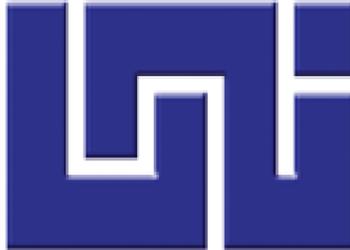


Universidad Nacional de Ingeniería  
Facultad de Electrotecnia y Computación



**"Integración de autenticación en servicio de correo electrónico y aulas virtuales del sistema nacional de inversión pública (SNIP)"**

Marbely de los Ángeles Lara López 2008-23876

Tutor: Ing. Néstor Traña Obando

Managua, Noviembre 2018

## Contenido

I.	INTRODUCCIÓN.....	1
II.	ANTECEDENTES .....	3
III.	JUSTIFICACIÓN.....	4
IV.	OBJETIVO GENERAL.....	5
V.	OBJETIVOS ESPECÍFICOS .....	5
VI.	MARCO TEÓRICO.....	6
6.1	Seguridad Informática .....	6
6.1.1	Seguridad en la web .....	7
6.1.2	Tipos de seguridad informática.....	7
6.2	Ataques Informáticos.....	8
6.2.1	Tipos de ataques .....	8
6.3	Sistema de detección de intrusos .....	11
6.3.1	Arquitectura de un IDS.....	11
6.4	Latch .....	12
6.4.1	Funcionalidades De Latch.....	12
6.4.2	Precios de membresías .....	13
6.4.3	Plugins Gratuitos.....	14
6.4.4	SDK Disponibles .....	14
6.5.	Aulas Virtuales .....	15
6.5.1	Ventajas de Moodle .....	17
6.5.2	Características de Moodle .....	17
6.6	Servidor de correo electrónico.....	18
6.6.1	Squirrelmail.....	18
6.7	Wordpress.....	19
6.8	OSSTMM.....	20
6.8.1	Secciones y módulos Metodología OSSTMM .....	20
6.9	WPScan.....	23
6.10	Zenmap .....	25
6.10.1	Características .....	25
VII.	DISEÑO METODOLÓGICO .....	27
7.1	Fase 1: Recopilación De Datos .....	27
7.1.1	Estudio de Factibilidad .....	29

7.2 Fase 2: Realización De Pruebas De Intrusión .....	34
7.2.1 Prueba de acceso al servicio de aulas Virtuales .....	36
7.2.2 Prueba de acceso al sitio web “Snip.com” .....	37
7.2.3 Prueba de acceso al servicio de Correo electrónico.....	38
7.3 Fase 3: Implementación de Latch .....	39
7.3.1 Crear una aplicación en Latch.....	39
7.3.2 Agregar Latch a Wordpress .....	40
7.3.3 Agregar Latch a Moodle.....	41
7.3.4 Agregar Latch a SquirrelMail.....	42
7.3.5 Casos de Uso .....	44
7.3.6 Plantilla de Casos Usos .....	50
7.4 Fase 4: Capacitación A Usuarios.....	68
7.4.1 Moodle.....	68
7.4.2 Wordpress .....	69
7.4.3 Correo.....	70
7.4.4 Pruebas acceso .....	72
VIII. CONCLUSIONES.....	77
IX. RECOMENDACIONES.....	78
X. GLOSARIO.....	79
XI. BIBLIOGRAFÍA .....	80
XII. ANEXOS .....	82
12.1 Integración de Latch en Moodle .....	82
12.2 Integrar Latch en Wordpress .....	86
12.2.1 Paso 1: Crear aplicación en Latch.....	86
12.2.2 Paso 2: Añadir Plugins.....	87
12.3 Integrar Latch en SquirrelMail.....	89
12.3.1 Paso 1: Crear aplicación en Latch.....	89
12.3.2 Paso 2: Integrar Latch.....	90
12.4 Añadir un servicio en la aplicación de latch .....	93

## Índice de Ilustraciones

Ilustración 1 Fases de un Ataque Informático .....	9
Ilustración 2 Plugins .....	14
Ilustración 3 SDK.....	14
Ilustración 4 Metodología OSSTMM (Creación Propia).....	22
Ilustración 5 Escaneo Wordpress.....	24
Ilustración 6 Interfaz ZenMap .....	26
Ilustración 7 Topología de red del SNIP .....	28
Ilustración 8 Escaneo base de datos Whols .....	34
Ilustración 9 Identificación de Servicios.....	35
Ilustración 10 Prueba de acceso Moodle 1 .....	36
Ilustración 11 Prueba de acceso Moodle 2 .....	36
Ilustración 12 Intento de acceso SNIP 1 .....	37
Ilustración 13 Intento de acceso SNIP 2 .....	37
Ilustración 14 Intento de acceso Correo 1.....	38
Ilustración 15 Intento de acceso Correo 2.....	38
Ilustración 16 Agregar nueva aplicación.....	39
Ilustración 17 integración de latch en WordPress .....	40
Ilustración 18 Opción de plugins en Wordpress .....	40
Ilustración 19 integración de latch en Moodle .....	41
Ilustración 20 Comprobación de plugins Moodle.....	41
Ilustración 21 integración de latch en SquirrelMail .....	42
Ilustración 22 Edición archivo Config.php .....	42
Ilustración 23 LatchConfiguration .....	43
Ilustración 24 Pareo de Latch con Moodle .....	68
Ilustración 25 Pareo de Latch con Wordpress.....	69
Ilustración 26 Pareo de Latch con SquirrIMail .....	70
Ilustración 27 Servicios Agregados .....	71

Ilustración 28 Servicios desbloqueados .....	72
Ilustración 29 Notificación de acceso Correo .....	73
Ilustración 30 Notificación de Acceso Moodle .....	73
Ilustración 31 Notificación de acceso Wordpress .....	74
Ilustración 32 Servicios bloqueados .....	74
Ilustración 33 Notificación de acceso Correo .....	75
Ilustración 34 Notificación de acceso Moodle.....	75
Ilustración 35 Notificación de acceso Wordpress.....	76
Ilustración 36 Creación de aplicación Moodle .....	82
Ilustración 37 Archivos De Latch.....	83
Ilustración 38 Comprobación de plugins .....	84
Ilustración 39 Plugins actualizados .....	84
Ilustración 40 Activación de Plugins .....	85
Ilustración 41 Ingreso de ID y Secreto .....	85
Ilustración 42 Creación de aplicación Wordpress.....	86
Ilustración 43 Búsqueda de Plugins .....	87
Ilustración 44 Descarga e instalación de plugins.....	87
Ilustración 45 Comprobación de plugins instalado .....	88
Ilustración 46 Ingreso de ID y Secreto .....	88
Ilustración 47 Creación de aplicación Correo .....	89
Ilustración 48 Archivos de instalación latch.....	90
Ilustración 49 Ubicación archivo Config.php.....	91
Ilustración 50 Edición archivo config.php .....	91
Ilustración 51 Ubicación archivo LatchConfig.....	92
Ilustración 52 Edición archivo LatchCofiguration.php.....	92
Ilustración 53 Generar Código.....	93
Ilustración 54 Ingreso de Token .....	94
Ilustración 55 Notificación de servicio Agregado .....	94

Ilustración 56 Ingreso de Token en Moodle .....	95
Ilustración 57 Notificación se servicio pareado.....	95
Ilustración 58 Opción para configurar Latch.....	96
Ilustración 60 Ingreso de Token .....	96
Ilustración 59 Notificación de servicio Pareado.....	96

## Índice de tablas

Tabla 1 Características .....	12
<b>Tabla 2 Precios</b> .....	13
Tabla 3 Entrevista .....	27
<b>Tabla 4 Recursos Humanos</b> .....	30
Tabla 5 Insumos.....	30
Tabla 6 Activos de la institución .....	32
Tabla 7 Equipos para implementar Latch.....	32
Tabla 8 Plantilla de casos de uso.....	50
Tabla 9 Configuración .....	51
Tabla 10 Notificaciones Sonoras.....	52
Tabla 11 Notificaciones de acceso.....	53
Tabla 12 Preguntar Contraseña .....	54
Tabla 13 Tiempo de bloqueo.....	55
Tabla 14 sugerencias de TOTP.....	56
Tabla 15 Condiciones de Uso .....	57
Tabla 16 Acuerdo de licencia .....	58
Tabla 17 Condiciones de uso .....	59
Tabla 18 Licencia de terceros .....	60
Tabla 19 Pestaña Ayuda .....	61
Tabla 20 Preguntas Frecuentes .....	62
Tabla 21 Contacta con nosotros.....	63

Tabla 22 Ajustes de Seguridad .....	64
Tabla 23 Gestión se Sesiones.....	65
Tabla 24 Cambio de Contraseña.....	66
Tabla 25 Acerca de Latch.....	67

### **Índice de Casos de uso**

CU 1 Latch .....	44
CU 2 Pestaña Configuración .....	45
CU 3 Pestaña de Condiciones de Uso .....	46
CU 4 Pestaña Ayuda.....	47
CU 5 Pestaña Ajuste de Seguridad.....	48
CU 6 Pestaña Acerca de Latch .....	49

## I. INTRODUCCIÓN

El último estudio realizado por Iifebelt revela que, *“la intensidad de uso de redes sociales en la región ha mostrado un incremento, debido a que las personas ven el uso de esta como una fuente de información y una manera de mantenerse comunicados.”* (V estudio de redes sociales Centroamérica y el Caribe, 2015). En Nicaragua diferentes instituciones o empresas, se han decidido por el uso de éstas para facilitar la comunicación entre sus empleados. En la mayoría de los casos los usuarios de las redes sociales solo hacen uso de las formas más comunes de autenticación las cuales se llevan a cabo haciendo uso de un usuario y una contraseña. El problema con esta práctica es que los atacantes sólo necesitan conocer el usuario y adivinar la contraseña para poner en riesgo las cuentas.

Los usuarios y administradores de los sitios web del Sistema Nacional de Inversión Pública (SNIP), institución perteneciente al Estado de Nicaragua, utilizan la opción de usuario y contraseña como método de autenticación en sus cuentas de correo electrónico institucional y aula virtual, debido a la vulnerabilidad de contar con autenticación simple, se han visto bajo riesgos de usurpación de identidades. Esto implica una búsqueda de soluciones óptimas para mitigar este tipo de situaciones.

Para brindar una mayor protección a las cuentas en línea, los sitios web están haciendo uso de diferentes métodos de autenticación con la ayuda de factores que complementan la autenticación simple, tales como el uso de huella digital, aplicaciones instaladas en los teléfonos inteligentes y el envío de códigos de verificación a través de mensajes de textos, que luego son introducidos en el servicio que se está utilizando. Aunque este tipo de autenticación resulta muy costosa *“sitios como Gmail y Facebook hacen uso de estos, los cuales son conocidos como mensajes TOTP (Time-based One Time Password o Contraseña de un único uso basada en el tiempo)”*, (Alberto Castro Gallardo, 2015).

Los Hardware Token de seguridad, son otro tipo de autenticación, “*estos son pequeños dispositivos que generan códigos para facilitar la autenticación de los usuarios autorizados.*” (HSBC Argentina, 2015). En Nicaragua existen instituciones bancarias (BAC, FICOHSA) que ofrecen este servicio a sus clientes. Además de estos dispositivos existen los Soft Tokens, estos son **softwares** que permiten el acceso remoto a sistemas informáticos empresariales y servicios en línea sin tener que utilizar los dispositivos antes mencionados (Token de seguridad). Este último tipo de autenticación se lleva a cabo en dos pasos, por lo tanto, es el más indicado a emplearse en el SNIP, con el fin de proteger las identidades digitales de sus usuarios.

## II. ANTECEDENTES

El desarrollo de las tecnologías en la última década ha dado un impulso notable a nuevas tendencias de seguridad para la información en lo que a empresas o instituciones se refiere, debido al incremento de robos de identidad que se presentan cada vez más a menudo.

El Sistema Nacional de Inversión Pública (SNIP), es una institución encargada del proceso de inversión en Nicaragua. Además, de formular las políticas de inversión, otorga certificación técnica a los proyectos que demandan financiamiento público, monitorea y da seguimiento a la ejecución e impacto del programa de inversiones, también, genera y difunde información integra, confiable y oportuna de la inversión.

El SNIP al estar encargado de información clasificada, cuenta con un servidor de correo llamado After Logic, además pretende brindar cursos online de capacitación y entrenamiento en el área de contabilidad, auditoría y finanzas al colegio de contadores públicos de Nicaragua, haciendo uso de aulas virtuales, mediante la utilización de la herramienta Moodle. Los servicios antes mencionados solo hacen uso de usuario y contraseña como método de autenticación, lo cual no es viable para la institución ya que es una vulnerabilidad que puede ser aprovechada por agentes externos maliciosos.

Esta institución no cuenta con reportes de intrusión o intento de intrusión en tiempo real a los servicios de correo electrónico institucional, aula virtual ni sitio web, por lo que no se logra detectar los accesos no autorizados hasta que ya fueron vulnerados los servicios de internet que poseen, poniendo en riesgo la información de los trabajadores y de la institución misma.

Pensando en mitigar este tipo de situaciones la institución adquirió una herramienta llamada **FORTIGATE**, pero esta herramienta no realiza un análisis de los paquetes que pueden ser intrusivos hacia la red interna o provenir de la misma.

### **III. JUSTIFICACIÓN**

El uso de identidades digitales ha aumentado significativamente, en muchas ocasiones una persona posee más de una identidad digital y se le asigna una protección que en la mayoría de los casos está basada en “Usuario y Contraseña”. El contar con muchas identidades digitales y al tratar de protegerlas, existe una alta probabilidad que se repita alguna contraseña y, además, que esta no sea lo suficientemente robusta o que se haya construido a partir de un método de generación de contraseñas, la cual se logra inferir luego de conocerse la primera contraseña.

Hoy en día es muy común leer noticias en internet en las que se han hackeado cuentas de sitios web (Sony PlayStation Network, Adobe, Dropbox), quizás por no tener buenas políticas de seguridad contra ataques de fuerza bruta, basados en valores de usuario y no en valores de contraseña. Es decir, ataque que fijan un usuario y van cambiando la contraseña hasta que se pueda encontrar la contraseña correcta y lograr entrar a los sitios web.

Teniendo en cuenta este posible riesgo, el sistema nacional de inversión pública (SNIP), como primera etapa solicito la implementación de un segundo factor de autenticación para sus principales servicios de internet: correo electrónico institucional, Aula virtual y Sitio Web. Por tal razón, se planteó la utilización de Latch, como segundo factor de autenticación para mitigar estos posibles riesgos.

Latch permitirá bloquear y desbloquear las cuentas digitales de los usuarios desde dispositivos móviles (teléfonos inteligentes, Tablets) en cualquier momento, limitando el tiempo de exposición de las cuentas que este posee ante intentos de accesos no autorizados.

#### **IV. OBJETIVO GENERAL**

Integrar Latch como segundo factor de autenticación en los servicios de aulas virtuales y correo electrónico institucional del Sistema Nacional de Inversión Pública.

#### **V. OBJETIVOS ESPECÍFICOS**

- Determinar que Latch permita reducir los riesgos de ataque dirigidos a los servicios de correo y aulas virtuales del Sistema Nacional de Inversión Pública.
- Equipar los dispositivos móviles de los empleados con la herramienta Latch que mejore la seguridad de la vida digital de los usuarios de la institución.
- Realizar pruebas de intrusión para medir el nivel de seguridad que brinda la aplicación Latch a las cuentas de los usuarios.

## VI. MARCO TEÓRICO

### 6.1 Seguridad Informática

La principal función de la seguridad informática es la protección de información, de equipos individuales o conectados en una red, contra riesgos accidentales o intencionados. La seguridad informática puede estar en función de varios elementos tales como: las amenazas sobre los datos a proteger, la vulnerabilidad, confidencialidad, integridad y la disponibilidad o accesibilidad de los datos.

Los daños pueden ser causados por el mal funcionamiento de hardware, pérdida física de datos y acceso no autorizado a las bases de datos. La implementación de diversas técnicas de seguridad puede dificultar a la delincuencia el acceso a información sensible e importante para la organización.

Existen muchos factores que pueden afectar la seguridad de los sistemas de información de una organización, las cuales pueden provenir de usuarios o empleados no autorizados para manejo de cierta información, usurpando la personalidad de los usuarios autorizados, accediendo indebidamente a datos para su consulta, borrado o bien realizar modificaciones para su provecho. Otras amenazas pueden provenir de controles inadecuados de programación.

Además de los factores antes mencionados los sistemas de información pueden ser afectados *“por fallos debidos a causas físicas, las cuales pueden ser cortes de energía eléctrica, fuegos, terremotos, intervenciones de animales, entre otros”*. (José Manuel García, (2010). *La ética como asignatura en los estudios de informática*. Marzo 2015).

### **6.1.1 Seguridad en la web**

Según Garfinkel, 1999. *“La seguridad en la web es un conjunto de procedimientos prácticos y tecnologías para proteger los servidores, usuarios de la web y las organizaciones que los rodean.”* La seguridad es una protección contra el comportamiento inesperado. Es decir, seguridad en la red son las medidas que se toman para proteger una red del acceso no autorizado o interferencia accidental o intencional.

La seguridad en la web requiere de especial atención. Internet es una red de doble sentido, así como hace posible que los servidores web divulguen información a millones de usuarios, permite a los hackers, crackers, criminales y otros irrumpir en las mismas computadoras donde se ejecutan los servidores web. Hoy en día las empresas, instituciones y gobiernos utilizan la web para distribuir información importante además de realizar transacciones importantes, las cuales se vuelven vulnerables cuando los servidores web son violados ocasionando el daño de la reputación y pérdida de dinero.

### **6.1.2 Tipos de seguridad informática**

#### **6.1.2.1 Seguridad Física**

La seguridad física es la encargada del resguardo de los elementos de hardware de una empresa o institución, consiste en la aplicación de barreras físicas y procedimientos de control como medida de prevención ante situaciones como incendios, fallas eléctricas, terremotos, entre otros. La seguridad informática es uno de los aspectos más olvidados a la hora de diseñar un sistema informático.

#### **6.1.2.2 Seguridad Lógica**

En muchas ocasiones los sistemas no pueden verse afectados solo de manera física, sino contra la información almacenada, el activo más importante que posee una empresa o institución es la información por lo que deben existir técnicas, más allá de la seguridad física para asegurarla, entre las técnicas más utilizadas podemos mencionar los controles de acceso, autenticación, antivirus (en caso de que se utilice windows), encriptación y la autenticación.

## **6.2 Ataques Informáticos**

Los ataques informáticos consisten en el aprovechamiento de las debilidades o fallas en el software, hardware o en los usuarios que forman parte de una red o que utiliza un sistema informático.

### **6.2.1 Tipos de ataques**

#### **Trashing (cartoneo):**

Este ocurre generalmente cuando un usuario anota su usuario y contraseña en un papelito y luego, cuando lo recuerda, lo arroja a la basura. Esto por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar al sistema.

#### **Monitorización**

Este tipo de ataque se realiza para observar a la víctima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso en el futuro.

#### **Ataques de autenticación**

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

#### **Ataque de denegación de servicios - Denial of Service(DoS)**

Los protocolos existentes actualmente fueron diseñados para ser hechos en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

#### **Modificación (daño)**

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos).

## Etapas de un ataque informático

Tener conocimiento de las etapas que conforman un ataque informático, permite a los profesionales en seguridad comprender la forma en que se realiza un ataque, permitiéndoles comprender la manera en que los atacantes los llevan a cabo, aprovechando estas habilidades para proteger los sistemas de este tipo de situaciones.

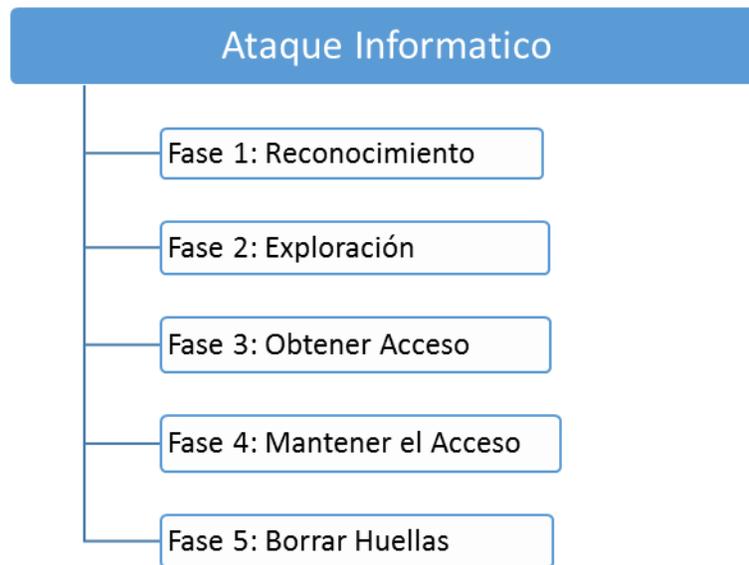


Ilustración 1 Fases de un Ataque Informático

**Fase 1:** Reconocimiento, Esta etapa involucra la obtención de información, con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas son la Ingeniería Social, el Dumpster Diving, el sniffing.

