar en una nube: Estudio de Seguridad en Tecnología Cloud Computing utilizando Backtrack 5 y Medusa.

Heredia H.; Coronel J.; Cortes J.
Instituto Tecnológico Superior Cordillera, Carrera de Análisis y Sistemas
Quito, Ecuador (Tel: 593-2-2262-041. Ext: 106; e-mail: hugo.heredia@cordillera.edu.ec)
Instituto Tecnológico Superior Cordillera, Carrera de Análisis y Sistemas
Quito, Ecuador (Tel: 593-2-2262-041. Ext: 106; e-mail: johnny.coronel@cordillera.edu.ec)
Instituto Tecnológico Superior Cordillera, Centro de Investigación y Desarrollo Tecnológico
Quito, Ecuador (Tel: 593-2-2433-732; e-mail: jose.cortes@cordillera.edu.ec)

Resumen:*El presente artículo describe el estudio sobre las respuestas de los niveles seguridad que ofrece una infraestructura generada bajo tecnología cloud computing cuando se trata de violentarla utilizando los ataques más comunes que se suelen dar en las redes informáticas. Para el estudio se diseñaron cinco tipos de ataque, a saber: Negación de Servicios (imposibilita el ingreso a usuarios autorizados), Fuerza Bruta (busca la contraseña correcta probando todas las posibles), Dominio Fantasma (Impide que se agote el tiempo de vida de un subdominio falso en el caché de servidores DNS), Llamada Telefónica (Utiliza ingeniería social para extraer contraseñas) y Robo de Contraseña (Aprovecha la falta de hábitos adecuados de los usuarios de cuentas en servidores para guardar contraseñas). Los resultados muestran la vulnerabilidad general de la infraestructura, destacando que el ataque más efectivo de los testeados para vulnerar este tipo de tecnología es el de Robo de Contraseña., por el contrario y en positivo, el nivel de seguridad que muestra más robustez tras recibir los cinco ataques diseñados, es el de Negación de Servicios. Finalmente, se describen algunas recomendaciones a tener en cuenta en el uso de la tecnología cloud computing a nivel organizacional.*

Palabras clave:*Seguridad, cloud computing, ataques, incursión en la nube, vulnerabilidad*

Abstract: This paper describes the study on the responses of layered security infrastructure that provides cloud computing technology generated under when it comes to violating it using the most common attacks that usually occur in computer networks. For the study, five types of attacks were designed, namely: Denial of Service (precludes entry to authorized users), Brute Force (finds the correct password by trying all possible), Ghost Domain (Prevents the lifetime expires a subdomain in the DNS cache servers), Phone Call (uses social engineering to extract passwords) and Password theft (Seize the lack of proper habits of users accounts on servers to store passwords). The results show the overall vulnerability of infrastructure, noting that the most effective of those tested to undermine this type of attack is the technology of password theft. Contrast and positive, the level of security that shows more robustness after receiving five attacks designed, is the Denial of Service. Finally, some recommendations to consider in the use of cloud computing technology at the organizational level are described.

Keywords:*IT security, cloud computing, cyber-attacks, foray into cloud networks, telematics*

1. INTRODUCCIÓN

La transformación que ha tenido la Tecnología de la Información y Comunicación (TIC) donde se apunta a un mundo que tuvo como punto de inicio la utilización de grandes mainframes, para luego pasar a tener arquitecturas cliente servidor alojados en grandes Data Centers, pasando por los servicios que desde la aparición del internet se ha logrado hasta lo que hoy conocemos como cloud computing.

[17]"Tata Consultancy Services (TCS)estima que el 39% del software de las grandes empresas de Latinoamérica se encuentran alojados en la nube, cifra que en Estados Unidos es del 19% y en Europa del 12%; alcanzando en el caso de las empresas de la zona de Asia Pacífico, donde también se está apostando por la implementación del *cloud computing*, el 28%".

Sin embargo hablar de *Cloud Computing* va más allá de la reducción de costos en la infraestructura, de ser un nuevo paradigma tecnológico, aspectos muy atractivos para las organizaciones, no obstante, al momento de contratar los servicios de los proveedores de cloud no sólo buscan la reducción de los costos en los Departamentos de Tecnología de la Información (TI), sino que surgen interrogantes sobre su activo más importante "La Información", sobre los niveles de seguridad que ofrecen, considerando que la ciberdelincuencia ha pasado de ser más que un pasatiempo de ocio a convertirse en el negocio de verdaderas mafias.

[16] INTECO-CERT en sus conclusiones del estudio sobre Riesgos y Amenazas en cloud computing destaca que la seguridad y la propiedad de los datos son aspectos claves que se deben considerarse al momento de buscar una solución de

sus problemas en la nube, así como los controles de acceso, la identidad, la privacidad y seguridad de la información.

En Ecuador como en toda América Latina se deben redoblar esfuerzos para desarrollar políticas de control que regule el uso y garantice la privacidad y seguridad de la información en la nube.

Ahora bien, ¿qué confianza podemos tener en la seguridad y privacidad de la información cuando utilizamos una nube?, es la pregunta que se tratará de responder. Todo usuario tiene interés en contestar a esta cuestión, y son pocos los estudios hasta la fecha que han intentado dar luz a esta inquietud.

El trabajo realizado por el equipo de investigadores, lo que busca es responder a esta interrogante mediante una serie de ataques que comúnmente suelen realizarse por los ciberdelincuentes en el momento de apoderarse de la información de sus víctimas, se han planteado dos objetivos principales:

1. Analizar la robustez de los niveles de seguridad de la tecnología *cloud computing* ante ataques intrusivos comunes.

2. Identificar el tipo de ataque que vulnera con mayor efectividad la nube creada.

Se describe la metodología que se ha seguido para el análisis de las variables de estudio. En este apartado se enuncian las fases que se han seguido en la investigación junto a las características técnicas de la infraestructura creada, así como la herramienta seguida para medirla respuesta a los diversos ataques a la que ha sido sometida. Posteriormente, se ofrecen los resultados obtenidos a través del análisis estadístico realizado utilizando SPSS V.21 que dan paso a la descripción de las conclusiones.