**Fase 2:** Exploración, En esta segunda etapa se utiliza la información obtenida en la fase de reconocimiento para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

**Fase 3:** Obtener acceso, En la fase 3 se empieza a materializar el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración.

Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDoS), Password filtering y Session hijacking.

**Fase 4:** Mantener el acceso, Una vez que se ha conseguido acceder al sistema, se implantan herramientas que permitan acceder en el futuro desde cualquier lugar donde se tenga acceso a Internet. Para ello, se puede recurrir a utilidades como backdoors, rootkits y troyanos.

**Fase 5:** Borrar huellas, Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS).

### 6.3 Sistema de detección de intrusos

Un sistema de detección de intrusos es una herramienta de seguridad encargada de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión que puedan comprometer la confidencialidad, integridad, disponibilidad de la información resguardada por la institución. Las intrusiones pueden producirse en diferentes formas como atacantes que acceden a los sistemas desde internet, usuarios que hacen mal uso de los privilegios asignados. La detección de intrusiones permite a las organizaciones proteger los sistemas de las amenazas que se presentan cuando incrementa la conectividad en la red. **(Álvarez Oliva, Alberto. (2013). Seguridad en Redes y Sistemas, Detección de Intrusiones con SNORT. Junio, 2015).**

#### 6.3.1 Arquitectura de un IDS

Aunque no es un estándar generado por alguna entidad certificadora, la arquitectura de IDS se compone de los siguientes parámetros:

1. **Recolección de datos:** A través de los logs de registro de los dispositivos de red se pueden recopilar datos.
2. **Parámetros:** Configuración de las reglas que determinan acciones particulares de amenazas o fallas de seguridad en la red.
3. **Filtros:** Comparan datos obtenidos en la parte de recolección de datos con los parámetros.
4. **Detector de eventos:** Función del IDS para alertar al administrador sobre actos inusuales en el tráfico de la red.
5. **Dispositivo generador de alarmas:** Según la configuración que el administrador le proporcione al IDS este está en capacidad de alertar mediante correo electrónico o vía SMS.

## 6.4 Latch

Latch es una aplicación desarrollada por ElevenPaths, esta permite proteger las cuentas y servicios online cuando el usuario no se encuentre conectado, permitiendo al usuario bloquear temporalmente funcionalidades del servicio como el mecanismo de inicio de sesión, en las cuentas de correo electrónico, usuarios de cuentas bancarias, servidores SSH u otro servicio que el usuario desee proteger.

Latch se comporta como un servicio totalmente independiente del sistema de autenticación que se utiliza en el servicio donde será implantado, por tal motivo no tiene acceso a las credenciales de las cuentas del sistema de destino (correo electrónico, Aula virtual o sitio web).

La integración de esta aplicación funciona sobre una infraestructura existente, integrándose fácilmente con los sistemas que el usuario posee.

### 6.4.1 Funcionalidades De Latch

Entre las funcionalidades de Latch se pueden mencionar las siguientes:

- Evitar los accesos no autorizados a las cuentas digitales de los usuarios, con la ayuda de un dispositivo inteligente (Teléfono celular o Tablet).
- Permite habilitar la programación de horarios para realizar un bloqueo automático del servicio.
- El usuario puede realizar un seguimiento de los intentos de acceso no validos que pueden realizarse al servicio online integrado a Latch.

<i>Características del servicio</i>	<b>Community</b>	<b>Silver</b>	<b>Gold</b>	<b>Platinum</b>
<i>Máximo de cuentas pareadas</i>	50	6,000	Ilimitadas	Ilimitadas
<i>Máximo de aplicaciones</i>	2	10	Ilimitadas	Ilimitadas
<i>Número máximo de operaciones por aplicación</i>	4	10	Ilimitadas	Ilimitadas
<i>Plugins Standard y SDKs</i>	Gratuitos	Gratuitos	Gratuitos	Gratuitos
<i>Actualizaciones gratuitas del servicio</i>	✓	✓	✓	✓

**Tabla 1 Características**

## 6.4.2 Precios de membresías

Community	Silver		Gold		Platinum
<b>Gratis</b>	<b>Licencias anuales para:</b>		<b>Licencias corporativas anuales</b>		<b>Información no disponible</b>
	100 Cuentas	\$79.32	3,000 Cuentas	\$6,798.44	
	500 Cuentas	\$ 396,58	6,000 Cuentas	\$13,596.89	
	1,000 Cuentas	\$793.15	10,000 Cuentas	\$22,661.48	
	3,000 Cuentas	\$ 2379,46	15,000 Cuentas	\$32,292.61	
	6,000 Cuentas	\$4758,91	25,000 Cuentas	\$50,988.33	
			50,000 Cuentas	\$96,311.29	
			100,000 Cuentas	\$169,961.10	
			200,000 Cuentas	\$294,59924	

*Precios válidos hasta el 31 de diciembre de 2018. Impuestos no incluidos.*

**Tabla 2 Precios**

### 6.4.3 Plugins Gratuitos

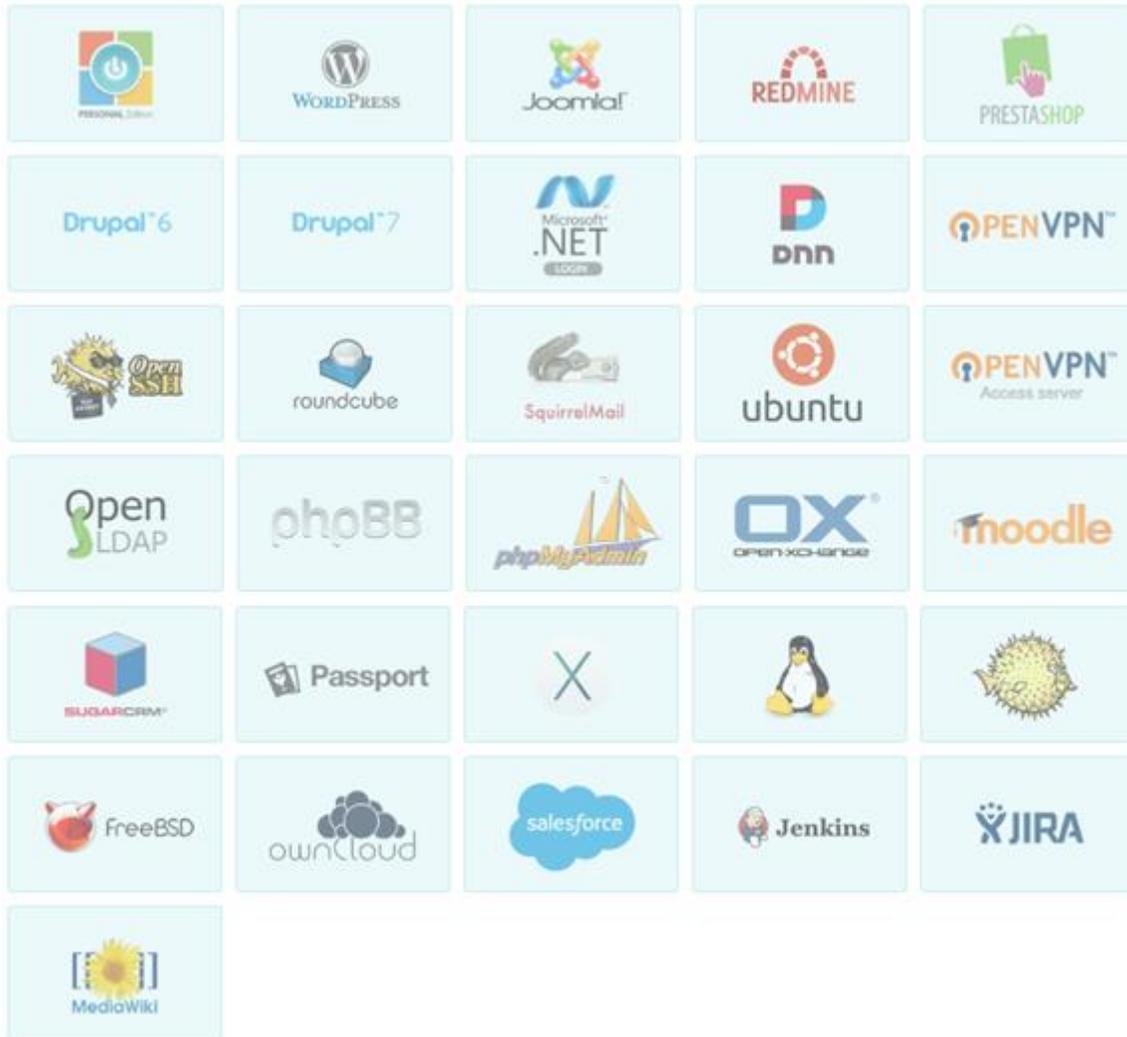


Ilustración 2 Plugins

### 6.4.4 SDK Disponibles

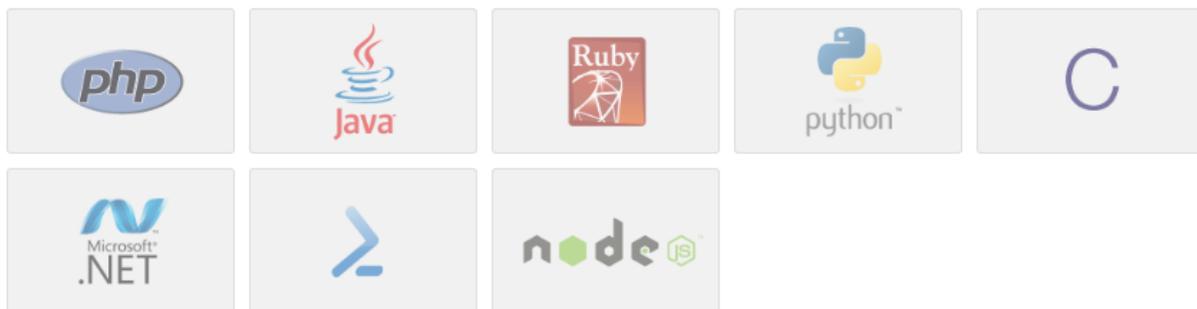


Ilustración 3 SDK

## 6.5. Aulas Virtuales

Las Aulas virtuales son plataformas de enseñanza virtual (elearning), mediante la cual docentes y alumnos disponen de diversas herramientas telemáticas que facilitan el desarrollo de los procesos de enseñanza y aprendizaje. Estas son plataformas que facilitan la docencia presencial/semipresencial/virtual y la creación de espacios colaborativos para grupos de trabajo multidisciplinarios<sup>1</sup>.

Algunas aulas virtuales son sistemas cerrados en los que el usuario se limita a las opciones brindadas por los creadores del espacio virtual para el desarrollo del curso, otras se extienden a lo largo y ancho de la red utilizando los hipertextos como su mejor aliado para que los alumnos no dejen de visitar o conocer otros recursos existentes en la red y relacionados con la clase.

Los elementos esenciales que componen un aula virtual son: distribución de la información entre educadores y educandos, intercambio de ideas y experiencias, aplicación y experimentación de lo aprendido, transferencia de los conocimientos e integración con otras disciplinas, evaluación de los conocimientos y el elemento más importante es la seguridad y confiabilidad del sistema.

Una de las Herramientas más conocidas para el desarrollo de Aulas virtuales es Moodle el cual es un sistema de gestión de cursos de libre distribución, desarrollado en GNU/Linux, utiliza plataforma Apache, PostgreSQL/MySQL y PHP (también conocida como plataforma LAMP).

---

<sup>1</sup> Moodle. (2015). *Acerca de Moodle*. Septiembre 2015, de Moodle Sitio web:

[https://docs.moodle.org/all/es/Acerca\\_de\\_Moodle](https://docs.moodle.org/all/es/Acerca_de_Moodle)

**Moodle está compuesto por módulos los cuales son:**

**Módulo tareas:** en este módulo se especifica la fecha final de entrega de una tarea, así como la calificación máxima que se podrá asignar. Los estudiantes pueden subir sus tareas al servidor.

**Módulo de Chat:** Permite una interacción fluida mediante texto síncrono, soporta direcciones URL, integración de HTML, imágenes, etc. Todas las secciones quedan registradas para verlas posteriormente además pueden ponerse a disposición de los estudiantes.

**Módulo consulta:** Es como una votación. Puede usarse para votar sobre algo o para recibir una respuesta de cada estudiante. El docente puede ver una tabla que presenta de forma intuitiva la información sobre quien ha elegido qué.

**Módulo Foro:** Hay dos tipos de foros disponibles: exclusivos para docentes, de noticias del curso y abiertos a todos. Las discusiones pueden verse anidadas, por rama o presentar los mensajes más antiguos o los más nuevos primeros. Si se usan las calificaciones de los foros, pueden restringirse a un rango de fechas.

**Módulo Cuestionarios:** Los docentes pueden definir una base de datos de preguntas que podrán ser reutilizadas en diferentes cuestionarios. Las preguntas pueden almacenadas en categorías de fácil acceso. Los cuestionarios se califican automáticamente y pueden ser recalificados si se modifican las respuestas. Además, pueden tener un límite de tiempo a partir del cual no estarán disponibles. Las preguntas y las respuestas de los cuestionarios pueden ser mezcladas (aleatoriamente) para disminuir las copias entre los alumnos.

**Módulo Recursos:** Admite la presentación de cualquier contenido digital, Word, power point, flash, video, sonidos, etc. Los archivos pueden subirse y manejarse en el servidor, o pueden ser creados sobre la marcha usando formularios web (de texto o HTML). Se pueden enlazar aplicaciones web, transfiriéndoles datos.

### **6.5.1 Ventajas de Moodle**

Accesible: Se puede acceder a Moodle desde cualquier parte del mundo con una conexión a internet.

Control: El docente hace un seguimiento muy exhaustivo de los alumnos, sobre el trabajo que estos realizan cada día y sus progresos a lo largo del curso.

Conocimientos: El alumno trabaja solo desde casa y los conocimientos adquiridos pueden llegar a ser mejores que en una clase presencial.

### **6.5.2 Características de Moodle**

- Presenta una interfaz que permite crear y gestionar cursos fácilmente.
- Los recursos creados en los cursos se pueden reutilizar
- Instalación sencilla requiriendo una plataforma que soporte PHP y la disponibilidad de una base de datos.
- Su arquitectura y herramientas son apropiadas para clases en línea, así como para complementar el aprendizaje presencial.

## **6.6 Servidor de correo electrónico**

Un servidor de correo está diseñado para operar y mantener las bases de correo y servicios de la organización. Los servidores de correos son aplicaciones de red ubicados en internet cuya función es parecida al correo postal. Los servidores de correo realizan una serie de procesos cuya finalidad es el transporte de información entre los usuarios<sup>2</sup>.

### **6.6.1 Squirrelmail**

Es una aplicación webmail desarrollada en PHP, es un software libre licenciado bajo GNU, puede ser instalada en la mayoría de servidores web que soporten PHP y el servidor web tenga acceso a un servidor IMAP y a otro SMTP. SquirrelMail sigue el estándar HTML 4.0 para su presentación, haciéndolo compatible con la mayoría de servidores web<sup>3</sup>.

Está diseñado para trabajar con plugins, lo cual hace más llevadera la tarea de agregar nuevas características entorno al núcleo de la aplicación.

---

*2 Servidor de Correo. Agosto 2016, de EcuRed. (2013). Sitio Web:*

*[https://www.ecured.cu/Servidor\\_de\\_correo](https://www.ecured.cu/Servidor_de_correo)*

*3 Instalación y configuración de SquirrelMail. Julio 2017 de Alcance Libre.org. Sitio Web:*

*<http://www.alcance Libre.org/staticpages/index.php/como-squirrelmail>.*

## 6.7 Wordpress

Es un sistema de gestión de contenidos CMS (Content Management System) que permite crear y mantener un blog u otro tipo de web. Dispone de un sistema de Plugins, que permiten extender las capacidades del mismo, de esta forma se consigue un CMS más flexible<sup>4</sup>.

Algunas de las características de WordPress son:

- Puede actuar como gestor de contenidos, como blog o como ambos simultáneamente.
- Al tener una base internacional, permite tener blogs y sitios web en casi cualquier idioma.
- Es fácilmente integrable con sus redes sociales favoritas y las de sus visitantes.
- La utilización de plantillas y temas permite hacer rediseños de todo el sitio más rápida y fácilmente que página a página.
- La comunidad de WordPress pone continuamente a disposición de sus usuarios gran cantidad de plugins que aumentan la capacidad básica de la aplicación.
- Funciona sobre PHP y MYSQL.
- Se instala localmente en el propio servidor, lo que proporciona mayor control sobre su configuración.

---

<sup>4</sup> Barberá, J. (2016). Qué es WordPress. Septiembre 2016, de sitio web: <https://www.xn--diseowebmurcia1-1qb.es/que-es-wordpress-y-para-que-sirve/>

## **6.8 OSSTMM**

OSSTMM (Open Source Security Testing Methodology Manual) es una metodología abierta de testeo de seguridad para la auditoría de los sistemas de información, que reúne de forma estandarizada y ordenada las diversas verificaciones y pruebas que se deben realizar durante el desarrollo de las auditorías informáticas. Esta metodología se divide en seis secciones las cuales están compuestas por módulos. *“Las secciones son puntos específicos en el mapa de seguridad, los módulos son el flujo de la metodología desde un punto de presencia de seguridad hacia el otro, cada módulo tiene una entrada y una salida. La entrada es la información usada en el desarrollo de cada área, la salida es el resultado de las tareas completadas, esta puede o no ser datos analizados, para servir como entrada de otro modulo”.* (2003, *Manual de Metodologías Abiertas de testeo de seguridad, ISECOM, Septiembre 2016*).

### **6.8.1 Secciones y módulos Metodología OSSTMM**

#### **I. Seguridad de la Información**

- 1 Revisión de la Inteligencia Competitiva
- 2 Revisión de Privacidad
- 3 Recolección de Documentos

#### **II. Seguridad de los Procesos**

- 1 Testeo de Solicitud
- 2 Testeo de Sugerencia Dirigida
- 3 Testeo de las Personas Confiables

#### **III. Seguridad en las tecnologías de Internet**

- 1 Logística y Controles
- 2 Sondeo de Red
- 3 Identificación de los Servicios de Sistemas
- 4 Búsqueda de Información Competitiva
- 5 Revisión de Privacidad
- 6 Obtención de Documentos
- 7 Búsqueda y Verificación de Vulnerabilidades
- 8 Testeo de Aplicaciones de Internet
- 9 Enrutamiento
- 10 Testeo de Sistemas Confiados
- 11 Testeo de Control de Acceso
- 12 Testeo de Sistema de Detección de Intrusos

- 13 Testeo de Medidas de Contingencia
- 14 Descifrado de Contraseña
- 15 Testeo de Denegación de Servicios
- 16 Evaluación de Políticas de Seguridad

#### **IV. Seguridad en las Comunicaciones**

- 1 Testeo de PBX 2
- 2 Testeo del Correo de Voz 3
- 3 Revisión del FAX 4
- 4 Testeo del Modem 5

#### **V. Seguridad Inalámbrica**

- 1 Verificación de Radiación Electromagnética (EMR)
- 2 Verificación de Redes Inalámbricas [802.11]
- 3 Verificación de Redes Bluetooth
- 4 Verificación de Dispositivos de Entrada Inalámbricos
- 5 Verificación de Dispositivos de Mano Inalámbricos
- 6 Verificación de Comunicaciones sin Cable
- 7 Verificación de Dispositivos de Vigilancia Inalámbricos
- 8 Verificación de Dispositivos de Transacción Inalámbricos
- 9 Verificación de RFID
- 10 Verificación de Sistemas Infrarrojos
- 11 Revisión de Privacidad

#### **VI. Seguridad Física**

- 1 Revisión de Perímetro
- 2 Revisión de monitoreo
- 3 Evaluación de Controles de Acceso
- 4 Revisión de Respuesta de Alarmas
- 5 Revisión de Ubicación
- 6 Revisión de Entorno

## Módulos de la Metodología OSSTMM

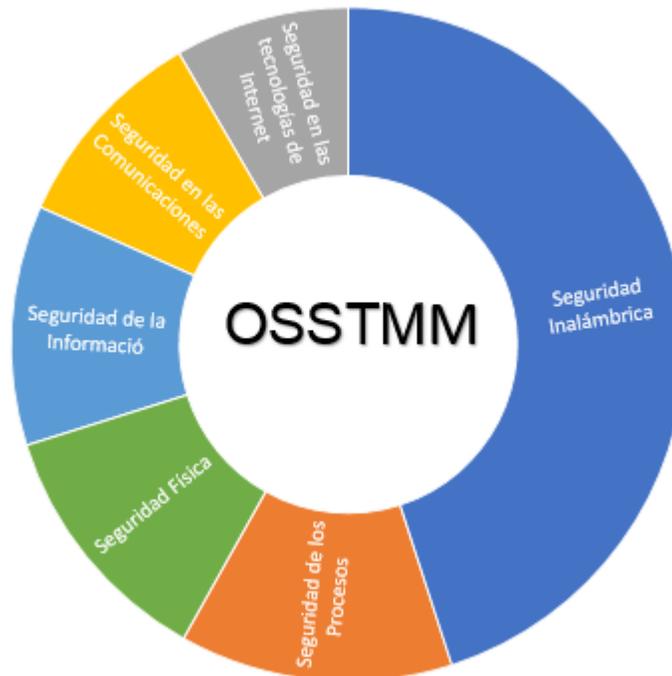


Ilustración 4 Metodología OSSTMM (Creación Propia)

Algunas de las tareas ejecutadas pueden no mostrar resultados, lo que significa que algunos módulos no tienen una entrada, por lo tanto, estos pueden ser ignorados durante el análisis.

Si un módulo no tiene salida como resultado, significa una de las siguientes opciones:

1. La tarea no fue ejecutada apropiadamente.
2. La tarea no es aplicable.
3. La tarea reveló niveles superiores de seguridad.
4. Los datos resultantes de la tarea no se analizaron correctamente.

Es muy importante identificar las tareas que pueden ser innecesarias y por lo tanto ser retiradas del análisis, donde el ámbito del proyecto o restricciones así lo requieran.

## 6.9 WPScan

WPSCAN es una herramienta más reconocidas y utilizadas para realizar auditorías de seguridad a Wordpress, dicha herramienta realiza un escáner de las vulnerabilidades de nuestro sitio con el fin de detectar posibles fallos de configuración que puedan comprometer la seguridad del sistema<sup>5</sup>.

Esta herramienta viene preinstalada en los sistemas operativos orientados a auditorias de seguridad, entre los sistemas en los que la herramienta viene preinstalada podemos mencionar BackBox Linux, Kali Linux asi como en Pentoo y SamuraiWTF.

Para realizar la instalación de dicha herramienta de debe contar con los siguientes requisitos: instalar Ruby con una versión mayor a 2.1.9 (La versión 2.3.1 es la recomendada), instalar Curl 7.21 (recomendable 7.29) y también RubyGems actualizadas a la última versión y Git.

Con WPScan es posible determinar los Plugins que fueron instalados en wordpress a través del siguiente comando:

```
ruby wpscan -url [URL del blog] -enumerate p
```

Una vez que los Plugins fueron detectados se realiza un chequeo contra las vulnerabilidades conocidas en los mismos, en el caso de que el resultado sea afirmativo, WPScan informara sobre la vulnerabilidad.

Con el siguiente comando es posible enumerar aquellos usuarios que utilizan la plataforma:

```
ruby wpscan -url [URL del blog] -enumerate u
```

---

<sup>5</sup> Mitchell, A. (2016). *WPScan: Encontrando Vulnerabilidades de WordPress*. Agosto 2017 Sitio web: <https://blog.sucuri.net/espanol/2015/12/usando-wpscan-encontrando-vulnerabilidades-de-wordpress.html>

WPScan posee un módulo que permite realizar fuerza bruta sobre aquellos usuarios que fueron enumerados utilizando un archivo del tipo diccionario. Otras de las funcionalidades que ofrece dicha herramienta es información sobre el tema (perfil gráfico) que tiene instalado el blog. Además, especifica la versión de WordPress que se encuentra instalada en el servidor. Esto puede utilizarse para comprobar que realmente se esté utilizando la versión más actual del sistema de gestión de contenidos. Además, en caso de que se tenga instalado una versión vulnerable de WordPress, WPScan especificará información relevante sobre dichas vulnerabilidades.

```
[+] WordPress version 4.8.2 (Released on 2017-09-19) identified from advanced fingerprinting, meta generator, links opml
[!] 1 vulnerability identified from the version number

[!] Title: WordPress 2.3-4.8.2 - Host Header Injection in Password Reset
    Reference: https://wpvulndb.com/vulnerabilities/8807
    Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html
    Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html
    Reference: https://core.trac.wordpress.org/ticket/25239
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295

[+] WordPress theme in use: wellington - v1.2.1

[+] Name: wellington - v1.2.1
    | Latest version: 1.2.1 (up to date)
    | Last updated: 2017-08-31T00:00:00.000Z
    | Location: http://192.168.1.111/wordpress/wp-content/themes/wellington/
    | Readme: http://192.168.1.111/wordpress/wp-content/themes/wellington/readme.txt
    | Style URL: http://192.168.1.111/wordpress/wp-content/themes/wellington/style.css
```

Ilustración 5 Escaneo Wordpress

## 6.10 Zenmap

Es una herramienta de código abierto de NMAP, multiplataforma, es utilizada para la exploración de redes y auditorias de seguridad, fue diseñada para analizar grandes redes pero esta también funciona contra equipos individuales, además permite extender dichas funciones mediante el uso de scripts para proveer servicios de detección avanzados, Nmap utiliza la captura de paquetes IP para determinar qué equipos se encuentran disponibles en una red, qué servicios ofrecen, qué sistemas operativos ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando. Además, durante el escaneo es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma<sup>6</sup>.

### 6.10.1 Características

- 1- Descubrimiento de servidores: identifica computadoras en una red.
- 2- Identifica puertos abiertos en una computadora objetivo.
- 3- Determinar los servicios que se están ejecutando, el sistema operativo y versión utiliza dicha computadora.
- 4- Obtiene algunas características del hardware de red de la máquina objetivo.

---

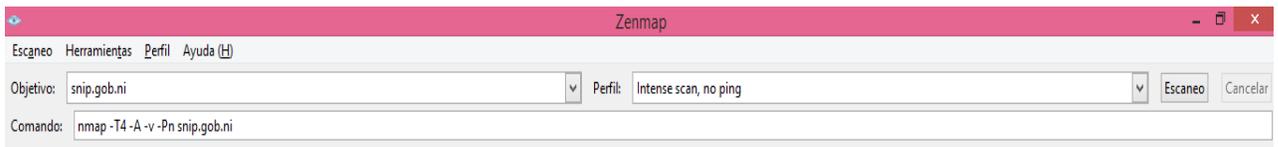
<sup>6</sup> Zenmap, la interfaz gráfica oficial de Nmap para escanear puertos a fondo. Noviembre 2018 Sitio Web: <https://www.redeszone.net/2014/01/18/zenmap-la-interfaz-grafica-oficial-de-nmap-para-escanear-puertos-a-fondo>.

En la interfaz gráfica de destacan las siguientes zonas:

**Objetivo:** En esta área se indica la dirección IP del objetivo o un rango de IPs.

**Perfil:** contiene una serie de perfiles de exploración determinados.

**Comando:** se muestra la orden Nmap que se está generando al ir indicando el perfil seleccionado y opciones añadidas.



**Ilustración 6 Interfaz ZenMap**

## VII. DISEÑO METODOLÓGICO

En el presente trabajo monográfico se hizo uso de metodologías de tipo intervención, evaluación y acción. De tipo intervención porque se realizaron pruebas de intrusión hacia las cuentas de algunos usuarios con el uso de la metodología OSSTMM, con el fin verificar la existencia de vulnerabilidades en el uso de autenticación simple, una vez realizadas dichas pruebas se realizaron acciones para mitigar la pérdida de información, con el fin de garantizar mayor seguridad a la información de los usuarios.

El trabajo monográfico se realizó en cinco fases.

### 7.1 Fase 1: Recopilación De Datos

Para esta fase se realizaron reuniones de grupo con directivos de la institución, con el fin de obtener la información necesaria para el desarrollo de este trabajo monográfico. Las herramientas utilizadas para la recopilación de información fueron: entrevistas dirigidas a los directivos, *observación* del sitio, esto con el objetivo de recopilar información de la red física y lógica, así como información de los usuarios.

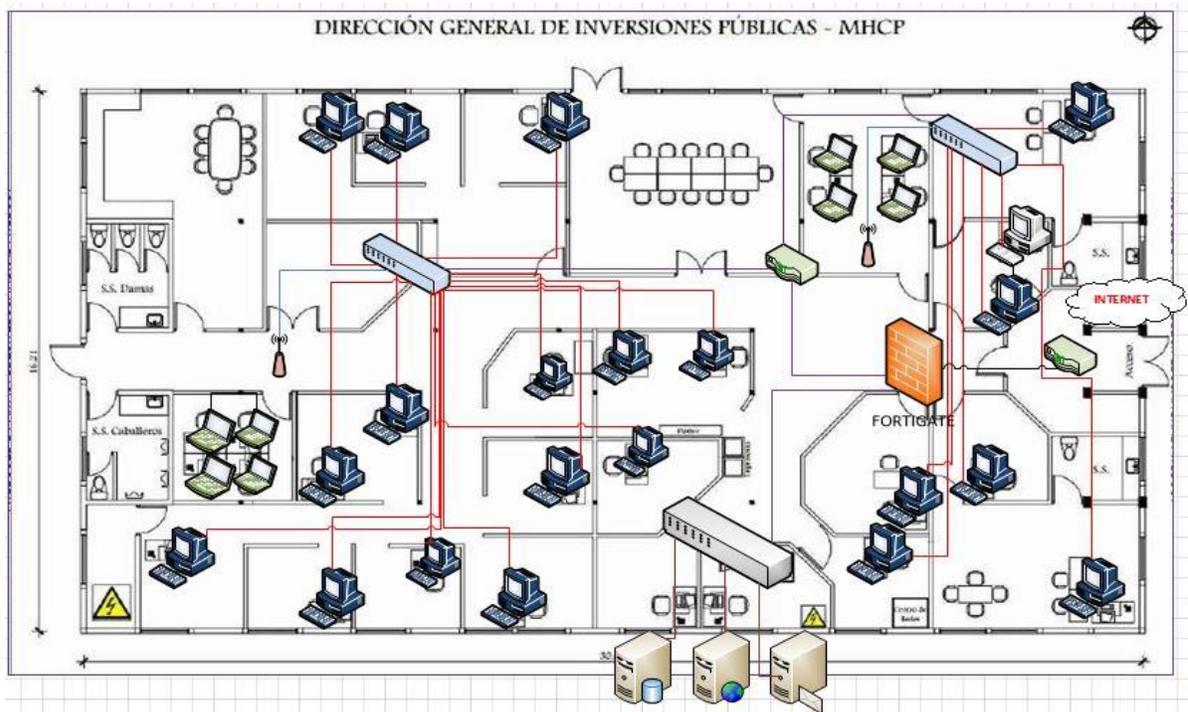
#### Entrevista

1. ¿Con cuántos servidores cuenta la institución y como se encuentran distribuidos?
2. ¿Dentro de la red de la institución cuentan con firewall?
3. ¿Qué tipo de servicios brindan a los usuarios?
4. ¿De los servicios brindados cual es el más vulnerable a ataques?
5. ¿Cuentan con alguna herramienta de seguridad para proteger los servicios indicados?
6. ¿De qué manera detectan cuando la cuenta de un usuario ha sido utilizado por personas no autorizadas?
7. ¿Cómo institución que medidas toman para reducir los ataques a las cuentas de usuarios?

Tabla 3 Entrevista

A continuación de se detalla la información obtenida luego de implementar las herramientas mencionadas anteriormente.

La institución cuenta con un servidor PowerEdge dell 2650 cuya función es maximizar la velocidad de procesamiento además de ofrecer un ancho de banda de memoria y la entrada/salida de datos. En esta visita se nos brindó un mapa de la red interna de la institución para poder observar la manera en que se encuentran distribuidos los recursos entre los trabajadores.



**Ilustración 7 Topología de red del SNIP**

La institución cuenta con un dispositivo de seguridad UTM Fortigate (Fortinet) el cual funciona como un firewall esto con el fin de prevenir intrusiones, filtrado web y protección frente a malware o correos no deseados, según nos indicaron el objetivo de la obtención de dicho dispositivo fue para evaluar las acciones que se deben llevar a cabo ante ataques externos, pero este no ha sido de gran utilidad ya que la herramienta es manipulada por terceros los cuales no reportan análisis instantáneos, por lo que tanto es una herramienta sin ningún provecho.

La institución actualmente solo ofrece el servicio de correo institucional y su sitio web, pero pretenden implementar el servicio de Aulas virtuales bajo Moodle, así como una herramienta para brindar protección de dichos servicios esto con el fin de brindar seguridad a los datos de los usuarios que utilicen dichos servicios.

### **7.1.1 Estudio de Factibilidad**

Implementar nuevos elementos en una institución implica realizar un estudio de viabilidad consecuente a lo que se pretende efectuar, a esto se le conoce como estudio de factibilidad, dentro de este se realizan diferentes actividades para recopilar datos que contribuyan a la toma de decisiones sobre lo que se requiere implementar. Este estudio de factibilidad está conformado de 3 aspectos: Operativo, Económico y Técnico

#### **7.1.1.1 Factibilidad Operativa**

Desde el punto de vista operativo LATCH como segundo factor de autenticación, será de apoyo para la Institución y sus directivos en el uso cotidiano de sus dispositivos dentro de la red en el SNIP, puesto que contribuirá en la seguridad de sus cuentas y los datos que se encuentran bajo su resguardo.

Este sistema cuenta con una interfaz gráfica de fácil aprendizaje, con un alto nivel de interacción con el usuario, lo que lo convierte en una herramienta de gran utilidad para los usuarios.

El SNIP como tal acepta la implementación Latch como segundo factor de autenticación, debido a que este le proporciona mayor seguridad. La institución cuenta con personal capacitado para el uso de dicha herramienta.

### 7.1.1.2 Factibilidad Económica

Alternativa propuesta: LATCH

Se presenta el análisis de las cotizaciones para esta propuesta, en cuanto a costos de software, recursos humanos e insumos.

El software utilizado corresponde a Latch, el cual se encuentra disponible para dispositivos Android, BlackBerry, Iphone, Firefox SO y Windows Phone.

- **Recursos humanos**

Cantidad	Personal	Salario x Mes	Total
1	Analista/Implementación	\$300	\$300
Total			\$300

Tabla 4 Recursos Humanos

- **Insumos**

Cantidad	Descripción	Costo
1	PC Dell Optiplex	\$500
1	Smartphone	\$150
Total		\$650

Tabla 5 Insumos

Para la implementación de este proyecto la institución no incurrirá en gastos con la compra de nuevos equipos ya que se utilizarán los dispositivos móviles (teléfono celular, Tablet) con los que cuentan los usuarios.

### 7.1.1.3 Factibilidad Técnica.

En la actualidad la institución del Sistema de Inversión Pública cuenta con una variedad de computadoras asignadas al personal administrativo, estos a su vez están conectados a una LAN.

Cantidad	Descripción
21	PC Dell Optiplex Procesador Core i7 2,7 GHz Memoria Interna 8 GB DDR4 – SDRAM Almacenamiento total 1000 GB Puertos tipo A 1 3.0 Gen1 LAN 10,100,1000 Mbit/s
8	Laptop Pantalla LED 14 “ Intel Celeron N3000 series 1,1 GHz Memoria Interna 4 GB DDR3 – SDRAM Almacenamiento 500 GB
3	Routers <span style="float: right;">Cisco</span> <span style="float: right;">861</span> Interfaz WAN: 10/100 Mbps Fast Ethernet Interfaz de LAN: Conmutador gestionado 10/100 FE de 4 puertos
3	<ul style="list-style-type: none"> <li>• 2 Switch Dell 5324 24 puertos. Algoritmo de encriptación SSL, SSL 3.0, SSL 2.0. Protocolo Ethernet. Método de autenticación: Secure Shell (SSH), RADIUS, TACACS +</li> <li>• 1 Switch Cisco Catalyst 3560G 24 puertos. Protocolo Ethernet. Método de autenticación: Kerberos, RADIUS, TACACS +,</li> </ul>

	Secure Shell v.2 (SSH2)
1	Servidor Dell 2650, Almacenamiento interno máximo 730 GB (5 x 146 GB), Tarjeta de interfaz de red Dos tarjetas integradas Broadcom® Gigabit BaseT con soporte para recuperación tras fallos y distribución de carga. Software Microsoft® Windows® 2000 Server; Microsoft Windows 2000 Advanced Server; Red Hat® Linux® 7.2.

**Tabla 6 Activos de la institución**

Los equipos necesarios para la implementación de LATCH deberán contar con los siguientes requerimientos:

Cantidad	Descripción
1	<p>Pc Dell</p> <p>UPC Core i5</p> <p>Memoria 4 ranuras DIMM DDR3. Máx. capacidad de la memoria del sistema: 16GB</p> <p>BIOS 32Mb AMI UEFI Legal BIOS con soporte GUI</p> <p>Chipset Intel® H61</p> <p>Disco Duro de 320GB</p> <p>- 2 puertos USB 3.1 Gen1 de ASMedia ASM1042, compatible con USB 1.0 / 2.0 / 3.0 hasta 5 Gb / s</p> <p>LAN PCI Gigabit x1 x 10/100/1000 Mb / s, 2 NEXT 10/100/1000 Mb / s.</p>
1	<p>Celular Smartphone</p> <p>Características mínimas</p> <p>Ram: 2GB</p> <p>Memoria interna: 8GB</p>

**Tabla 7 Equipos para implementar Latch**

El hardware requerido para la implementación de LATCH se encuentra dentro de la lista de los dispositivos con los que cuenta la institución, por lo que esta no deberá realizar la compra de equipos nuevos para la implementación del proyecto.

#### **7.1.1.4 Conclusión del estudio de Factibilidad**

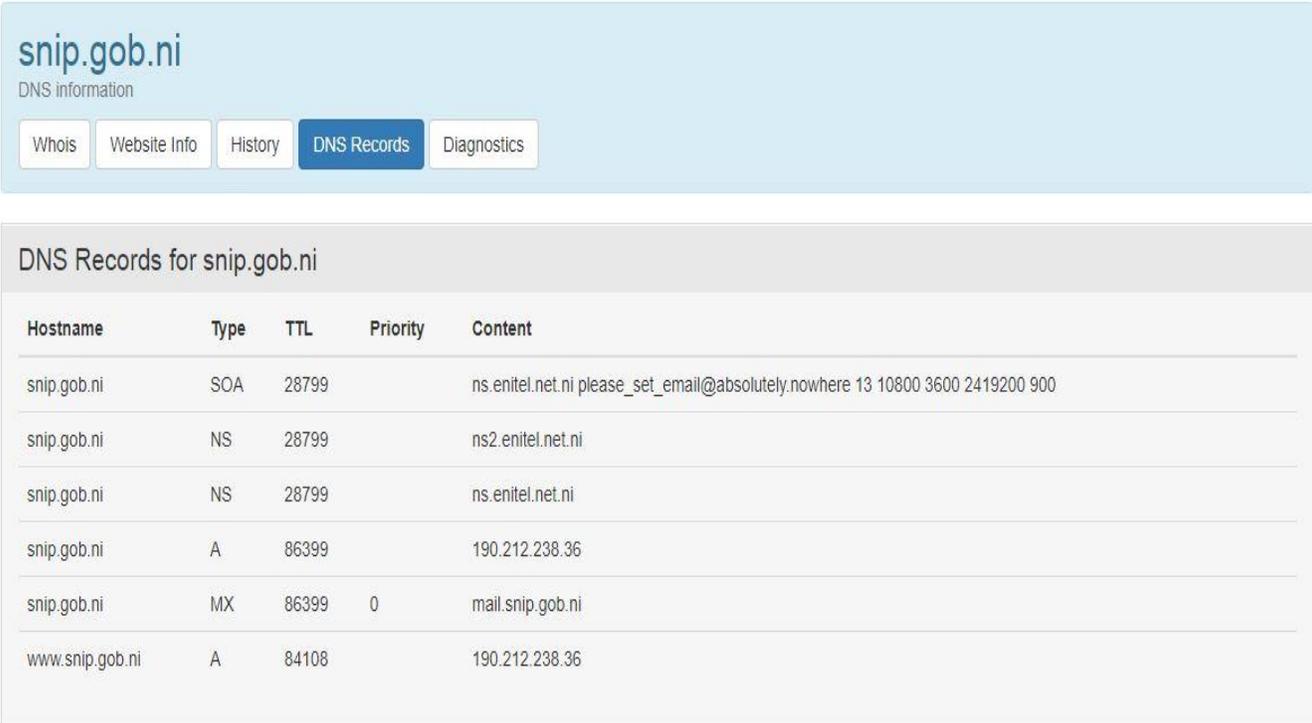
Demostrado en los puntos anteriores, tanto los estudios de factibilidad técnica, operativa y económica resultan ser favorables para la implementación del proyecto. Lo que determina su viabilidad. El proyecto resulta ser una buena herramienta para la institución, además de que no implica que el SNIP incurra en gastos.