2. MATERIALES Y MÉTÓDOS

El cumplimiento de los objetivos de la investigación ha requerido el planteamiento de una metodología de análisis, dentro de una investigación aplicada, que permita la extracción de conclusiones y del análisis de los resultados del Hacking Ético realizado a la infraestructura de *cloud computing* instalada en el Instituto Tecnológico Superior Cordillera.

El Hacking Ético se entiende como un conjunto de incursiones controladas y generadas por los expertos con el propósito de determinar los niveles de amenazas a la infraestructura tecnológica de una organización.

El enfoque metodológico que se presenta a continuación incluye, a modo de síntesis, los principales parámetros técnicos que se han adoptado para la realización del estudio.

Se han llevado a cabo procesos de análisis que aportan diferentes fuentesde información complementaria. La investigación documental de fuentes secundarias así comoel análisis de fuentes documentales nacionales e internacionales existentes sobre *cloud computing* ha permitido enfocar los conceptos clave del estudio y obtener información de contraste para los resultados obtenidos en el presente trabajo.

Al hacer un análisis sobre las incidencias de carácter legal en las cuales se incurriría al efectuar ataques a nubes públicas y las repercusiones en el equipo investigador e institucional,hizo que se decida generar una infraestructura tecnológica *cloud computing* propia del Institución.

Para comprender la infraestructura "*cloud computing*" que se implementó en el Instituto se dará una explicación breve de cada uno de los tipos y niveles de servicio, para proceder a explicar cómo fue implementada la infraestructura.

TIPOS DE CLOUD-COMPUTING

Modelo Público: este tipo de modelo de*cloud computing* o nube como lo llaman comúnmente tiene la característica que el proveedor de servicio tiene control total de la infraestructura, el cliente lo que hace es uso de ella desde cualquier lugar por medio de internet y no tiene control y seguridad de la información.

Modelo Privado: está caracterizado porque en este tipo de nube se tiene control sobre la privacidad y se determinan las políticas de seguridad de la información de acuerdo a las necesidades de las organizaciones, su costo de implementación es alto.

Híbrida: tiene la características de las dos anteriores, mejora la capacidad de una nube privada y la ventaja que el usuario hace uso de sus propios recursos.

NIVELES DE SERVICIO

Infraestructura como Servicio:es el primer nivel de los servicios de *Cloud Computing*, ésta provee por ejemplo: servicio de almacenamiento de información, conectividad, virtualización de servidores para balanceo de carga y otros, un buen ejemplo de esto en nuestro país es Telconet empresa de servicios, que nos permite alquilar un espacio de almacenamiento en sus servidores con el afán respaldar los datos de la empresa.

Plataforma como Servicio:tiene como objetivo el prestar un entorno para el desarrollo de aplicaciones que pueden ser variadas en relación a los lenguajes de programación como PHP, JAVA, .NET. Un buen ejemplo son los servicios de Google App Engine, Windows Azure y otros.

Software como Servicio: el más popular en el sentido que probablemente la gran mayoría ha utilizado, por ejemplo el servicio de correo que tenemos en nuestros trabajos o los clásicos correos gratuitos, mensajería instantánea, entretenimiento como Netflix, entre otros. Esto permite ver

que los servicios en la nube se han multiplicado y van en creciente demanda.

Analizando y entendiendo las conceptualizaciones anteriores el nivel de servicio escogido para el desarrollo de esta infraestructura que sirvió para medir los niveles de seguridad en la tecnología *cloud computing* es el SaaS (Software como Servicio), utilizando Microsoft 2008 server R2 donde se publicó servicios de correo (Microsoft Exchange 2007) y un sitio documental (Share Point 2010), los mismos que estuvieron atados al dominio itscosistemas.edu.ec con un modelo de despliegue de nube privada.

Se implementaron 3 servidores que a continuación se describen detalladamente. Los equipos estuvieron instalados con Windows server 2008 R2 estándar, como se muestra en la figura 1.

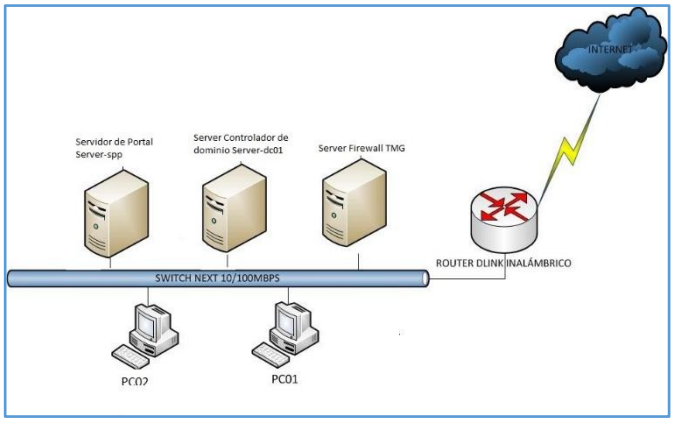

Figura 1: Esquema de la Infraestructura cloud implementada

Para la realización de este prototipo de *cloud computing* se consideró las siguientes especificaciones de hardware tanto para el front end como para cada uno de los nodos clientes, así como la distribución física de los equipos y de la red:

Nombre de servidor: server-dc01 (Servidor de Controlador de Dominio), dirección IP: 172.16.1.1, submáscara: 255.255.0.0, puerta de enlace: 172.16.1.3, DNS: 172.16.1.1, software instalado: Windows Server 2008 R2;Roles levantados: DNS Active Directory, Usuario: Administrator, Clave: P@ssw0rd.

Nombre de servidor: server-frw (Servidor de Firewall & Correo electrónico), dirección IP: 172.16.1.3, submáscara: 255.255.0.0, puerta de enlace: DNS: 172.16.1.1, dirección IP, WAN 186.3.71.118, submáscara: 255.255.255.248, puerta de enlace: 186.3.71.113, DNS: 200.93.216.2, DNS alternativo: 200.93.216.5, software instalado, Windows Server 2008 R2.