## 7.2 Fase 2: Realización De Pruebas De Intrusión

En esta fase se realizaron pruebas de intrusión internas y externas a los inicios de sesión en los servicios de correo electrónico, aula virtual y sitio web con el fin de conocer la vulnerabilidad de estos servicios.

Para desarrollar esta fase se utilizó la metodología OSSTMM, las secciones utilizadas fueron las siguientes:

*Seguridad de la información:* en esta sección se ejecutó el módulo: **Revisión de inteligencia competitiva** en el cual se analizaron las bases de datos WHOIS con el fin de obtener información de los servicios de la institución y los nombres de hosts registrados.



The screenshot shows the 'snip.gob.ni' DNS information page. At the top, there are navigation buttons for 'Whois', 'Website Info', 'History', 'DNS Records' (which is selected), and 'Diagnostics'. Below this is a table titled 'DNS Records for snip.gob.ni' with the following data:

Hostname	Type	TTL	Priority	Content
snip.gob.ni	SOA	28799		ns.enitel.net.ni please_set_email@absolutely.nowhere 13 10800 3600 2419200 900
snip.gob.ni	NS	28799		ns2.enitel.net.ni
snip.gob.ni	NS	28799		ns.enitel.net.ni
snip.gob.ni	A	86399		190.212.238.36
snip.gob.ni	MX	86399	0	mail.snip.gob.ni
www.snip.gob.ni	A	84108		190.212.238.36

**Ilustración 8** Escaneo base de datos Whois

En la ilustración se muestra la información de la institución obtenida del sitio who.is

La siguiente sección que se utilizó es Seguridad en las tecnologías de Internet, donde se llevaron a cabo los siguientes módulos:

**Identificación de los Servicios de Sistemas**, en este módulo se realizó un escaneo a los hosts obtenidos en el módulo Revisión de inteligencia competitiva, para la realización de este módulo se utilizó la herramienta NMAP.

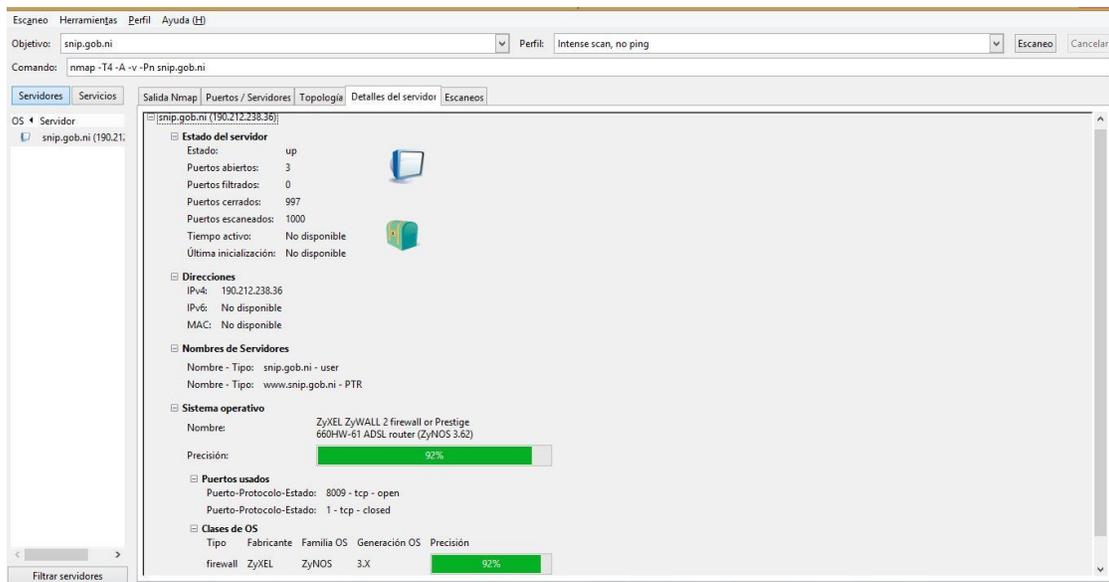


Ilustración 9 Identificación de Servicios

El último módulo que se realizó fue el **Testeo de control de acceso**, el cual consistió en realizar pruebas de acceso a los servicios de Aulas virtuales, sitio web y correo electrónico, contando únicamente con el usuario y escogiendo aleatoriamente contraseñas para dicho usuario, esto con el fin comprobar la vulnerabilidad del sistema frente a accesos o manipulaciones no autorizadas.

Para realizar este test se seleccionó un usuario específico y se ingresaron diferentes contraseñas con un tiempo estimado de 5 minutos, en total se ingresó cinco veces la contraseña errónea en cada uno de los servicios, en los cuales únicamente se obtuvo el mensaje de contraseña incorrecta, ninguno de los servicios emitió los mensajes tales como: Se ha excedido en número de intentos o que el servicio ha sido bloqueado por la cantidad de veces que se ingresó la contraseña incorrecta. Cabe mencionar que estos intentos de ingreso no generan ninguna alerta hacia los administradores ni usuarios de los servicios.

## 7.2.1 Prueba de acceso al servicio de aulas Virtuales

### Acceder

 Datos erróneos. Por favor, inténtelo otra vez.

Nombre de usuario

Contraseña

Recordar nombre de usuario

[¿Olvidó su nombre de usuario o contraseña?](#)

Las 'Cookies' deben estar habilitadas en su navegador 

Algunos cursos permiten el acceso de invitados

**Ilustración 10 Prueba de acceso Moodle 1**

### Acceder

 Datos erróneos. Por favor, inténtelo otra vez.

Nombre de usuario

Contraseña

Recordar nombre de usuario

[¿Olvidó su nombre de usuario o contraseña?](#)

Las 'Cookies' deben estar habilitadas en su navegador 

Algunos cursos permiten el acceso de invitados

**Ilustración 11 Prueba de acceso Moodle 2**

## 7.2.2 Prueba de acceso al sitio web “Snip.com”



The screenshot shows the WordPress login interface. At the top center is the WordPress logo. Below it, a red-bordered error message reads: "ERROR: La contraseña que has introducido para el usuario admin es incorrecta. ¿Has perdido tu contraseña?". Underneath, there are two input fields: "Nombre de usuario" containing the text "admin" and "Contraseña" containing six dots. At the bottom left is a checkbox labeled "Recuérdame" and at the bottom right is a blue button labeled "Acceder".

**Ilustración 12 Intento de acceso SNIP 1**



This screenshot is identical to the previous one, showing the WordPress login page with the same error message and login fields. The "Nombre de usuario" field contains "admin" and the "Contraseña" field contains six dots. The "Recuérdame" checkbox and "Acceder" button are also present.

**Ilustración 13 Intento de acceso SNIP 2**

### 7.2.3 Prueba de acceso al servicio de Correo electrónico

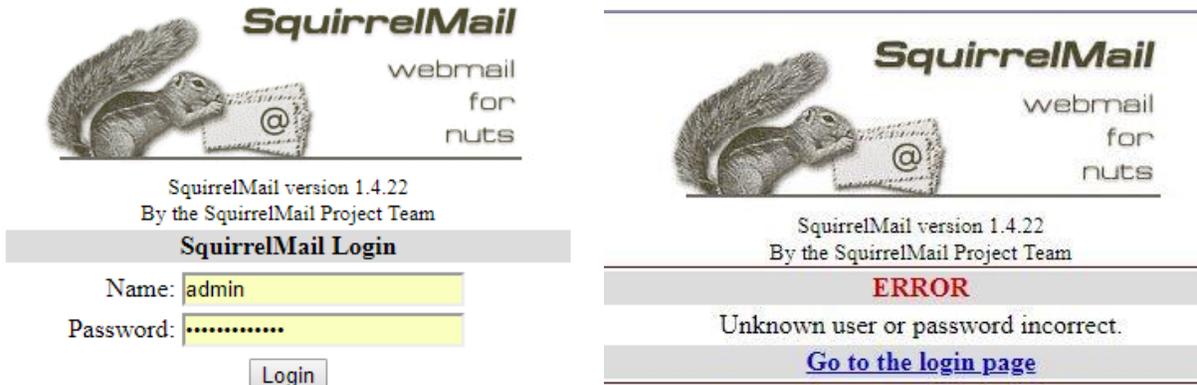


Ilustración 14 Intento de acceso Correo 1

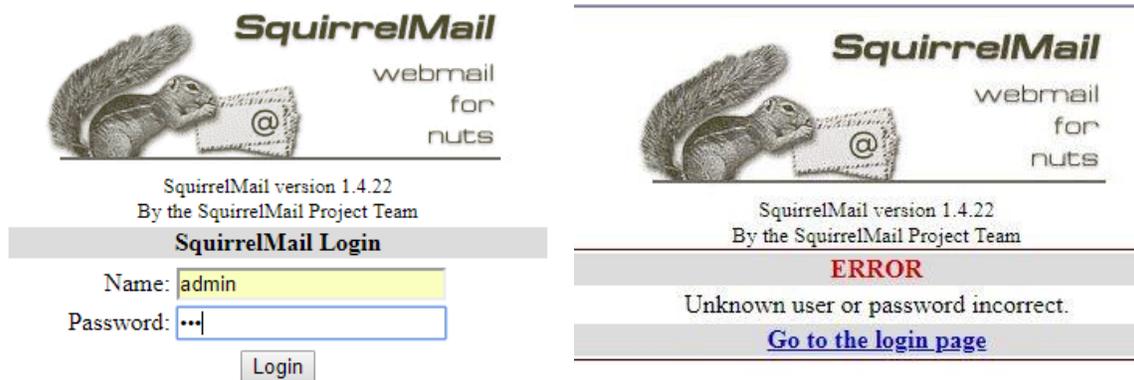


Ilustración 15 Intento de acceso Correo 2

### 7.3 Fase 3: Implementación de Latch

En esta fase se realizó la integración de Latch en los servicios de Moodle, SquirrelMail y Wordpress, a continuación se detallan los procedimientos.

Como primer paso se procedió a crear una cuenta de Latch de tipo desarrollador, para tener acceso a añadir nuevas aplicaciones.

#### 7.3.1 Crear una aplicación en Latch

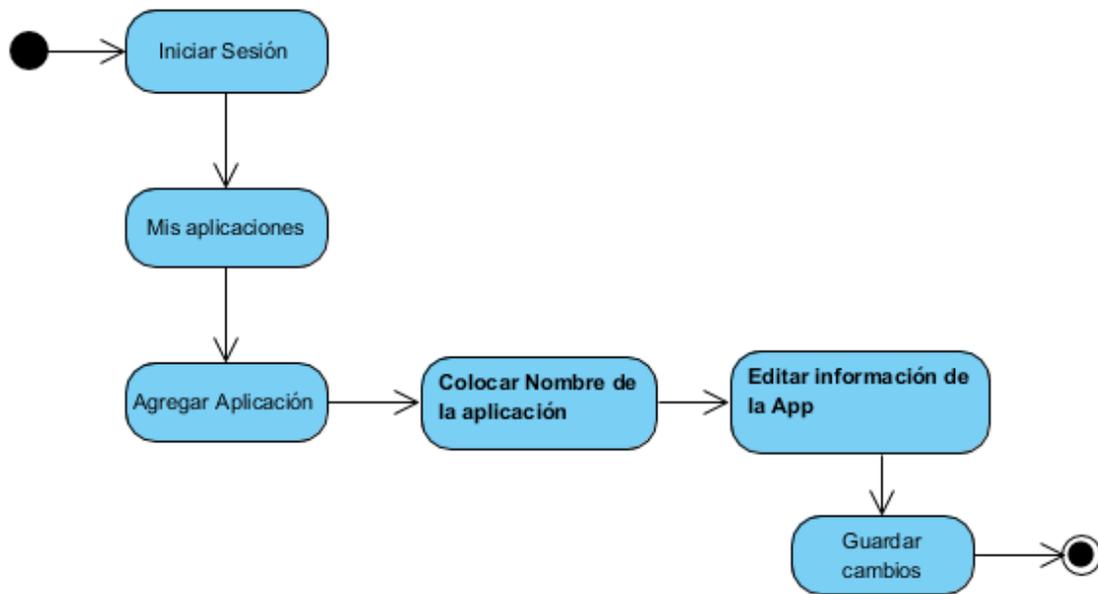


Ilustración 16 Agregar nueva aplicación

Para añadir una nueva aplicación se seleccionó la pestaña “Mis Aplicaciones” en la cual se muestra la opción para agregar nuevas aplicaciones y realizar las configuraciones necesarias para cada aplicación.

### 7.3.2 Agregar Latch a Wordpress

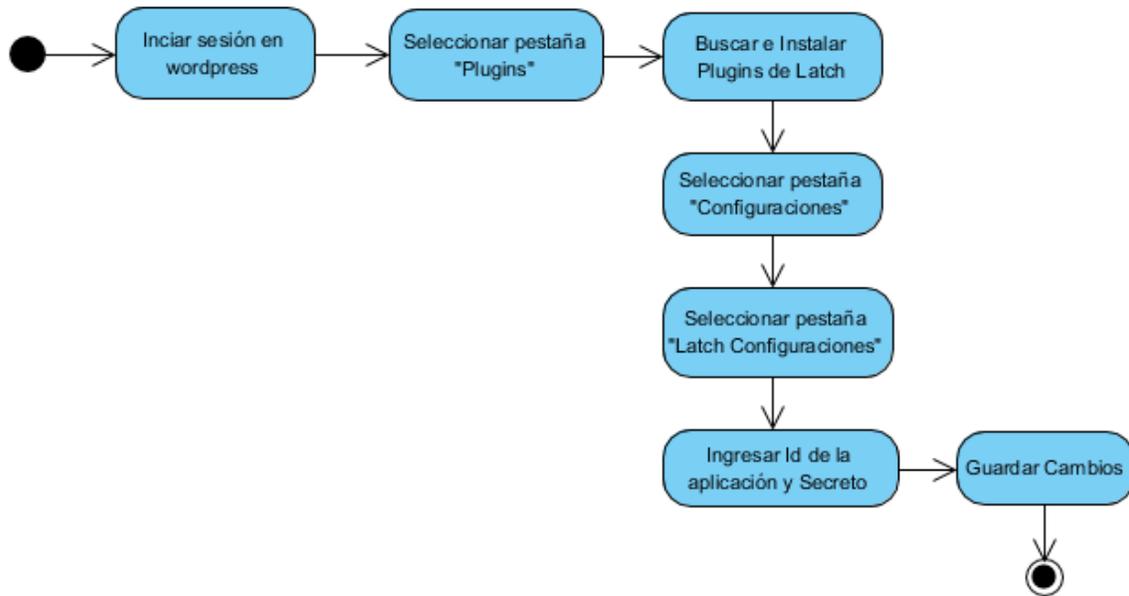


Ilustración 17 integración de latch en WordPress

Para añadir Latch en wordpress se inicia sesión como administrador, la pestaña de “Plugins”, se procede a buscar e instalar el Plugins de Latch.



Ilustración 18 Opción de plugins en Wordpress

Una vez que la aplicación se ha instalado, en la pestaña de configuraciones se seleccionó la opción “Configuraciones de Latch” la cual muestra un formulario en donde se ingresa el ID de la aplicación y el secreto finalmente guardan los cambios.

### 7.3.3 Agregar Latch a Moodle

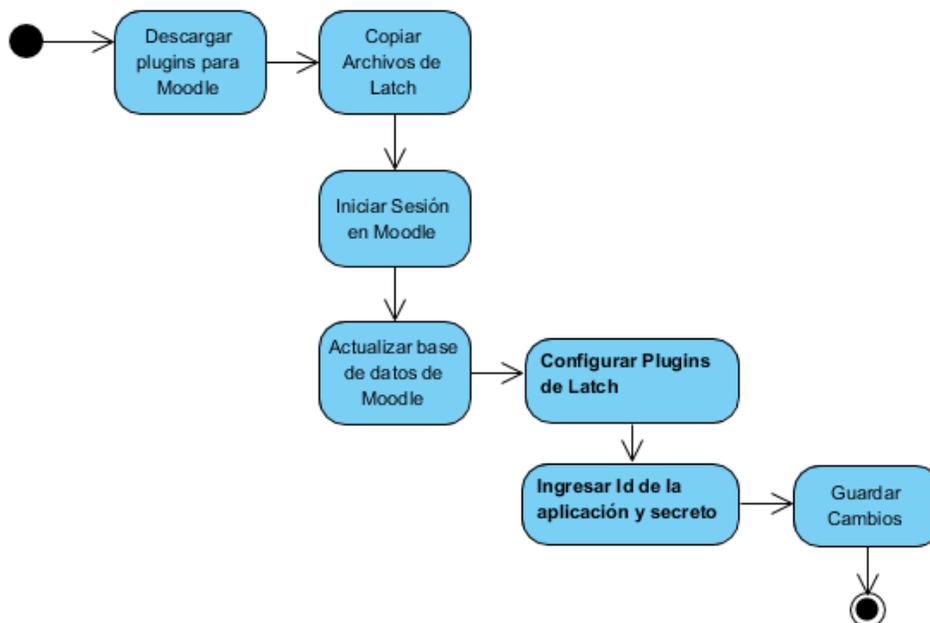


Ilustración 19 integración de latch en Moodle

Para agregar Latch a Moodle se descarga el Plugins desde la página principal de latch: <https://latch.elevenpaths.com>. La carpeta del Plugins se copia en la raíz de la carpeta de instalación de Moodle.

Luego se inicia sesión como administrador, donde el servicio muestra un mensaje de actualización de Plugins y se procede a actualizar la base de datos:

#### Comprobación de 'plugins'

Esta página muestra las extensiones (plugins) que pueden requerir su atención durante la actualización. Los elementos resaltados incluyen nuevas extensiones (plugins) que están a punto de ser instalados, los que van a ser actualizados y las extensiones anteriores que ahora faltan. Los módulos externos (add-ons) también se destacan. Se recomienda que compruebe si hay versiones más recientes de los módulos externos disponibles y actualice su código fuente antes de continuar con esta actualización de Moodle.

Compruebe actualizaciones disponibles

Última comprobación realizada el 10 de julio de 2017, 19:59

**Número de extensiones (plugins) que requieren atención durante esta actualización: 2**

Mostrar la lista completa de extensiones (plugins) instalados

Nombre de la extensión	Directorio	Origen	Versión actual	Nueva versión	Requiere	Estado
<b>Extensiones de identificación</b>						
latch		Adicional	2014030600			Ausente del disco
<b>Tipos de campos de perfiles</b>						
latch		Adicional	2014030600			Ausente del disco

Recargar

Actualizar base de datos Moodle ahora

Ilustración 20 Comprobación de plugins Moodle

Luego que las actualizaciones se instalaron, se procede a configurar el Plugins ingresando el ID y secreto correspondiente.

### 7.3.4 Agregar Latch a SquirrelMail

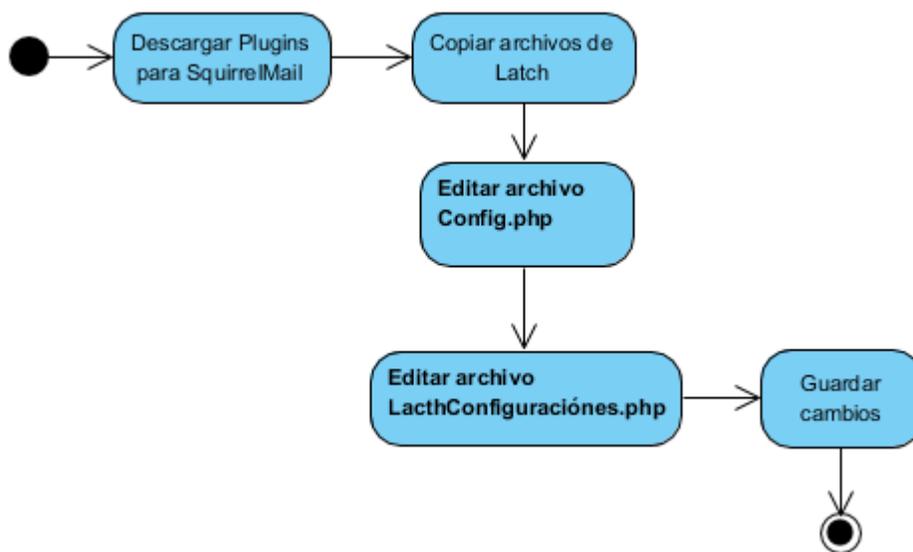


Ilustración 21 integración de latch en SquirrelMail

Para configurar Latch en squirrelMail, se descarga el Plugins desde la página de Latch, luego se descomprime y se guarda en la carpeta de “Plugins” que se encuentra en la carpeta de instalación de SquirrelMail. Después se procede a editar el archivo “Config.php” en el cual se activa la variable del Plugins de Latch.

```
937 * To install plugins, just add elements to this array that have
938 * the plugin directory name relative to the /plugins/ directory.
939 * For instance, for the 'squirreldspell' plugin, you'd put a line like
940 * the following.
941 *     $plugins[0] = 'squirreldspell';
942 *     $plugins[1] = 'listcommands';
943 */
944 $plugins[] = 'latch';
945
946 // Add list of enabled plugins here
947 |
948
949 /** Database */
950 /**
```

Ilustración 22 Edición archivo Config.php

En la carpeta de Latch que se copió anteriormente se procede a editar el archivo “LatchConfiguration.php”, en el cual se agregará el ID de la aplicación y el secreto.