Forefront Threat Management Gateway | ISA Server.

Microsoft Exchange Server 2007 con service pack 3, Roles Levantados: IIS 6, Entidad certificadora, Microsoft Forefront Threat Management Gateway | ISA Server (Configurado con reglas de publicación para correo y publicación de portal interno de la organización), Microsoft Exchange Server 2007 con los siguientes servicios (IMAP – POP3 – Microsoft Exchange ActiveSync - OWA) (https://correo.itscosistemas.edu.ec/owa), nombre de usuario: Admin_frw, clave: Atencion01.

Nombre de servidor: server-spp (Servidor de SharePoint Server), dirección IP: 172.16.1.2, submáscara: 255.255.0.0, puerta de enlace: 172.16.1.3, DNS: 172.16.1.1, software instalado: Windows Server 2008 R2, Microsoft SharePoint server 2010 Standard. Roles levantados: IIS 6, entidad certificadora: Microsoft SharePoint Server 2010 Stándard (http://portal.itscosistemas.edu.ec) servicio DHCP deshabilitado: rango de IP desde 172.16.1.10 hasta 172.16.1.254.

Nombre RED ITSCO, claves de acceso: SERVER-DC01: user: Administrator, clave: P@ssw0rd, dominio Itsco. Server-frw: user: Admin_frw, clave: Atencion01, dominio Itsco. Server-spp: user: Admin_portal, clave: Atencion01, dominio Itsco. Usuarios creados en el Active Directory (Server-dc01): user: cromero, clave: Atencion01. User: anieto, clave: Pa$$w0rd, user: hheredia, clave: Atencion01.

Una vez generada la infraestructura se realizó una sesión de trabajo interno para definir los protocolos de actuación a seguir para testear la seguridad de la nube generada. Para ello se explicó a todo el equipo técnico vinculado a la investigación sobre las variables de estudio que forman parte del diseño del mismo, y cómo realizar cada ataque sincrónico.

El equipo de investigación basado en su experiencia y en el análisis de sus vivencias profesionales determinó la composición de los criterios e indicadores de medición de cada una de las variables a estudiar que a continuación se presentan.

Variables de estudio:

1. Nivel de Seguridad compuesto por:
   a) Nivel de seguridad Correo Electrónico (NSCE).
   b) Nivel de seguridad Cultura Informática (NSCI)
   .
   c) Nivel de seguridad de Servidor de Dominio (NSSD).
   d) Nivel de seguridad de obtención de información (NSOI).
   e) Nivel de seguridad de Servidor DNS (NSSDNS).
2. Ataques a la nube. Esta variable estaba configurada por los siguientes componentes:

a. Ataque de Negación de Servicios (ANS).

b. Ataque de Fuerza Bruta (AFB).

c. Ataque de Dominio Fantasma (ADF).

d. Ataque de Llamada Telefónica (ALLT).

e. Ataque de Robo de Contraseña (ARC).

A continuación se explica el objetivo y el procedimiento que definen a cada uno de los ataques:

a) Ataque de Negación de Servicios:

Objetivo.- Este ataque tiene como objetivo, saturar de peticiones al servidor escogido para la operación, para desbordar su capacidad de procesamiento, esto hace que el servidor se cuelgue y no pueda atender a los usuarios que no pertenezcan a la organización.

En nuestro caso vamos atacar al portal documental http://portal.itscosistemas.edu.ec.

Procedimiento.- Para entender cómo se realizó este ataque se lo describe a continuación.

Con el conocimiento del dominio atacar http://portal.itscosistemas.edu.ec se rastree en http://network-tools la dirección IP pública asignada.

Se escoge el tipo de negación servicios, es decir, si se va a atacar el ancho de banda para saturarlo o si se va saturar el tiempo de procesador, no se puede saturar el ancho de banda porque los servicios de la institucionestán controlados por el mismo proveedor de internet, así que se atacaró el tiempo de ejecución del servidor.

La herramienta seleccionada para este tipo de ataque es backtrack 5 sobre Linux, para ello se ejecuta la sentencia hping3 -a 192.168.0.221 -S -p 80 --flood 186.3.71.118".

Una vez ejecutada la sentencia el servidor recibe en promedio 2200 peticiones de conexión en 20seg, es decir agota el tiempo de respuesta, pues su ejecución es de manera simultánea desde otras conexiones.

Generando una ráfaga SYN que son cabeceras de paquetes de datos que solicitan conexión al server e inmediatamente se desconectan, como la IP que se utiliza está enmascarada en una IP falsa que es creada por el servidor backtrack 5, el servidor no puede devolver la petición y la descarta.

b) Ataque de Fuerza Bruta (AFB)

Objetivo.- Consiste en realizar una búsqueda de la clave válida de un usuario para poder ingresar a un sistema y posteriormente poder secuestrar los servicios como por ejemplo el correo electrónico que en nuestro caso será el propósito, nuestro servidor de correo está publicado a través de OWA, con la dirección:https://correo.itscosistemas.edu.ec.

Aunque el objetivo es secuestrar la base de datos de correo el método que se aplicará será atacar al servidor de firewall, para poder establecer un escritorio remoto embistiendo el puerto de conexión del mismo.

Procedimiento.Descubrir la dirección IP pública del servidor 186.3.71.118, esto se lo hace con http://network-tools.com donde se coloca el nombre de dominio itscosistemas.edu.ec y luego se realiza una consulta de DNS, para obtener la IP pública que atiende al servicio.

Se realiza un scanport con backtrack 5, pero no devuelve resultado positivo, probablemente el firewall no lo permite, lo bueno es que si está habilitado el acceso remoto, se puede intentar el ataque, suponiendo que el servicio está operativo. Se aplicó la herramienta medusa, este software se usa con Linux, en nuestro caso Ubuntu 11.0, al instalarlo se levantó el demoniun de medusa y se envió a ejecutar el comando #medusa.

Lo siguiente que se hizo es escoger el módulo correcto seleccionado con el siguiente código medusa –d.

Luego de escoger el de puertos se debe ejecutar la siguiente sintaxis: #medusa -186.3.71.118 -administrador /home/d14m4nt3/crack_passwords.txt -M ssh –f.

Habrá que esperar hasta que el software aplique su funcionalidad para devolver el password.

La efectividad de éste se evidencia en la complejidad y extensión que el usuario administrador asignó a la clave.

c) Ataque de Dominio Fantasma.

Objetivo.- Consiste en realizar una suplantación del servidor de DNS que resuelve el nombre hhtp://itscosistemas.edu.ec. Lo que se ataca es una vulnerabilidad en los registros de memoria caché que tienen estos servidores DNS, la idea es crear un registro falso en servidores alternos que se

configurarán para el propósito, estos están versados en Linux y Microsoft.
Procedimiento. Se utilizó servidores de DNS, gratuitos para registrar un nombre subdominio, estos servidores son Microsoft y Linux.

Luego se realizó peticiones a nuestro subdominio, para crear tráfico, de esta manera se crean registros de ruta hacia nuestro servidor de dominio.

Hay que borrar el suddominio, en los servidores de DNS, se queda registrada la ruta del dominio que se quería usar.

Posteriormente hay que hacer una nueva petición al servidor DNS y este devolverá una IP y a la vez recibirá un nuevo nombre de dominio, el servidor de dominio pensará que existe una actualización en el nombre y reescribirá el registro.

Hay que probar la efectividad, desde distintos servidores de DNS. Sean en Microsoft y Linux.

En dominios que tengan ya un tiempo funcionando este procedimiento es muy complicado y no se asegura el éxito, pero se puede hacer a la vez en distintos dominios hasta encontrar uno que no tenga tanto tiempo en publicación.

d) Ataque de Llamada Telefónica.

Objetivo.- Obtener información confidencial de los usuarios mediante la realización de un vínculo de comunicación vía telefónica.

Procedimiento. Para realizar este ataque primero se debe obtener el número telefónico de las víctimas así como de sus extensiones.

Se coordinará con los encargados de ejecutar este ataque los horarios en los que se debe realizarlos, es importante que cada atacante establezca un vínculo de familiaridad con la víctima para de esta manera obtener la información que se necesita.

hacerse pasar por personal del área de soporte indicando que existe problemas de configuración con el equipo asignado, de esta manera se deberá obtener información como direcciones IPs, nombres de usuarios al sistemas, claves de acceso y posteriormente se les informa sobre los cambios realizados.

e) Ataque de Robo de Contraseña.

Objetivo.- Obtener información de las cuentas de correo electrónico de las víctimas.

Procedimiento. Para la obtención de las cuentas de correo electrónico no se necesitará de mayor trabajo, pues cada cuenta creada de las victimas tiene un patrón como por ejemplo Cromero@itscosistemas.edu.ec por lo que obtenerlas no será muy complicado.

Se utilizará el software bootservice con el cual se enviará un correo falso a las víctimas con una página solicitando que ingrese cierta información de interés para el proyecto, para que posteriormente llegue al correo del atacante un email con la información que se obtuvo.

Una vez desarrollado cada uno de los ataques se describe los siguientes casos validados.

Nivel de Servicio	Casos Validados
Nivel de seguridad Correo Electrónico (NSCE)	180
Nivel de seguridad Cultura Informática (NSCI)	90
Nivel de seguridad de Servidor de Dominio (NSSD)	180
Nivel de seguridad de obtención de información (NSOI)	90
Nivel de seguridad de Servidor DNS (NSSDNS)	180

Figura 2: Nivel de Efectividad. Escala de Valoración

En los niveles de seguridad Cultura Informática, Obtención de Información se ha validado la mitad de los casos debido a que no todos cumplieronel cien por ciento del procedimiento señalado en los ataques de Llamada Telefónica, y el Robo de contraseñas.

Para operativizar el impacto de cada uno estos ataques en la seguridad de la nube se generó el índice Nivel de Efectividad del Ataque por el cual a través de una escala Likert de 0-5 de *Muy Bajo-Muy Alto*, se podía recoger el resultado por cada ataque. Cuanto más efectivo es el ataque mayor vulnerabilidad presenta la estructura. Ver Figura 3.

De igual modo se obtuvo el Nivel de Efectividad Global de Ataque, y el índice de robustez de cada nivel de seguridad.

NIVEL DE EFECTIVIDAD DE CADA ATAQUE			
A	MUY BAJO	No se ha tenido incursiones	
B	BAJO	El nivel de acceso es limitado	
C	MEDIO	El nivel de acceso no ha causado mayores daños en la infraestructura	
D	ALTO	El nivel de acceso ha causado daños considerables en la infraestructura	
E	MUY ALTO	Colapso del nivel de seguridad de la infraestructura	

Figura 3: Nivel de Efectividad. Escala de Valoración

A continuación se crearon los protocolos de actuación para cada uno de los catorce docentes especializados de la carrera de Análisis de Sistemas que intervinieron en la investigación.

A través de estos protocolos de actuación se homogenizaron tanto el proceso, el tiempo y la sincronización de cada ataque.De igual modo, con el fin de asegurar la calidad del trabajo final se capacitó a los docentes por expertos externos sobre ataques a la infraestructura y servicios.

Seguidamente, se realizó una distribución del operativo configurando siete equipos de análisis con dos personas y un líder por cada uno de ellos que realizaron los ataques establecidos.

La fase de ataque dio como resultado 720 incursiones sobre la nube desarrollada que permitió poder analizar la efectividad de intrusión de cada ataque en cada uno de los niveles de seguridad establecidos.

Por último, se recogió la información de los resultados del índice de efectividad de cada ataque por nivel de seguridad de todos los investigadores para realizar un tratamiento informático de los datos obtenidos a través del SPSS V.21.