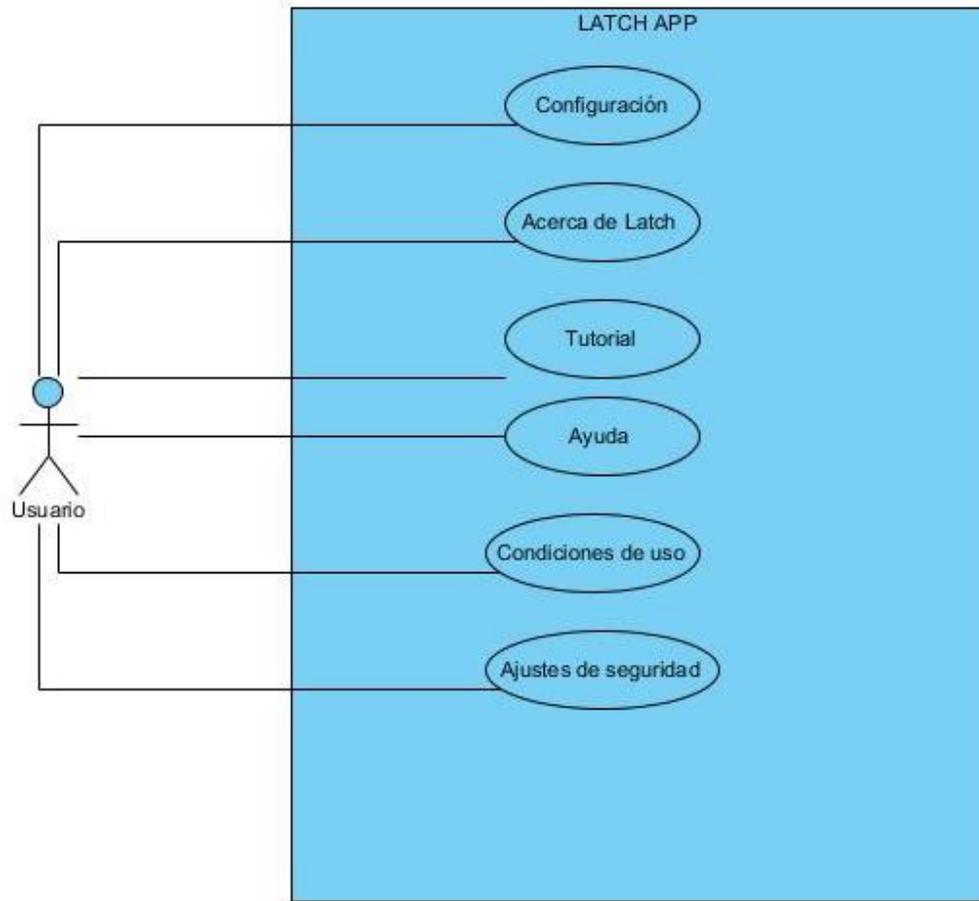
```
*/  
  
class LatchConfiguration {  
    /*  
     * Application ID. To get an application ID go to the developer area  
     * at https://latch.elevenpaths.com.  
     */  
    public static $applicationId = "3eXWrziYeZPZQjYNQqWY";  
  
    /*  
     * Application secret. To get the application secret go to the developer area  
     * at https://latch.elevenpaths.com.  
     */  
    public static $applicationSecret = "ACfhcnHKCmgRyhicPBPvV7mTGdbRjvH9yneNBJBg";  
  
    /*  
     * Host. Latch remote server location (optional).  
     */  
    public static $host = "";  
}
```

**Ilustración 23 LatchConfiguration**

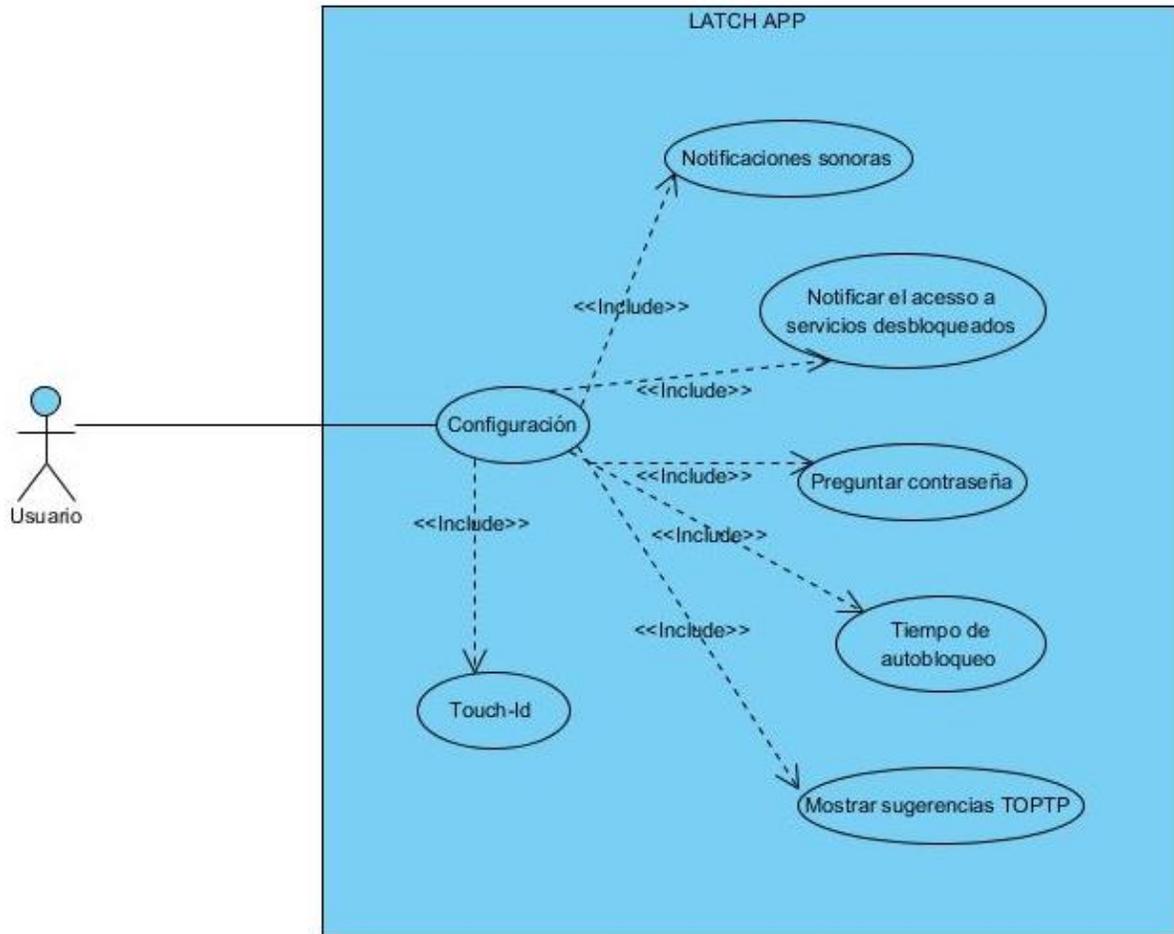
Una vez guardados los cambios en dichos archivos, se inicia sesión en squirrelMail y en la pestaña “Opciones” se muestra el servicio integrado.

### 7.3.5 Casos de Uso

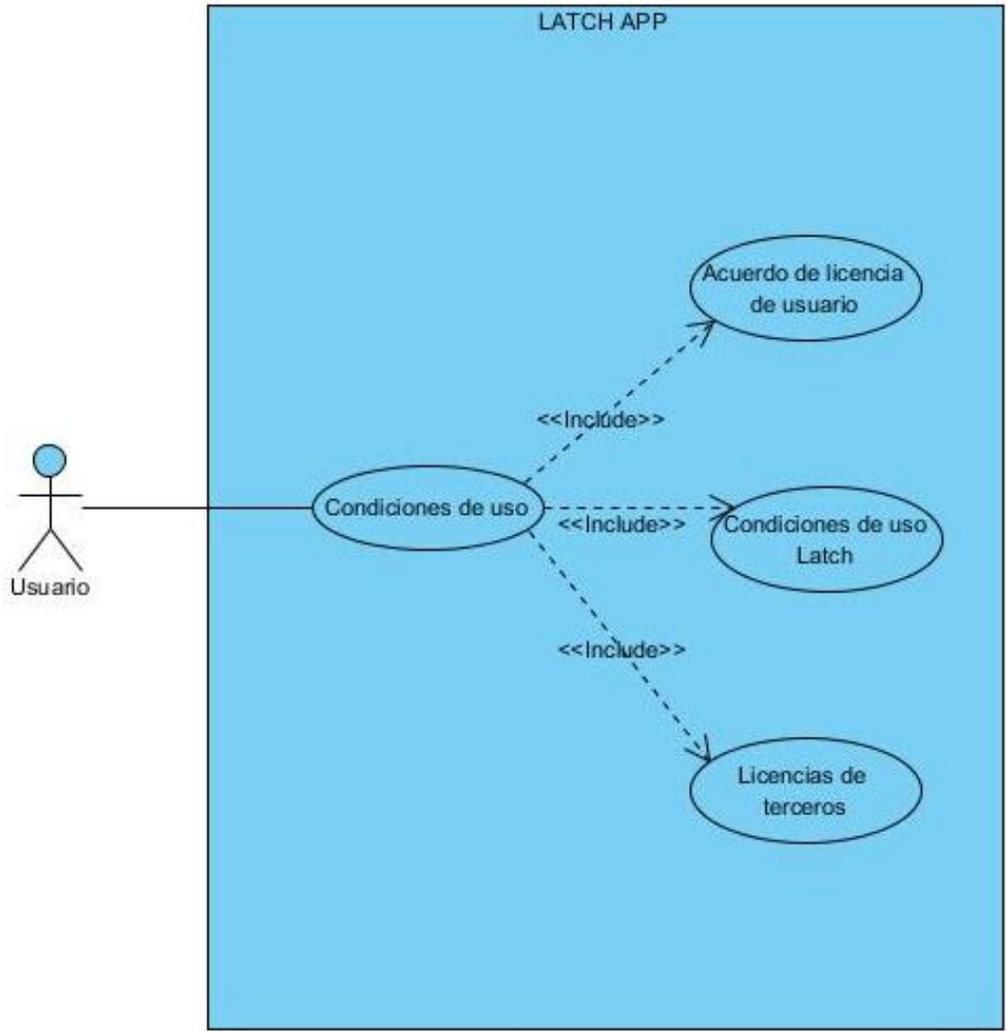
A través de la utilización de casos de uso se muestra de que manera funciona la aplicación y las interacciones de la misma con cada uno de los usuarios.



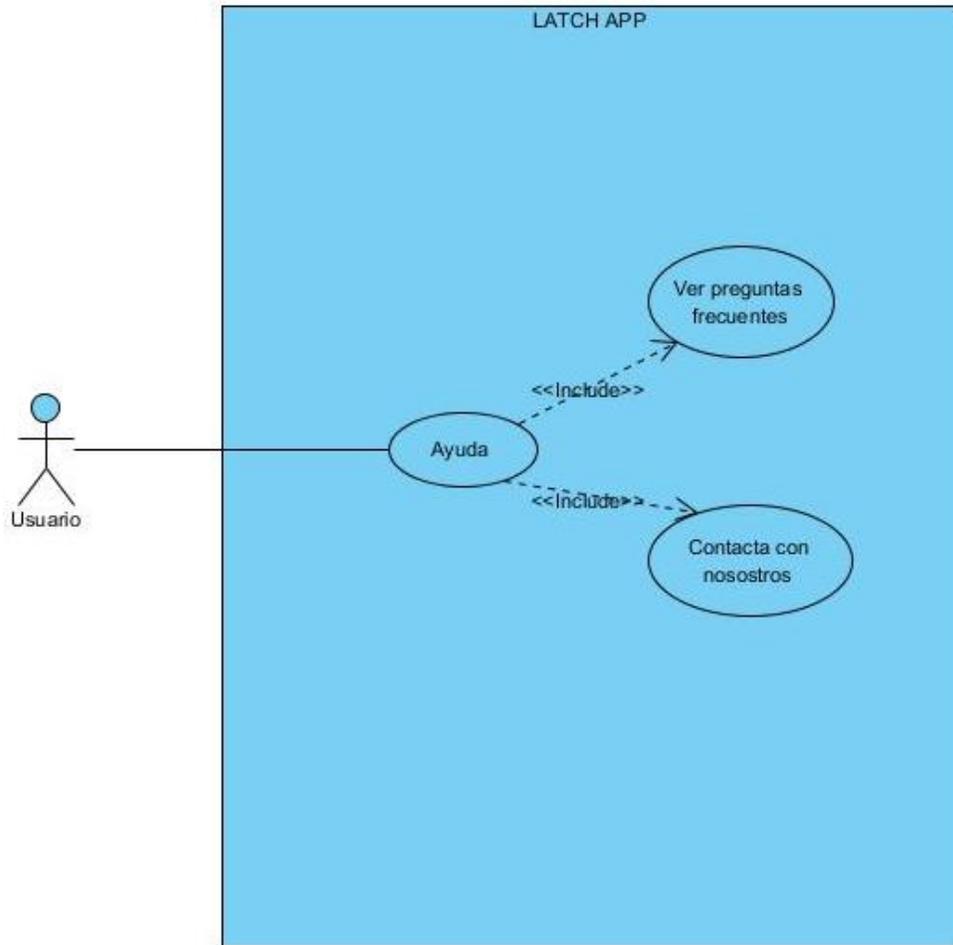
CU 1 Latch



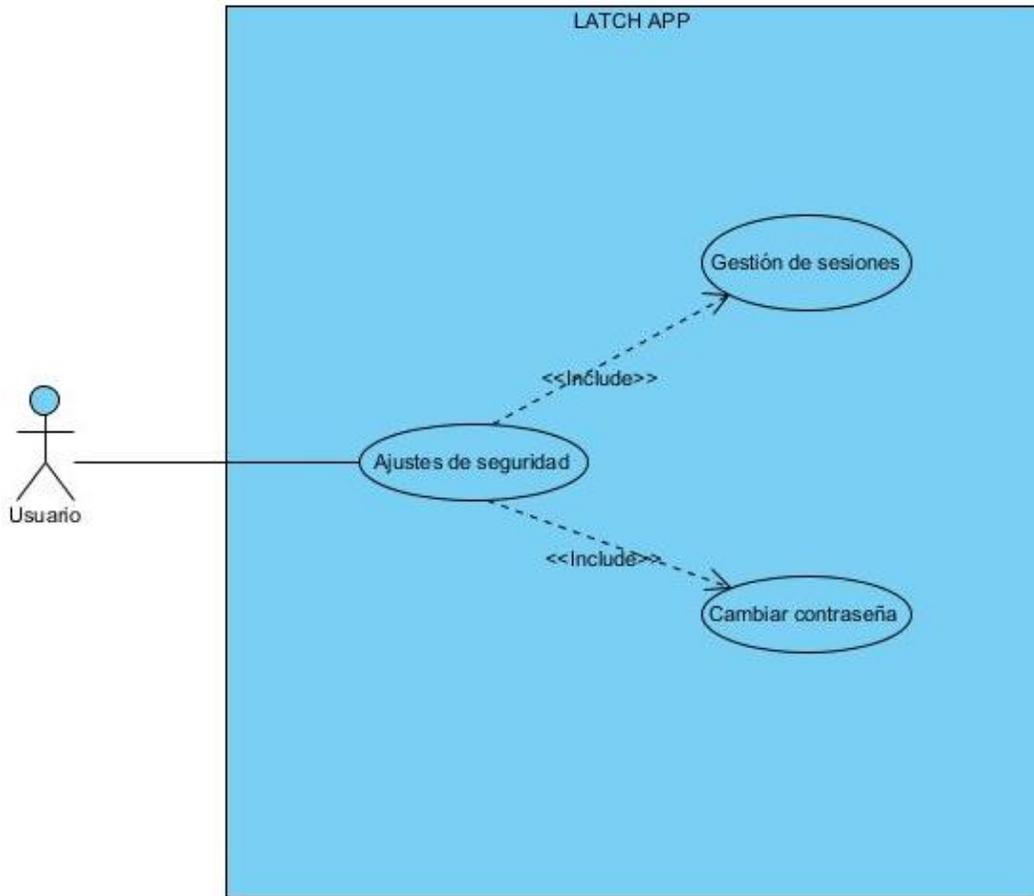
CU 2 Pestaña Configuración



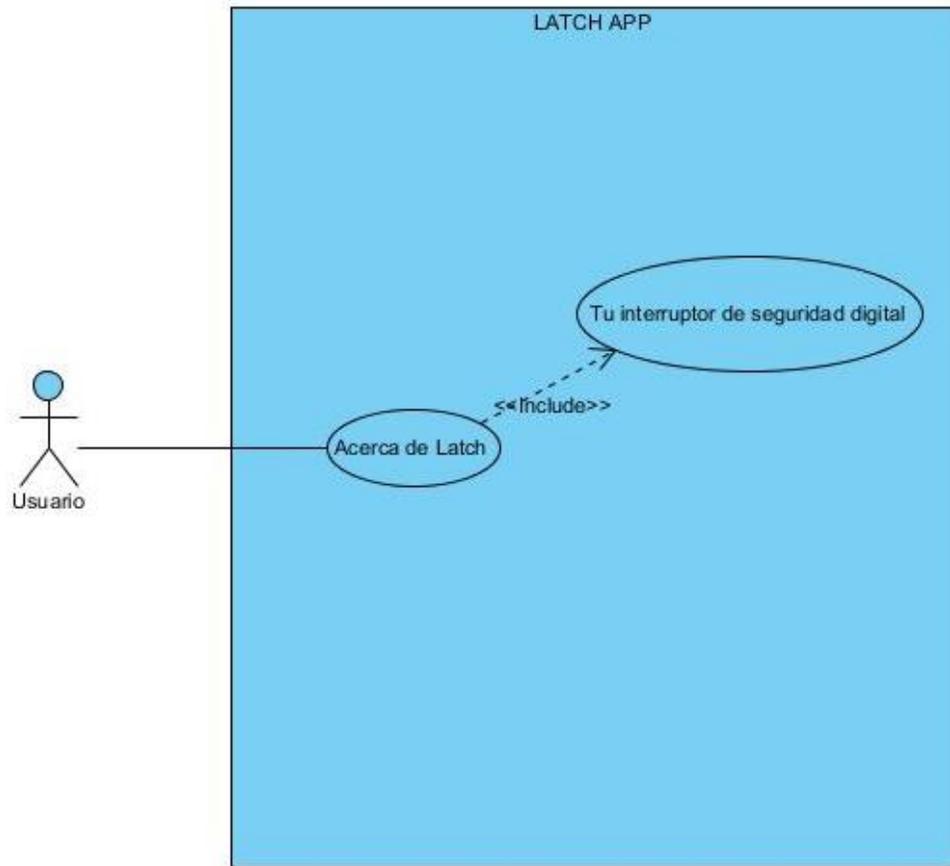
CU 3 Pestaña de Condiciones de Uso



CU 4 Pestaña Ayuda



CU 5 Pestaña Ajuste de Seguridad



CU 6 Pestaña Acerca de Latch

### 7.3.6 Plantilla de Casos Usos

En las plantillas de los casos de usos se muestra la descripción de cada uno de ellos, dichas plantillas están compuesta por los siguientes campos.

ID	CU1
Nombre	Nombre del caso de uso
Autor	Nombre del autor del caso de uso
Fecha	Fecha de creación del caso de uso
Actores	Especificación de los usuarios que interactúan con el caso de uso
Prioridad	Nivel de importancia de la realización del caso de uso
Frecuencia	Regularidad con la que se lleva a cabo el caso de uso
Descripción: Breve explicación del funcionamiento del caso de uso.	
Precondiciones: Establece las condiciones que deben cumplirse para la ejecución del caso de uso.	
Flujo Normal: Listado de las actividades necesarias para el correcto desarrollo del caso de uso.	