A continuación se muestran los resultados obtenidos:

3. RESULTADOS

A continuación se muestra la tabla de contingenciacon los resultados obtenidos del análisis de las dos variables:

Tabla 1: Nivel de Efectividad. Escala de Valoración

Tabla de contingencia Tipo de Ataque * Nivel de Efectividad * Nivel de Seguridad

Nivel de Seguridad			Recuento Nivel de Efectividad Muy Bajo	Bajo	Medio	Alto	Muy Alto	Total
NSCE	Tipo de Ataque	ANS	0	0	1	32	3	36
		AFB	24	12	0	0	0	36
		ADF	35	1	0	0	0	36
		ALLT	33	3	0	0	0	36
		ARC	0	0	0	15	21	36
	Total		92	16	1	47	24	180
NCI	Tipo de Ataque	ANS	4	8	5	1	0	18
		AFB	12	4	2	0	0	18
		ADF	7	11	0	0	0	18
		ALLT	4	2	0	4	8	18
		ARC	0	5	1	9	3	18
	Total		27	30	8	14	11	90
NSSD	Tipo de Ataque	ANS	0	0	5	24	7	36
		AFB	27	8	0	1	0	36
		ADF	21	10	4	1	0	36
		ALLT	34	2	0	0	0	36
		ARC	4	2	5	17	8	36
	Total		86	22	14	43	15	180
FOI	Tipo de Ataque	ANS	6	9	3	0	0	18
		AFB	13	3	1	0	1	18
		ADF	7	10	1	0	0	18
		ALLT	0	1	0	11	6	18
		ARC	2	2	2	5	7	18
	Total		28	25	7	16	14	90
NSSDNS	Tipo de Ataque	ANS	0	0	13	18	5	36
		AFB	33	3	0	0	0	36
		ADF	20	8	3	5	0	36
		ALLT	34	2	0	0	0	36
		ARC	12	3	5	13	3	36
	Total		99	16	21	36	8	180
Total	Tipo de Ataque	ANS	10	17	27	75	15	144
		AFB	109	30	3	1	1	144
		ADF	90	40	8	6	0	144
		ALLT	105	10	0	15	14	144
		ARC	18	12	13	59	42	144
	Total		332	109	51	156	72	720

Resultados de análisis individuales por nivel de seguridad:

1. Nivel de seguridad correo electrónico.

Tabla 2: Nivel de Seguridad de Correo Electrónico

Tabla de contingencia Tipo de Ataque * Nivel de Efectividad * Nivel de Seguridad

Nivel de Seguridad			Recuento Nivel de Efectividad Muy Bajo	Bajo	Medio	Alto	Muy Alto	Total
NSCE	Tipo de Ataque	ANS	0%	0%	3%	89%	8%	100%
		AFB	67%	33%	0%	0%	0%	100%
		ADF	97%	3%	0%	0%	0%	100%
		ALLT	92%	8%	0%	0%	0%	100%
		ARC	0%	0%	0%	42%	58%	100%
	Total							

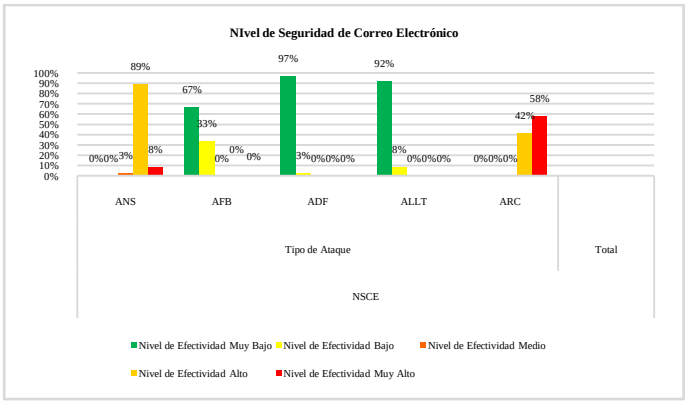

Figura 4: Nivel de Seguridad de Correo Electrónico

Los dos ataques que han mostrado mayor efectividad son: el Ataque de Negación de Servicios y el de Robo de Contraseñas, el primero de ellos ha tenido una respuesta de *Muy Alta efectividad* del 8% y *Alta efectividad* del 89%, y el segundo una respuesta de *Muy Alta efectividad* del 58% y *Alta efectividad* del 42%, lo que supone para ambos que en el 100% de los casos se ha vulnerado con gran eficiencia la seguridad del correo electrónico.

Mientras que los Ataques de Fuerza Bruta, Dominio Fantasma, Llamada Telefónica muestran un nivel de efectividad *Muy Baja* del 67%, 97%, 92% respectivamente.

2. Nivel de seguridad Cultura Informática (NCI)

Tabla 3: Porcentaje de Nivel de Seguridad Cultura Informática

Tabla de contingencia Tipo de Ataque * Nivel de Efectividad * Nivel de Seguridad

Nivel de Seguridad			Recuento Nivel de Efectividad Muy Bajo	Bajo	Medio	Alto	Muy Alto	Total
NCI	Tipo de Ataque	ANS	22%	44%	28%	6%	0%	100%
		AFB	67%	22%	11%	0%	0%	100%
		ADF	39%	61%	0%	0%	0%	100%
		ALLT	22%	11%	0%	22%	44%	100%
		ARC	0%	28%	6%	50%	17%	100%
	Total							

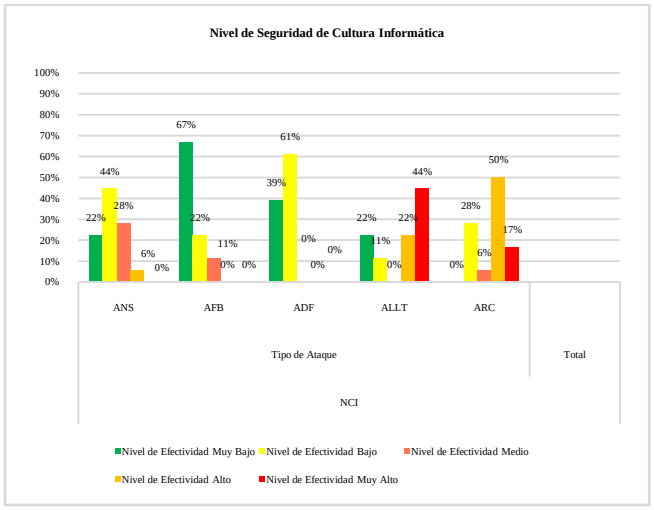

Figura 5: Nivel de Seguridad de Cultura Informática

Los dos ataques que han mostrado mayor efectividad son: el Ataque de Robo de Contraseñas y el de Llamadas Telefónicas, el primero de ellos ha tenido una respuesta de *Muy Alta efectividad* del 8% y *Alta efectividad* del 89%, y el segundo una respuesta de *Muy Alta efectividad* del 58% y *Alta efectividad* del 42%.

Mientras que los Ataques de Fuerza Bruta, Dominio Fantasma, Negación de servicio, muestran un nivel de efectividad *Muy Baja* del 67%, 39%, 22% respectivamente.

3. Nivel de seguridad de Servidor de Dominio (NSSD)

Tabla 4: Porcentaje de Nivel de Seguridad Servidor de Dominio

Tabla de contingencia Tipo de Ataque * Nivel de Efectividad * Nivel de Seguridad								
Recuento								
Nivel de Seguridad			Nivel de Efectividad					Total
			Muy Bajo	Bajo	Medio	Alto	Muy Alto	
NSSD	Tipo de Ataque	ANS	0%	0%	14%	67%	19%	100%
		AFB	75%	22%	0%	3%	0%	100%
		ADF	58%	28%	11%	3%	0%	100%
		ALLT	94%	6%	0%	0%	0%	100%
		ARC	11%	6%	14%	47%	22%	100%
	Total							

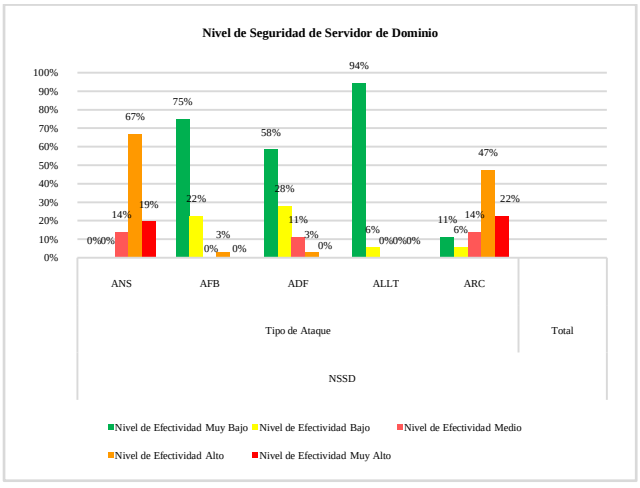

Figura 6: Nivel de Seguridad de Servidor de Dominio

Los dos ataques que han mostrado mayor efectividad son: el Ataque de Robo de Contraseñas y el de Negación de Servicio, el primero de ellos ha tenido una respuesta de *Muy Alta efectividad* del 22% y *Alta efectividad*del 47%, y el segundo una respuesta de *Muy Alta efectividad* del 19% y *Alta Efectividad* del 67%.

Mientras que los Ataques de Llamadas Telefónicas, Fuerza Bruta, Dominio Fantasma, muestran un nivel de efectividad *Muy Baja* del 94%, 58%, y 22% respectivamente.

4. Nivel de seguridad de obtención de información (NSOI)

Tabla 5: Porcentaje de Nivel de Seguridad de Obtención de la Información

Tabla de contingencia Tipo de Ataque * Nivel de Efectividad * Nivel de Seguridad								
Recuento								
Nivel de Seguridad			Nivel de Efectividad					Total
			Muy Bajo	Bajo	Medio	Alto	Muy Alto	
FOI	Tipo de Ataque	ANS	33%	50%	17%	0%	0%	100%
		AFB	72%	17%	6%	0%	6%	100%
		ADF	39%	56%	6%	0%	0%	100%
		ALLT	0%	6%	0%	61%	33%	100%
		ARC	11%	11%	11%	28%	39%	100%
	Total							

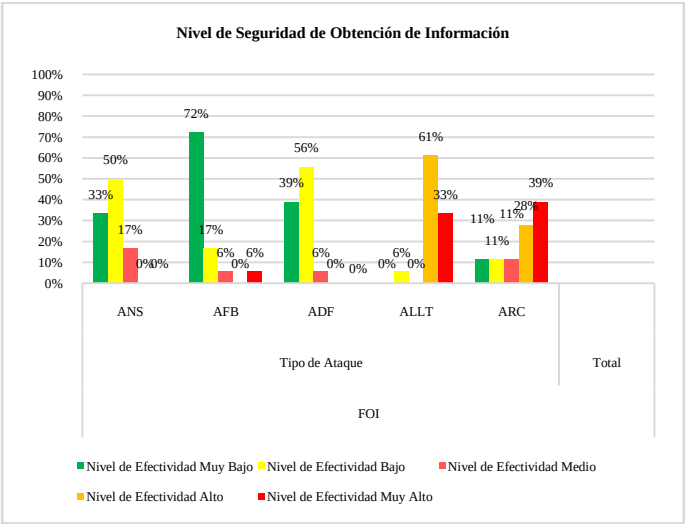

Figura 7: Nivel de Seguridad de Obtención de la Información

El ataque Llamada Telefónica destaca su efectividad en vulnerar este nivel de seguridad ya que en el 94% de los casos tiene un nivel de *Muy Alta* y *Alta efectividad.L*e sigue el ataque de Robo de Contraseña que sumando los dos niveles de efectividad *Muy Alta* y *Alta* arroja un resultado global de 67%.