Tabla 8 Plantilla de casos de uso

ID	CU1
Nombre	Pestaña configuración
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Alta
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Configuraciones de la aplicación</li> <li>✓ Cambiar contraseñas</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
<p>Flujo Normal:</p> <ul style="list-style-type: none"> <li>✓ El actor configura las notificaciones de la APP</li> <li>✓ Configurar Opciones de acceso</li> <li>✓ Configura opciones de bloqueo</li> </ul>	

**Tabla 9 Configuración**

ID	CU1
Nombre	Notificaciones Sonoras
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
Descripción:	
<ul style="list-style-type: none"> <li>✓ Permite al usuario activar o desactivar las notificaciones de la aplicación</li> </ul>	
Precondiciones:	
<ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
Flujo Normal: El usuario puede activar o desactivar las notificaciones sonoras enviadas por la aplicación.	

**Tabla 10 Notificaciones Sonoras**

ID	CU1
Nombre	Notificaciones de acceso a servicios desbloqueados
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Permite al usuario activar o desactivar las notificaciones acceso a los servicios desbloqueados</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
<p>Flujo Normal:</p> <p>El usuario puede activar o desactivar las notificaciones de acceso a los servicios que no encuentran bloqueados.</p>	

**Tabla 11 Notificaciones de acceso**

ID	CU1
Nombre	Preguntar Contraseña
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Permite al usuario elegir el intervalo de tiempo para que la aplicación solicite la contraseña.</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
<p>Flujo Normal:</p> <p>El usuario puede seleccionar el intervalo de tiempo para que la aplicación solicite la contraseña de acceso o bien mantener la opción desactivada.</p>	

**Tabla 12 Preguntar Contraseña**

ID	CU1
Nombre	Tiempo de bloqueo
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Permite al usuario configurar un tiempo de bloqueo automático de los servicios desbloqueados.</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
<p>Flujo Normal:</p> <p>El usuario puede configurar el tiempo de autobloqueo de los servicios que se encuentran desbloqueados.</p>	

**Tabla 13 Tiempo de bloqueo**

ID	CU1
Nombre	Mostrar sugerencias de TOTP
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Permite al usuario utilizar el servicio de mensajes TOTP para iniciar sesión sin hacer uso de mensajes de texto</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> <li>✓ El servicio debe contar con la opción de mensajes TOTP</li> </ul>	
<p>Flujo Normal:</p> <p>La aplicación brindara al usuario un tokens TOTP el cual será usado después de haber ingresado el usuario y contraseña correspondiente, sin necesidad de esperar dicho código a través de sms.</p>	

**Tabla 14 sugerencias de TOTP**

ID	CU2
Nombre	Condiciones de Uso
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Muestra información de acuerdo de licencias, condiciones de uso y licencias de terceros.</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
<p>Flujo Normal: El usuario puede obtener información legal sobre el uso de la aplicación de Latch.</p>	

**Tabla 15 Condiciones de Uso**

ID	CU2
Nombre	Acuerdo de licencia de usuario
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Baja
Frecuencia	Baja
Descripción:	
<ul style="list-style-type: none"> <li>✓ El usuario puede obtener información legal de la aplicación.</li> </ul>	
Precondiciones:	
<ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
Flujo Normal:	
<p>El Usuario puede descargar el acuerdo de licencia de uso en un documento PDF.</p>	

**Tabla 16 Acuerdo de licencia**

ID	CU2
Nombre	Condiciones de uso
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Muestra al usuario las condiciones de que debe cumplir para hacer uso de aplicación.</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
<p>Flujo Normal:</p> <p>El usuario puede acceder a información importante donde se le brindan las pautas para hacer un buen uso de la aplicación.</p>	

**Tabla 17 Condiciones de uso**

ID	CU2
Nombre	Licencia de terceros
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
Descripción:	
<ul style="list-style-type: none"> <li>✓ Muestras información legal sobre el uso de software de terceros.</li> </ul>	
Precondiciones:	
<ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
Flujo Normal: El usuario puede acceder a la información legal del uso adecuado de software brindado por terceros.	

**Tabla 18 Licencia de terceros**

ID	CU3
Nombre	Pestaña de Ayuda
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Muestra la opción de preguntas frecuentes y el enlace para contactar al equipo de Latch.</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
<p>Flujo Normal: El usuario puede obtener información sobre el uso de la aplicación.</p>	

**Tabla 19 Pestaña Ayuda**

ID	CU3
Nombre	Preguntas frecuentes
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
Descripción:	
<ul style="list-style-type: none"> <li>✓ Brinda información sobre el uso de la herramienta</li> </ul>	
Precondiciones:	
<ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
Flujo Normal:	
<p>El usuario tiene acceso a las preguntas frecuentes realizadas por otros usuarios, las cuales pueden facilitar el uso de la aplicación y de la funcionalidad de la misma.</p>	

**Tabla 20 Preguntas Frecuentes**

ID	CU3
Nombre	Contacta con nosotros
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
<p>Descripción:</p> <ul style="list-style-type: none"> <li>✓ Brinda al usuario los medios para realizar consultas sobre el uso de la aplicación.</li> </ul>	
<p>Precondiciones:</p> <ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
<p>Flujo Normal:</p> <p>El usuario puede contactar al equipo de Latch a través de correo electrónico cuando tenga alguna sobre el uso de la aplicación.</p>	

**Tabla 21 Contacta con nosotros**

ID	CU4
Nombre	Ajuste de seguridad
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
Descripción:	
<ul style="list-style-type: none"> <li>✓ Brinda la opción de gestión de sesiones y cambio de contraseña</li> </ul>	
Precondiciones:	
<ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
Flujo Normal:	
<p>El usuario tiene acceso a la información de los dispositivos donde ha iniciado sesión de latch</p>	

**Tabla 22 Ajustes de Seguridad**

ID	CU4
Nombre	Gestión se sesiones
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
Descripción:	
<ul style="list-style-type: none"> <li>✓ Brinda información de los dispositivos donde se ha iniciado sesión</li> </ul>	
Precondiciones:	
<ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
Flujo Normal:	
<p>El usuario puede obtener información de los últimos dispositivos y de la fecha donde ha iniciado sesión de latch</p>	

**Tabla 23 Gestión se Sesiones**

ID	CU4
Nombre	Cambio de contraseña
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
Descripción:	
<ul style="list-style-type: none"> <li>✓ Brinda la opción para cambiar contraseña</li> </ul>	
Precondiciones:	
<ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
Flujo Normal:	
<p>El usuario puede cambiar la contraseña para acceder a la aplicación cuando el lo requiera.</p>	

**Tabla 24 Cambio de Contraseña**

ID	CU5
Nombre	Acerca de Latch
Autor	Usuario
Fecha	20/08/2018
Actores	Usuario
Prioridad	Media
Frecuencia	Baja
Descripción:	
<ul style="list-style-type: none"> <li>✓ Brinda información de la aplicación</li> </ul>	
Precondiciones:	
<ul style="list-style-type: none"> <li>✓ El usuario debe estar autenticado</li> </ul>	
Flujo Normal:	
<p>El usuario tiene acceso a una breve descripción y de la versión que utiliza actualmente de Latch.</p>	

**Tabla 25 Acerca de Latch**

## 7.4 Fase 4: Capacitación A Usuarios

En esta fase se brinda a los usuarios las herramientas para poder empezar a utilizar Latch. Una de las primeras indicaciones es realizar instalación de la APP en los equipos inteligentes, luego se procede a crear una cuenta de usuario.

Posteriormente que los usuarios creen sus cuentas de Latch e inicien sesión se brindan las indicaciones necesarias para realizar el pareo de los servicios configurados anteriormente.

### 7.4.1 Moodle

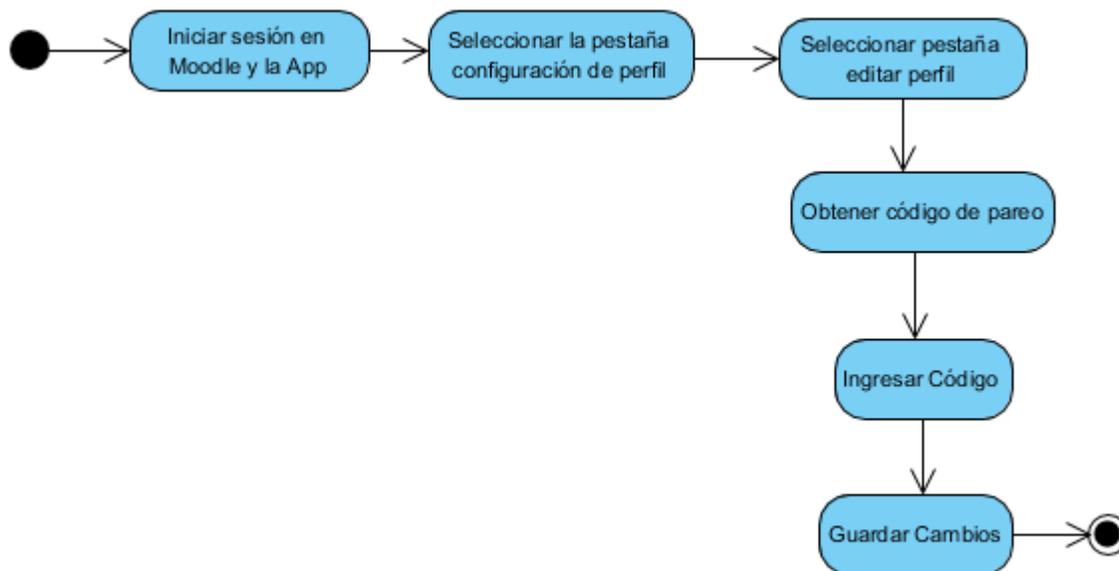
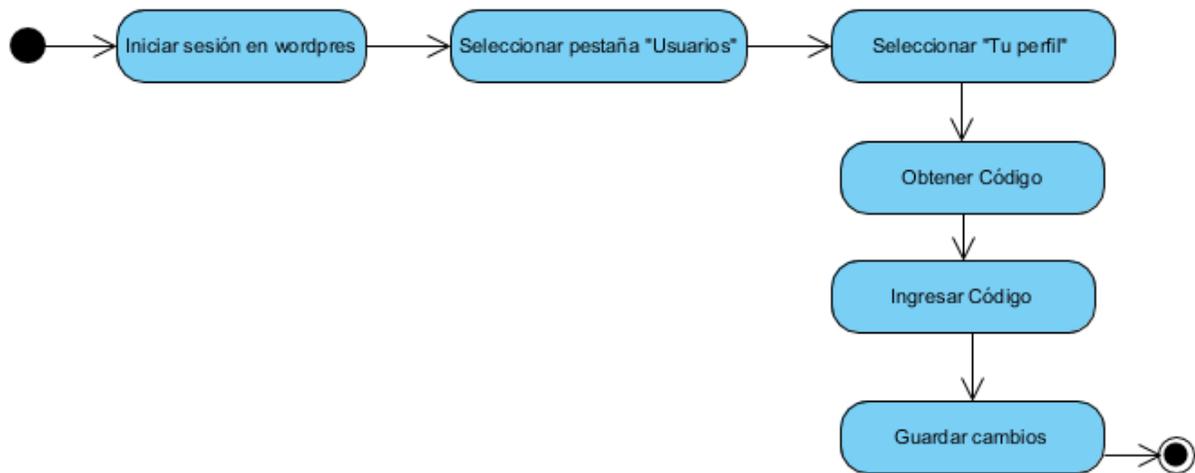


Ilustración 24 Pareo de Latch con Moodle

Para realizar el pareo de Moodle, el usuario debe seleccionar la opción para configurar su perfil en la cual le aparecerá que Latch está activo; se visualiza un cuadro de texto donde deberá ingresar el código que obtuvo desde la aplicación móvil.

## 7.4.2 Wordpress



**Ilustración 25 Pareo de Latch con Wordpress**

Para realizar el pareo de Latch con wordpress, el usuario debe seleccionar la opción para editar su perfil, en la cual se le mostrará un cuadro de texto donde deberá ingresar el código que le brindó la aplicación.

### 7.4.3 Correo

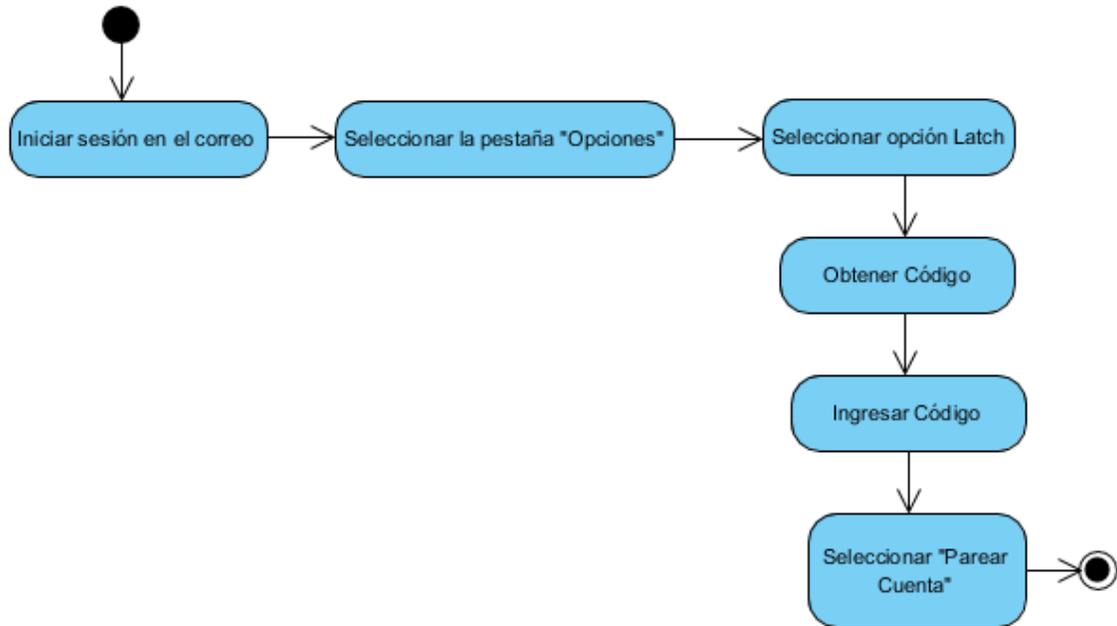


Ilustración 26 Pareo de Latch con SquirrelMail

Para realizar el pareo de Latch con la cuenta de correo el usuario debe dirigirse a la opción de configuración de Latch, donde se le mostrará un cuadro de texto en el que ingresará el código de pareo brindado por la app.

Una vez realizados los pasos anteriores se visualizaran en la aplicación móvil los servicios que el usuario agregó en la configuración antes realizada, desde donde se podrán bloquear y desbloquear cuando el usuario desee.



**Ilustración 27 Servicios Agregados**

#### 7.4.4 Pruebas acceso

Luego de haber añadido Latch a los servicios se realizaron pruebas de inicio de sesión al servicio de correo, con dichas pruebas se logró verificar de qué manera Latch protege las cuentas de los usuarios.

A continuación, se mostrará paso a paso la manera en que realizaron pruebas de acceso al servicio de correo. La prueba acceso se realizó con los datos del usuario creados anteriormente y con el servicio de correo desbloqueados desde la aplicación.

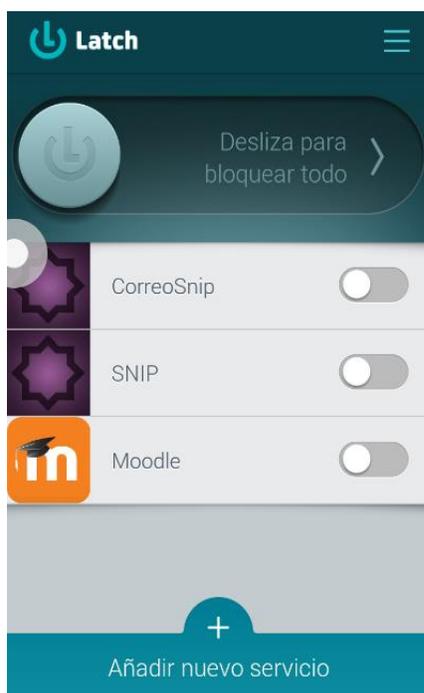


Ilustración 28 Servicios desbloqueados

Como los servicios no se encontraban bloqueados se permite el acceso y únicamente se recibe una notificación de acceso al servicio.



Ilustración 29 Notificación de acceso Correo

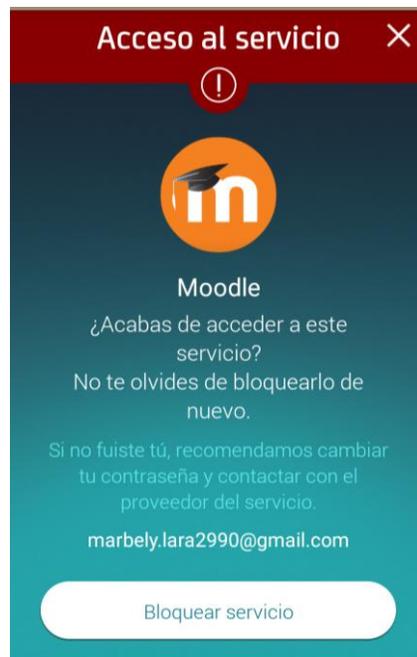


Ilustración 30 Notificación de Acceso Moodle



**Ilustración 31 Notificación de acceso Wordpress**

Luego se bloqueó el servicio en la aplicación y se intentó nuevamente ingresar al correo.



**Ilustración 32 Servicios bloqueados**

En esta ocasión no se permitió el acceso y se recibió una notificación en el móvil.



Ilustración 33 Notificación de acceso Correo



Ilustración 34 Notificación de acceso Moodle



**Ilustración 35** Notificación de acceso Wordpress

## **VIII. CONCLUSIONES**

La implementación de este trabajo monográfico permite garantizar seguridad a los servicios de aula virtual y correo electrónico con los que cuenta el SNIP. Gracias a dicha implementación, se determinó que con el uso de Latch los riesgos de ataque dirigidos a los servicios de la institución son mínimos, puesto que los usuarios estarán alertados ante cualquier intento de acceso no autorizado en sus equipos inteligentes y ante esta situación poder realizar bloqueo o desbloqueo a las aplicaciones agregadas al momento de configurar Latch.

Con la ejecución de pruebas de intrusión, se observó el nivel de seguridad con el que contarán los usuarios que utilicen la aplicación, haciendo uso de herramientas que intentan obtener acceso a los servicios en modo no autorizado.

Por lo que se concluye, que al usar Latch como segundo factor de Autenticación se protege información sensible con la que cuentan los usuarios de los servicios del SNIP.

## **IX. RECOMENDACIONES**

Si en algún momento la institución desea poner en marcha la propuesta presentada anteriormente, se recomienda que la institución brinde un teléfono móvil exclusivo para el uso de la herramienta y evitar que el usuario utilice su teléfono personal.

Además, es necesario que los usuarios mantengan actualizada la aplicación y que los administradores se mantengan informados de las nuevas actualizaciones de los Plugins instalados en los servicios.

## X. GLOSARIO

1. Elevenpaths: Empresa dedica a la creación de productos para solucionar problemas de seguridad
2. Fortigate: Sistema de seguridad desarrollado por Fortinet, software libre y funciona como detector de amenazas.
3. Identidades digitales: El conjunto de la información sobre un individuo o una organización expuesta en Internet.
4. IMAP: *Internet Message Access Protocol*. (Protocolo de acceso a mensajes de internet). Este sistema permite a nuestro programa de correo electrónico conectarse a nuestra cuenta de correo electrónico y visualizar los mensajes allí almacenados.
5. LAMP: (*Linux, Apache, MySql y PHP*). Plataforma para el desarrollo y ejecución de aplicaciones web de alta performance.
6. Moodle: *Modular Object-Oriented Dynamic Learning Environment*. (Entorno de Aprendizaje Dinámico Modular, Orientado a Objetos). Moodle es un Software diseñado para crear cursos en línea y entornos de aprendizajes virtuales.
7. SMTP: *Simple Mail Transfer Protocol*. (Protocolo de transferencia de correo simple). procedimiento que permite el transporte del email en la Internet.
8. Securizados: hacer que un ordenador o una operación realizada por internet sean seguros.

## XI. BIBLIOGRAFÍA

After Logic. (2015). After Logic WebMail Lite. Agosto 2015, de After Logic Corp Sitio web: <http://www.afterlogic.org/webmail-lite>

Alberto Castro Gallardo. (2015). Doble autenticación: actívala en Google, Facebook y Dropbox. Junio 2015, de PActual Sitio web: [http://www.pactual.com/articulo/zona\\_practica/paso\\_a\\_paso/paso\\_a\\_paso\\_internet/13237/doble\\_autenticacion\\_activala\\_google\\_facebook\\_dropbox.html](http://www.pactual.com/articulo/zona_practica/paso_a_paso/paso_a_paso_internet/13237/doble_autenticacion_activala_google_facebook_dropbox.html)

Álvarez Oliva, Alberto. (2013). Seguridad en Redes y Sistemas, Detección de Intrusiones con SNORT. Junio, 2015, de Universidad Oberta de Catalunya <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/22909/5/lalvarezoTFM0613memoria.pdf>

Delivery Tech. (2015). Qué es un servidor SMTP. Septiembre, de Turbo SMTP Sitio web: <http://www.serversmtp.com/es/que-es-servidor-smtp>

DIMAGIN Web development. (2015). Tecnología LAMP. Agosto 2015, de DIMAGIN Sitio web: [http://www.dimagin.net/es/tec\\_lamp.php](http://www.dimagin.net/es/tec_lamp.php)

Fred Kerby. (Noviembre 2012). Autenticación de dos factores. Agosto 2015, de Programa Securing The Human de SANS Sitio web: [https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201211\\_sp.pdf](https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201211_sp.pdf)

Guía para Usuarios: identidad digital y reputación online. Recuperado el 12 de Marzo de 2015, de INTECO

HSBC Argentina. (2015). e-Token | Dispositivo de Seguridad. Agosto 2015, de HSBC Sitio web: <http://www.hsbc.com.ar/minisitios/pc-banking/eToken.asp>

ISECOM. (2003). Manual de Metodologías Abiertas de testeo de seguridad. Septiembre 2016, de ISECOM Sitio web: [http://www.isecom.org/press/hispasec\\_nov24\\_2003.htm](http://www.isecom.org/press/hispasec_nov24_2003.htm)

Jose Kont. (Junio 2015). V Estudio de redes sociales, Centroamérica y el Caribe. Septiembre 2015, de iLifebelt Sitio web: <http://blog.internacionaldemarketing.com/wp-content/uploads/2015/07/Estudio-iLifebelt2015-1.2.pdf>

José Manuel García. *La ética como asignatura en los estudios de informática.* Septiembre 2015, Universidad de Murcia.

Jorge Mieres. (Enero 2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas. Septiembre 2016, de evilfingers Sitio web: [https://www.evilfingers.com/publications/white\\_AR/01\\_Atques\\_informaticos.pdf](https://www.evilfingers.com/publications/white_AR/01_Atques_informaticos.pdf)

Moodle. (2015). Acerca de Moodle. Septiembre 2015, de Moodle Sitio web: [https://docs.moodle.org/all/es/Acerca\\_de\\_Moodle](https://docs.moodle.org/all/es/Acerca_de_Moodle)

Sistema nacional de inversión pública de Nicaragua. <http://www.snip.gob.ni/snip>

Servicio de Informática. (2015). Configurar IMAP. Septiembre 2015, de Universidad de Cantabria Sitio web: [https://sdei.unican.es/Paginas/servicios/correo/manual\\_imap.aspx](https://sdei.unican.es/Paginas/servicios/correo/manual_imap.aspx)

Soft Tokens. <http://www.hidglobal.mx/products/cards-and-credentials/activid/soft-tokens>

Telefónica. (Junio 2013). Telefónica lanza “Eleven Paths”, una nueva compañía de seguridad digital. Septiembre 2015, de Telefónica Sitio web: [http://saladeprensa.telefonica.es/documentos/nprensa/NdP\\_11Paths\\_Final.pdf](http://saladeprensa.telefonica.es/documentos/nprensa/NdP_11Paths_Final.pdf)

## XII. ANEXOS

### 12.1 Integración de Latch en Moodle

#### 12.1.1 Paso 1: Crear aplicación en Latch

Para realizar la instalación del Plugins de Latch se hace desde la página oficial de Latch, desde la cual se creará una nueva aplicación indicando el nombre que se desea aparezca en la aplicación móvil del usuario.

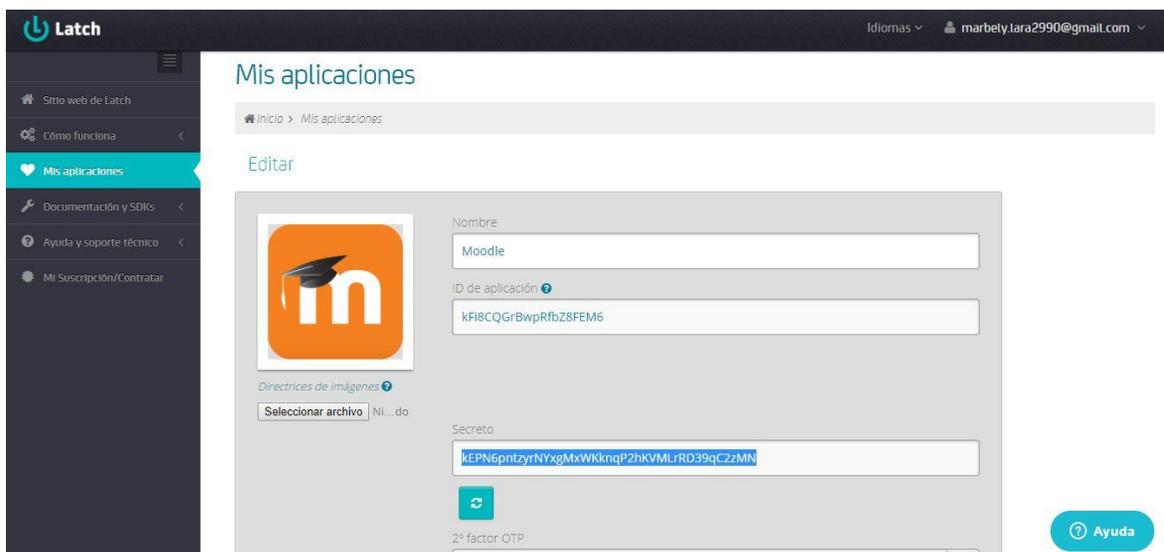


Ilustración 36 Creación de aplicación Moodle

## 12.1.2 Paso 2: Descargar y añadir Plugins

Después de haber añadido a aplicación, se descargó la carpeta del Plugins desde la página oficial de Latch, la cual se copió en la carpeta de instalación de Moodle.

Este equipo > OS (C:) > wamp > www > moodle

Nombre	Fecha de modifica...	Tipo	Tamaño
admin	10/07/2017 13:05	Carpeta de archivos	
auth	10/07/2017 15:08	Carpeta de archivos	
error	10/07/2017 13:05	Carpeta de archivos	
files	10/07/2017 13:05	Carpeta de archivos	
filter	10/07/2017 13:05	Carpeta de archivos	
grade	10/07/2017 13:05	Carpeta de archivos	
group	10/07/2017 13:05	Carpeta de archivos	
install	10/07/2017 13:05	Carpeta de archivos	
iplookup	10/07/2017 13:06	Carpeta de archivos	
lang	10/07/2017 13:06	Carpeta de archivos	
lib	10/07/2017 15:08	Carpeta de archivos	
user	10/07/2017 13:07	Carpeta de archivos	
userpix	10/07/2017 13:07	Carpeta de archivos	
webservice	10/07/2017 13:07	Carpeta de archivos	
.jshintrc	13/07/2014 1:10	Archivo JSHINTRC	2 KB
.shifter	13/07/2014 1:10	JSON File	1 KB
behat.yml.dist	13/07/2014 1:10	Archivo DIST	1 KB
brokenfile	13/07/2014 1:10	Archivo PHP	2 KB
composer	13/07/2014 1:10	JSON File	1 KB
config	28/09/2017 12:44	Archivo PHP	1 KB
config-dist	13/07/2014 1:10	Archivo PHP	37 KB
COPYING	13/07/2014 1:10	Documento de tex...	35 KB
drafffile	13/07/2014 1:10	Archivo PHP	3 KB
file	13/07/2014 1:10	Archivo DHD	4 KB

0 ítems seleccionados

Ilustración 37 Archivos De Latch

Luego se inició sesión como administrador en Moodle donde apareció la opción de instalación de Latch. Click en “Actualizar bases de datos Moodle ahora”.

## Comprobación de 'plugins'

Esta página muestra las extensiones (plugins) que pueden requerir su atención durante la actualización. Los elementos resaltados incluyen nuevas extensiones (plugins) que están a punto de ser instalados, los que van a ser actualizados y las extensiones anteriores que ahora faltan. Los módulos externos (add-ons) también se destacan. Se recomienda que compruebe si hay versiones más recientes de los módulos externos disponibles y actualice su código fuente antes de continuar con esta actualización de Moodle.

Compruebe actualizaciones disponibles

Última comprobación realizada el 10 de julio de 2017, 19:59

### Número de extensiones (plugins) que requieren atención durante esta actualización: 2

Mostrar la lista completa de extensiones (plugins) instalados

Nombre de la extensión	Directorio	Origen	Versión actual	Nueva versión	Requiere	Estado
<b>Extensiones de identificación</b>						
latch		Adicional	2014030600			Ausente del disco
<b>Tipos de campos de perfiles</b>						
latch		Adicional	2014030600			Ausente del disco

Recargar

Actualizar base de datos Moodle ahora

Ilustración 38 Comprobación de plugins

## Actualizando la versión

### auth\_latch

Éxito

### profilefield\_latch

Éxito

Continuar

Ilustración 39 Plugins actualizados

Una vez realizada la actualización de la base de datos, seleccionar la pestaña **Herramientas** luego en la pestaña de Plugins seleccionar la opción **Autenticación** y luego en **gestionar identificación** deberá aparecer el Plugins de Latch habilitado.

Nombre	Usuarios	Habilitar	Arriba/Abajo	Configuración	Configuración del test	Desinstalar
Cuentas manuales	2			Configuración		
No hay sesión	0			Configuración		
Identificación basada en Email	0		↓	Configuración		Desinstalar
Latch	0		↑	Configuración		Desinstalar
Usar un servidor CAS (SSO)	0			Configuración		Desinstalar
Usar una base de datos externa	0			Configuración	Configuración del test	Desinstalar
Usar servidor FirstClass	0			Configuración		Desinstalar
Usar un servidor IMAP	0			Configuración		Desinstalar
Usar un servidor LDAP	0			Configuración		
Identificación de la Red Moodle (*Moodle Network*)	0			Configuración		
Usar un servidor NNTP	0			Configuración		Desinstalar
Sin identificación	0			Configuración		Desinstalar
PAM (Pluggable Authentication Modules)	0			Configuración		Desinstalar
Servidor POP3	0			Configuración		Desinstalar
Usar un servidor RADIUS	0			Configuración		Desinstalar

**Ilustración 40 Activación de Plugins**

Luego en Moodle seleccionar “**configuración**”, después la opción “**Latch**”, donde se debe colocar el ID de la aplicación y el secreto, los cuales fueron obtenido en el primer paso como se mostró en la ilustración “”.

**Sistema Nacional de Inversión Pública**

Página Principal > Administración del sitio > Extensiones > Autenticación > Latch

Activar la edición de bloques

**NAVEGACIÓN**

- Página Principal
- Área personal
- Páginas del sitio
- Mi perfil
- Cursos

**MARCAS DEL ADMINISTRADOR**

Marcar esta página

**ADMINISTRACIÓN**

- Ajustes de mi perfil
- Administración del sitio
  - Notificaciones
  - Registro
  - Opciones avanzadas

**Latch**

Plugin de integración del servicio Latch

Introduce aquí tu Application ID y secreto. Si no tienes unos, por favor visita nuestra web

App ID:

App Secret:

Guardar cambios

**Ilustración 41 Ingreso de ID y Secreto**

## 12.2 Integrar Latch en Wordpress

### 12.2.1 Paso 1: Crear aplicación en Latch

Como se indicó anteriormente en la instalación de Latch para Moodle, el primer paso que se realizó fue crear una aplicación en la página de Latch para obtener el ID y secreto.

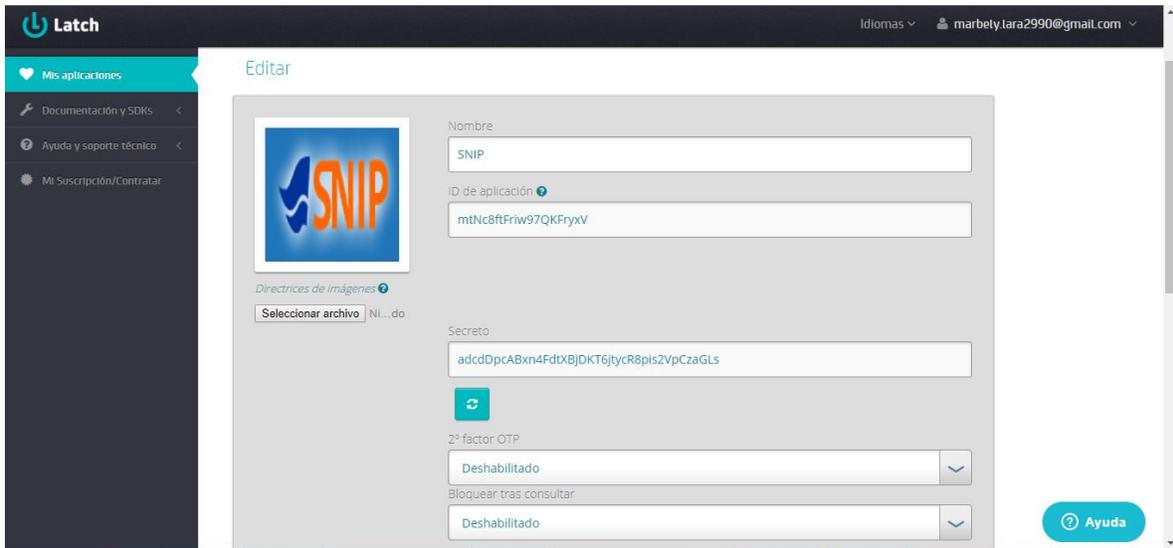


Ilustración 42 Creación de aplicación Wordpress

## 12.2.2 Paso 2: Añadir Plugins

La versión instalada de wordpress ya cuenta con el Plugins de Latch para ser instalado, para ello se seleccionó la pestaña de Plugins, buscamos el Plugins de Latch y se procedió con la instalación del mismo.



Ilustración 43 Búsqueda de Plugins

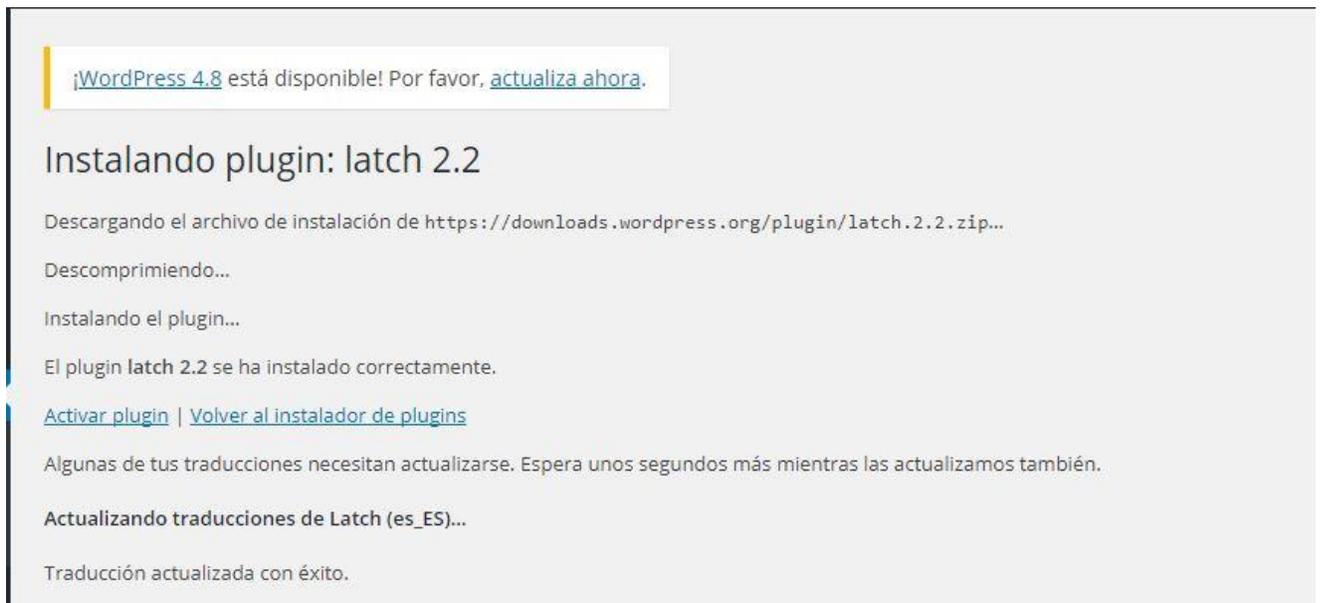
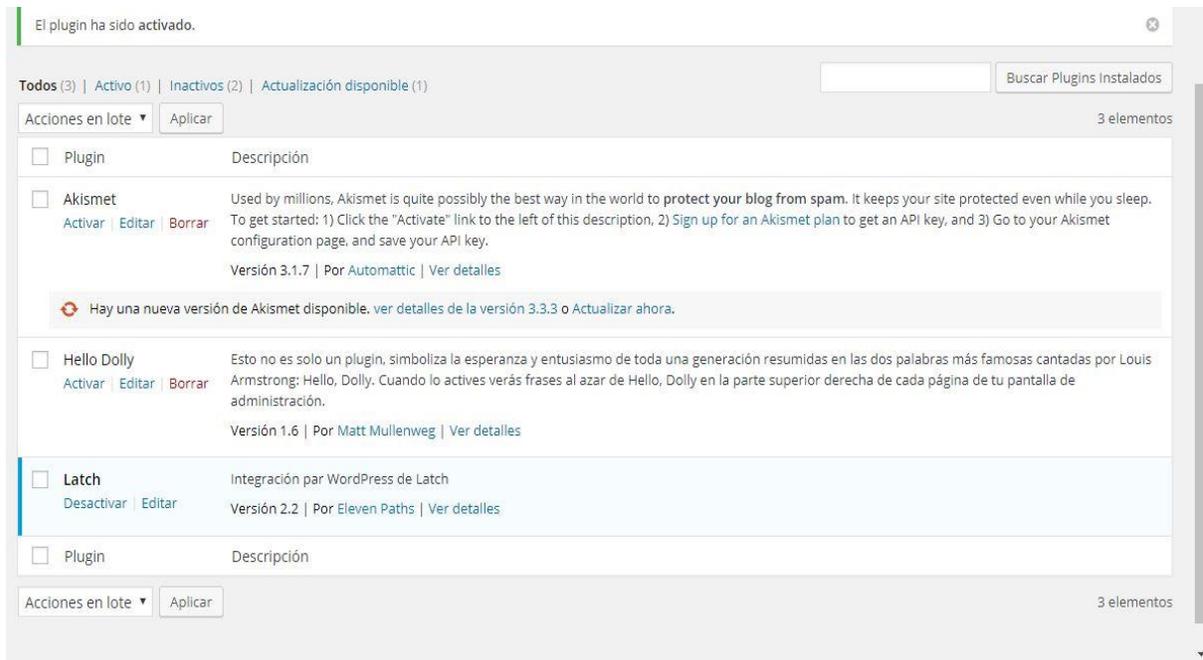
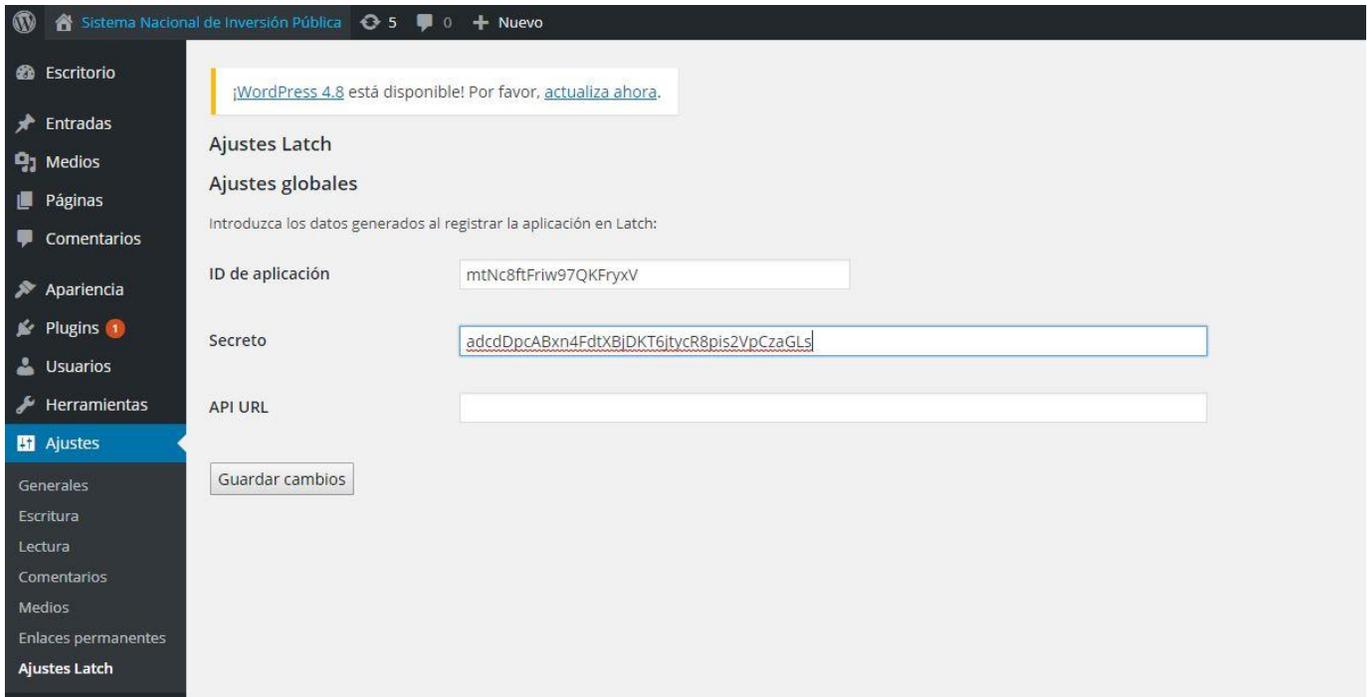


Ilustración 44 Descarga e instalación de plugins



**Ilustración 45 Comprobación de plugins instalado**

Luego de que el plugin se encuentre activo se procedió a ingresar el ID de la aplicación y código secreto, dicha información es obtenida desde la página de Latch.