Por otro lado los Ataques de Negación de Servicio, Dominio Fantasma, Fuerza Bruta con un nivel de efectividad *Muy bajo* del 33%, 39%, 72% respectivamente.

5. Nivel de seguridad de Servidor DNS (NSSDNS)

6. Tabla 6: Porcentaje de Nivel de Seguridad de servidor DNS

Tabla de contingencia Tipo de Ataque * Nivel de Efectividad * Nivel de Seguridad								
Recuento								
Nivel de Seguridad			Nivel de Efectividad					Total
			Muy Bajo	Bajo	Medio	Alto	Muy Alto	
NSSDNS	Tipo de Ataque	ANS	0%	0%	36%	50%	14%	100%
		AFB	92%	8%	0%	0%	0%	100%
		ADF	56%	22%	8%	14%	0%	100%
		ALLT	94%	6%	0%	0%	0%	100%
		ARC	33%	8%	14%	36%	8%	100%
	Total							

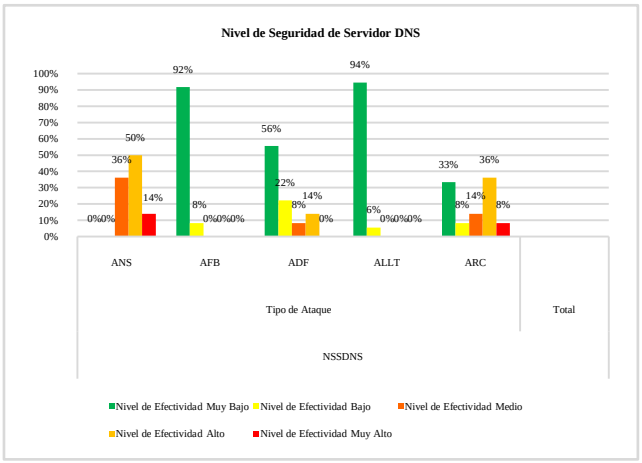

Figura 8: Nivel de Seguridad de Servidor DNS

Los dos ataques que han mostrado mayor efectividad son: el Ataque de Negación de Servicio y el de Robo de Contraseña, el primero de ellos ha tenido una respuesta de *Muy Alta efectividad* del 14% y *Alta efectividad* del 50%, y el segundo una respuesta de *Muy Alta efectividad* del 8% y *Alta Efectividad* del 36%.

Mientras que los Ataques de Llamadas Telefónicas, Fuerza Bruta, Dominio Fantasma, muestran un nivel de efectividad *Muy baja* del 94%, 92%, y 56% respectivamente.

Se ofrecen los resultados globales sobre el nivel de efectividad global de los ataques, y el porcentaje de Robustez mostrado por los diferentes niveles de seguridad:

<u>Resultados de análisis global efectividad de ataque y robustez nivel de seguridad</u>

1. Nivel de Efectividad Global de Ataque

Este índice indica cual es el ataque que se ha comportado como más eficaz para vulnerar las defensas de los diferentes niveles de seguridad. Para ello se han agrupado las respuestas de cada uno de los ataques por cada nivel de seguridad analizado.

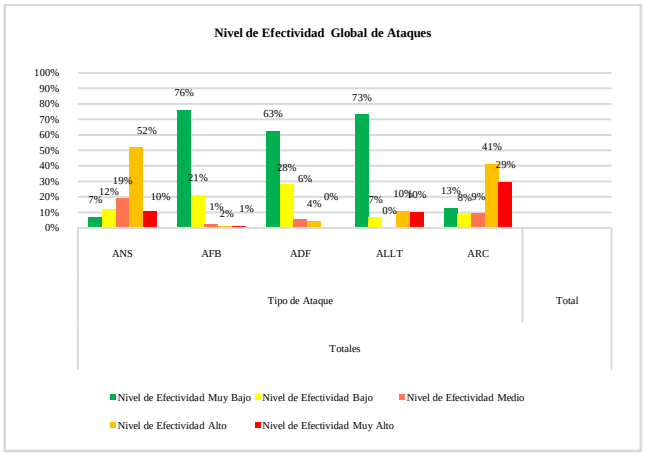

Figura 9: Nivel de efectividad Global de Ataques

2. Porcentaje Robustez Nivel de Seguridad

Este índice desarrollado por el equipo de investigación informa sobre cuál es el nivel de seguridad que se ha mostrado más robusto, es decir, que es el menos afectado por los cinco ataques que ha recibido. Para ello se han agrupado las respuestas extremas de la escala de efectividad de ataque, por un lado forman una categoría las respuestas Muy Alta-Alta y por otro lado la que conforman las respuestas Muy Baja y Muy Baja. Una vez agrupada se ha analizado a la inversa, es decir, aquel ataque que sobre un nivel de seguridad obtiene un nivel de efectividad de Muy Alto es que el nivel de seguridad es muy bajo en su protección, y al contrario.

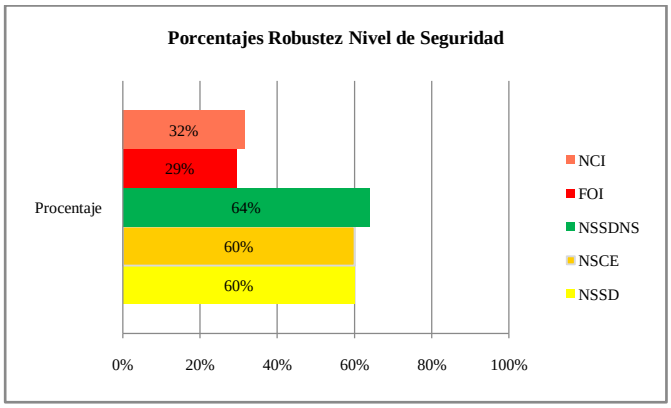

Figura10: % Robustez Nivel de Seguridad

5. CONCLUSIONES

En una conclusión inicial observamos que en líneas generales ha sido bastante accesible romper las medidas protectoras de los diversos niveles de seguridad ya que en todos ellos ha sido posible generar algún tipo de intrusión.