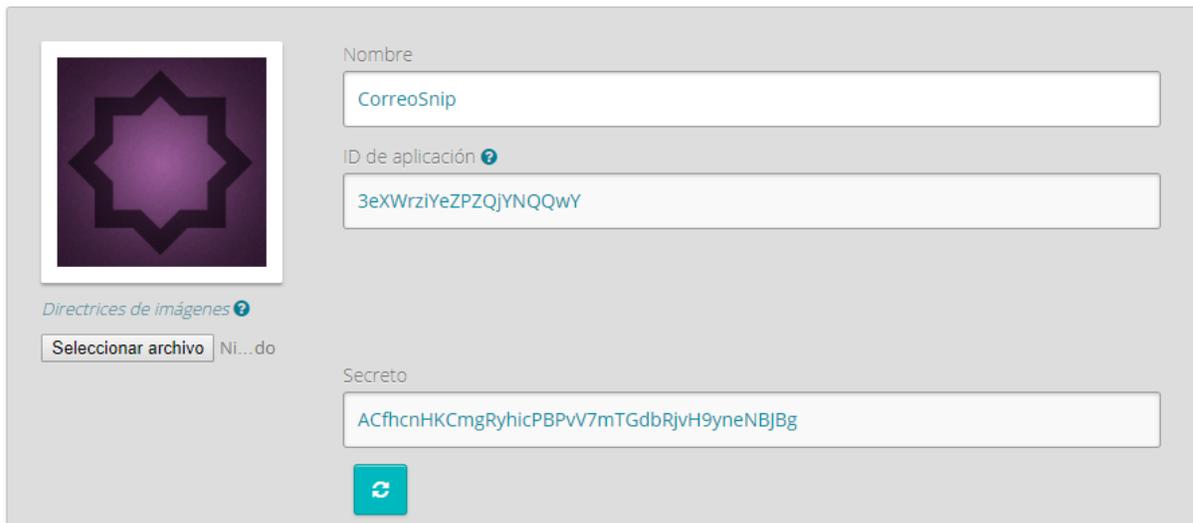


**Ilustración 46 Ingreso de ID y Secreto**

## 12.3 Integrar Latch en SquirrelMail

### 12.3.1 Paso 1: Crear aplicación en Latch

Como se indicó en los servicios anteriores, el primer paso que se realizó fue la creación de la aplicación del servicio de correo.



Nombre

CorreoSnip

ID de aplicación ?

3eXWrziYeZPZQjYNQQwY

Directrices de imágenes ?

Seleccionar archivo Ni...do

Secreto

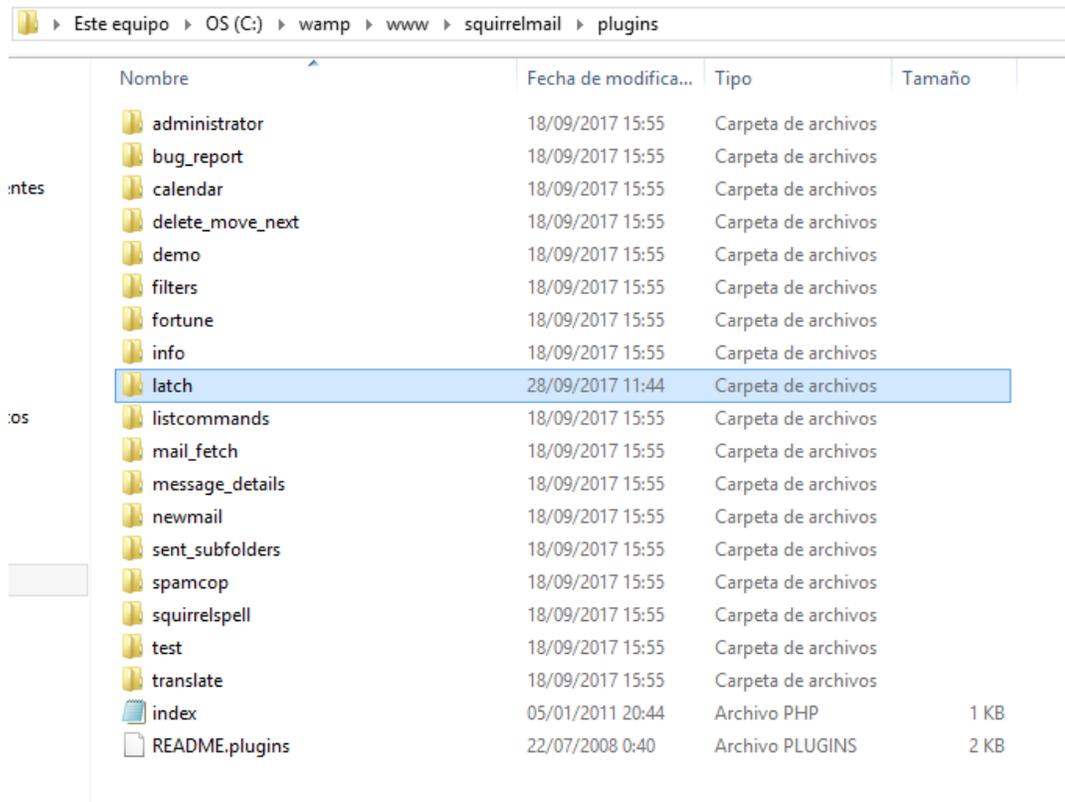
ACfhnHKCmgRyhicPBPw7mTGdbRjvH9yneNBJBg



Ilustración 47 Creación de aplicación Correo

### 12.3.2 Paso 2: Integrar Latch

Una vez que se creó la aplicación se procedió a descargar el Plugins de latch para el servidor de correo SquirrelMail, el cual se añadió la carpeta **Plugins** que se encuentra en la carpeta de instalación de squirrelMail:



The screenshot shows a Windows File Explorer window with the address bar displaying the path: Este equipo > OS (C:) > wamp > www > squirrelmail > plugins. The main area shows a list of files and folders. The 'latch' folder is highlighted in blue. The list includes folders like administrator, bug\_report, calendar, delete\_move\_next, demo, filters, fortune, info, latch, listcommands, mail\_fetch, message\_details, newmail, sent\_subfolders, spamcop, squirreldspell, test, translate, and files like index and README.plugins.

Nombre	Fecha de modifica...	Tipo	Tamaño
administrator	18/09/2017 15:55	Carpeta de archivos	
bug_report	18/09/2017 15:55	Carpeta de archivos	
calendar	18/09/2017 15:55	Carpeta de archivos	
delete_move_next	18/09/2017 15:55	Carpeta de archivos	
demo	18/09/2017 15:55	Carpeta de archivos	
filters	18/09/2017 15:55	Carpeta de archivos	
fortune	18/09/2017 15:55	Carpeta de archivos	
info	18/09/2017 15:55	Carpeta de archivos	
<b>latch</b>	28/09/2017 11:44	Carpeta de archivos	
listcommands	18/09/2017 15:55	Carpeta de archivos	
mail_fetch	18/09/2017 15:55	Carpeta de archivos	
message_details	18/09/2017 15:55	Carpeta de archivos	
newmail	18/09/2017 15:55	Carpeta de archivos	
sent_subfolders	18/09/2017 15:55	Carpeta de archivos	
spamcop	18/09/2017 15:55	Carpeta de archivos	
squirreldspell	18/09/2017 15:55	Carpeta de archivos	
test	18/09/2017 15:55	Carpeta de archivos	
translate	18/09/2017 15:55	Carpeta de archivos	
index	05/01/2011 20:44	Archivo PHP	1 KB
README.plugins	22/07/2008 0:40	Archivo PLUGINS	2 KB

Ilustración 48 Archivos de instalación latch

Luego de haber copiado la carpeta del plugin de latch, se procedió a editar el archivo config.php en donde se activa la variable correspondiente al Plugins de Latch.

Este equipo > OS (C:) > wamp > www > squirrelmail > config

Nombre	Fecha de modifica...	Tipo	Tamaño
 .htaccess	26/03/2009 16:26	Archivo HTACCESS	1 KB
 conf	03/05/2011 1:46	Archivo PL	156 KB
 config	11/06/2018 23:29	Archivo PHP	31 KB
 config_local	05/01/2011 20:44	Archivo PHP	1 KB
 index	05/01/2011 20:44	Archivo PHP	1 KB

Ilustración 49 Ubicación archivo Config.php

```
925 $abook_file_line_length = 2048;
926
927 /**
928  * MOTD
929  *
930  * This is a message that is displayed immediately after a user logs in.
931  * @global string $motd
932  */
933 $motd = "";
934
935
936 /**
937  * To install plugins, just add elements to this array that have
938  * the plugin directory name relative to the /plugins/ directory.
939  * For instance, for the 'squirrelspell' plugin, you'd put a line like
940  * the following.
941  *   $plugins[0] = 'squirrelspell';
942  *   $plugins[1] = 'listcommands';
943  */
944 $plugins[] = 'latch';
945
946 // Add list of enabled plugins here
947 |
948
949 /*** Database ***/
950 /**
```

Ilustración 50 Edición archivo config.php

Una vez activado el Plugins se procedió a editar el archivo latchConfiguration.php en el que agrego el ID aplicación y el secreto correspondientes.

Este equipo > OS (C:) > wamp > www > squirrelmail > plugins > latch

Nombre	Fecha de modifica...	Tipo	Tamaño
sdk	28/09/2017 11:35	Carpeta de archivos	
<b>latchConfiguration</b>	28/09/2017 11:44	Archivo PHP	2 KB
latchOperations	22/08/2014 3:41	Archivo PHP	4 KB
LICENSE	22/08/2014 3:41	Documento de tex...	27 KB
options	22/08/2014 3:41	Archivo PHP	3 KB
pairingForm	22/08/2014 3:41	Archivo PHP	4 KB
setup	22/08/2014 3:41	Archivo PHP	3 KB
symbol	22/08/2014 3:41	Imagen PNG	2 KB
twoFactorForm	22/08/2014 3:41	Archivo PHP	3 KB

Ilustración 51 Ubicación archivo LatchConfig

```
*/  
  
class LatchConfiguration {  
    /*  
     * Application ID. To get an application ID go to the developer area  
     * at https://latch.elevenpaths.com.  
     */  
    public static $applicationId = "3eXWrziYeZPZQjYNQQwY";  
  
    /*  
     * Application secret. To get the application secret go to the developer area  
     * at https://latch.elevenpaths.com.  
     */  
    public static $applicationSecret = "ACfhcnHKCmgRyhicPBPvV7mTGdbRjvH9yneNBjBg";  
  
    /*  
     * Host. Latch remote server location (optional).  
     */  
    public static $host = "";  
}
```

Ilustración 52 Edición archivo LatchCofiguration.php

## 12.4 Añadir un servicio en la aplicación de latch

Para llevar a cabo este proceso el usuario deberá descargar la aplicación de latch disponible en play store y **App Store**, Luego deberá crear una cuenta de usuario.

Para agregar un nuevo servicio en la aplicación móvil el usuario deberá iniciar sesión cada uno de los servicio (MOODLE, WORDPRESS o Correo) y en la aplicación de latch.

Desde la aplicación móvil seleccionamos la opción “Generar Código”



**Ilustración 53 Generar Código**

Nota: La aplicación brindara un código, el cual será válido por 60 segundos, pasado ese tiempo el código será inválido y se debe generar un nuevo código. El Usuario debe generar un código diferente para cada servicio.

## Wordpress

Para realizar el pareo de la cuenta de wordpress el usuario debe seleccionar la pestaña de “Usuario”, luego “Tu Perfil” donde el usuario deberá ingresar el código generado por la App.

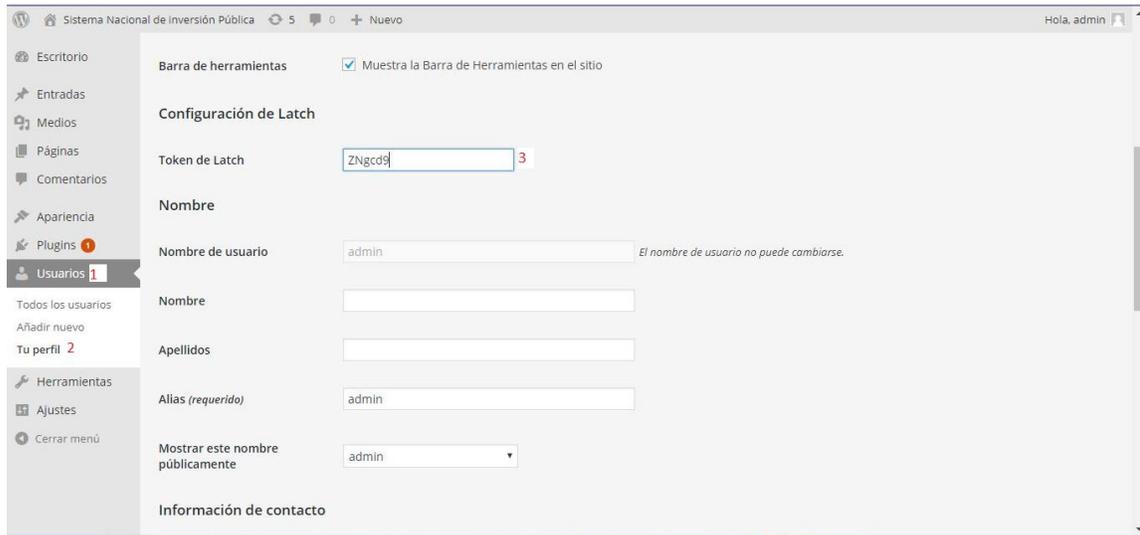


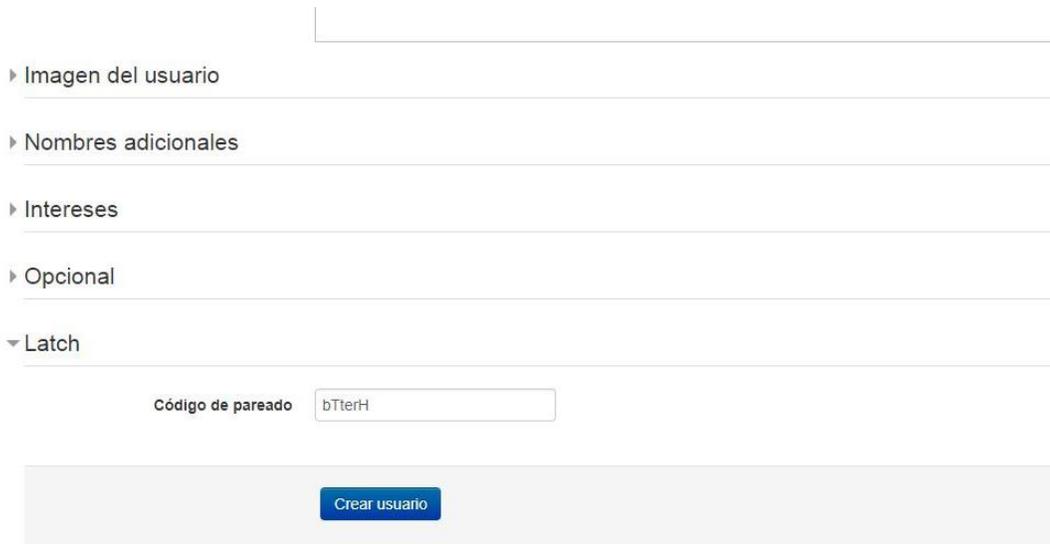
Ilustración 54 Ingreso de Token



Ilustración 55 Notificación de servicio Agregado

## Moodle

Para agregar el servicio de Moodle el usuario debe seleccionar la pestaña de configuración de perfil y seleccionar la opción de editar perfil, al final del formulario le mostrara la opción de Latch en donde debe introducir el código generado por la aplicación.



The screenshot shows a user profile configuration form with several sections: 'Imagen del usuario', 'Nombres adicionales', 'Intereses', 'Opcional', and 'Latch'. The 'Latch' section is expanded, showing a 'Código de pareado' (Pairing Code) field with the value 'bTterH' and a 'Crear usuario' (Create user) button.

Ilustración 56 Ingreso de Token en Moodle

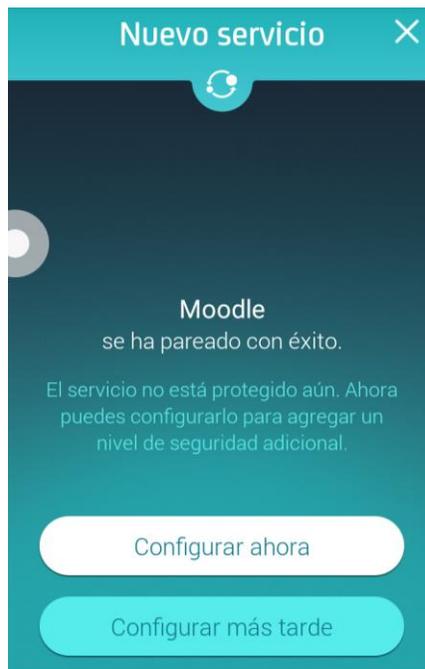


Ilustración 57 Notificación se servicio pareado

## Correo

Para realizar el pareo del servicio de correo el usuario debe seleccionar la pestaña de Opciones.

Luego la opción de la **Latch Settings**, donde ingresar el código generado por Latch y luego dar click en el botón **“Pair account”**.

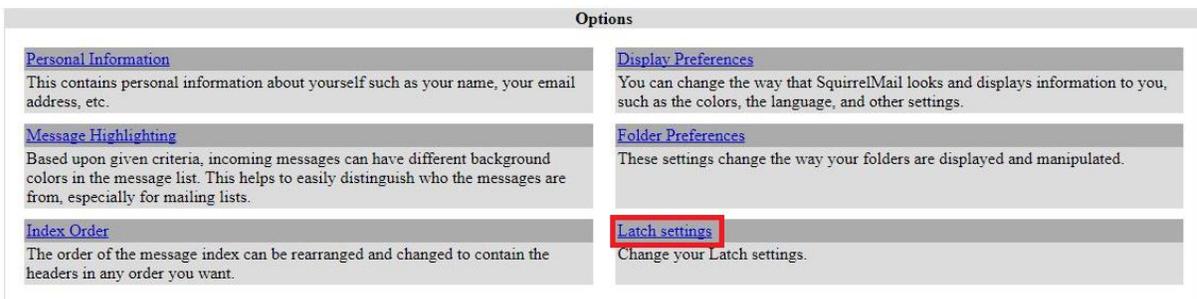


Ilustración 58 Opción para configurar Latch

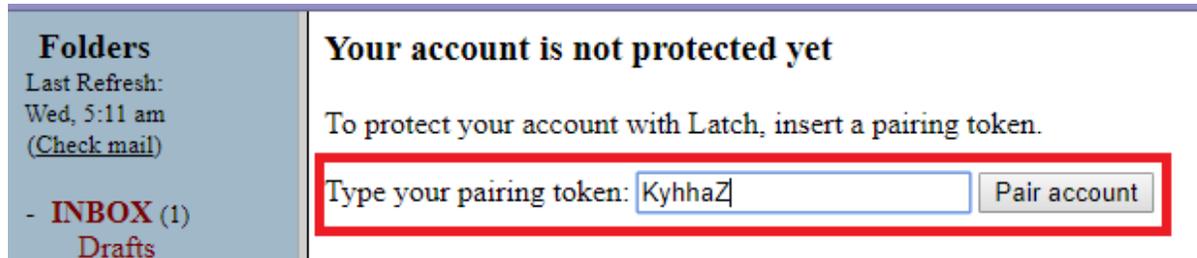


Ilustración 60 Ingreso de Token



Ilustración 59 Notificación de servicio Pareado