A la vista de los resultados obtenidos se puede concluir para dar respuesta a los objetivos inicialmente lo siguiente:

1. El ataque que se ha mostrado más efectivo para vulnerar los niveles de seguridad planteada ha sido el de Robo de Contraseña. Se observa que tiene un porcentaje sumado de Muy Alta, y Alta efectividad de 70%. Por el contrario, el ataque que se ha mostrado menos efectivo, y por tanto, ha sido menos intrusivo ha sido el de Fuerza Bruta con un escaso 97% sumando las evaluaciones de Muy Baja y Baja efectividad.

2. El nivel de seguridad que se ha mostrado más robusto a los diferentes ataques ha sido el de Negación de Servicios que muestra una aceptable respuesta de seguridad.

Los resultados nos ofrecen información para seguir mejorando esta tecnología cada vez más extendida entre la población actual y suministrada por diversos proveedores.

Si bien es cierto, habría que analizar en cada uno de los proveedores los protocolos y políticas de protección que tienen en cada una de sus nubes. La investigación realizada tiene la limitación que ha sido realizado en laboratorio y la extrapolación de resultados a la industria actual hay que tomarla con cautela ya que cada proveedor establece sus niveles de seguridad y sus acciones decontrol y protección ante externos.

No obstante, se ha podido comprobar cuál es el ataque de los cinco analizados más poderoso para acceder a niveles de seguridad de la nube, por lo que se podrá tener medidas concretas y personalizadas por cada usuario al respecto.

Teniendo en cuenta estos resultados y, en beneficio de la implantación progresiva con mayores estándares de seguridad de la tecnología *cloud computing*, se recomienda de forma específica a los responsables de tecnología de las empresas que definan claramente las normas y políticas de envío y recepción de correos electrónicos, y realizar auditorías informáticas buscando sobre el ingreso de información de los correos para medir la confiabilidad de los correos ingresados.

De igual manera, y ya a nivel general, se recomienda establecer y socializar las políticas de protección entre los clientes internos organizacionales, así como potenciar en la distribución de tiempo del personal tecnológico de la organización la gestión de la seguridad de la infraestructura *cloud computing*.

Finalmente, se considera que la tecnología *cloud computing* tiene más ventajas que inconvenientes y que como toda tecnología debe ser perfeccionada continuamente para dar el servicio de calidad y la confianza que necesitan sus usuarios.

REFERENCIAS

[1] Alliance, C. S., & Español, C. (2013). Estudio del ESTADO de la SEGURIDAD en CLOUD COMPUTING Año 2013 Objetivos • Caracterizar el estado de aplicación de • Aporte al Negocio de la Seguridad en Cloud • Puntos fuertes y débiles en la implantación actual de seguridad Cloud • Resultados obtenidos de Implantación Cloud.

[2] BATALLER, J. T. (2011). Seguridad en cloud computing, 1–25. Retrieved from http://dspace.cc.upv.es/handle/10251/11210

[3] Buyya, Rajkumar, y otros. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Retrieved from http://dx.doi.org/10.1016/j.future.2008.12.001.

[4] Catteddu, D., & Hogben, G. (2009). An SME perspective on Cloud Computing. Cloud Computing–SME Survey, ENISA report. Online: …. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:An+SME+perspective+on+Cloud+Computing#1

[5] Cloud computing: riesgos corporativos e implicaciones jurídicas. (2013). Retrieved June 09, 2013, from http://www.garrigues.com/es/publicaciones/articulos/Paginas/Cloud-computing-riesgos-corporativos-e-implicaciones-juridicas.aspx

[6] Computing, C. (2010). Conclusiones del Estudio "Estado y tendencias en Centros de Datos, 1–16.

[7] El 90% de las empresas ahorra costes con el cloud computing | Revista Cloud Computing. (2013). Retrieved April 04, 2013, from http://www.revistacloudcomputing.com/2013/03/el-90-de-las-empresas-ahorra-costes-con-el-cloud-computing/

[8] Hwang, K. (2009). Massively Distributed Systems: From grids and p2p to clouds. Retrieved from http://www.springerlink.com/content/b20700v83492544u.

[9] Mell, Peter y Grance, T. (2009). NIST Definition of Cloud Computing. Retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[10] Mena, E. K., & Guerrero, A. C. (2012). Computing de modelo privado para ofrecer Infraestructura como Servicio (IaaS).

[11] man, B., Eriksson, A. y Rembarz, R. (2009). What Networking of Information Can Do for Cloud Computing. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5159218&isnumber=5159183.

[12] ONE Digital Riesgos Actuales en la Implementación de Cloud Computing » ONE Digital. (2012). Retrieved December 18, 2013, from http://www.onedigital.mx/ww3/2012/12/18/riesgos-actuales-en-la-implementacion-de-cloud-computing/?utm_source=rss&utm_medium=rss&utm_campaign=riesgos-actuales-en-la-implementacion-de-cloud-computing#sthash.OgarbTva.dpbs

[13] Revista Lideres. (2012). Las empresas ecuatorianas se proyectan a la nube. Retrieved September 17, 2012, from http://www.revistalideres.ec/informe-semanal/EMPRESAS-ECUATORIANAS-PROYECTAN_0_775722433.html

[14] Sociedad Andaluza para el Desarrollo de las Telecomunicaciones. (2012). Cloud Computing, 144.

[15] Maya Proaño, I. (2011). *Ups.edu.ec*. Retrieved from Ups.edu.ec: http://retos.ups.edu.ec/documents/1999140/2025183/Art5.pdf

[16] INTECO-CERT. (2011). RIESGOS Y AMENAZAS EN CLOUD COMPUTING, 32.

[17] "América Latina lidera el cloud computing." [Online]. Available: http://www.madrimasd.org/informacionidi/noticias/noticia.asp?id=56223. [Accessed: 04-Sep-2013].