**LETRA ESCARLATA**

Autores: @cartesv (En busca de colaboradores en el diseño y la validación del proyecto.)

Agradecimientos: @pabloacastillo, @GisseJo, @markimeyer

Asunción, Paraguay.

*Un mecanismo colaborativo para el etiquetado y la alerta de asaltantes.*

# **1. RESUMEN EJECUTIVO**

Letra Escarlata es un mecanismo colaborativo para el etiquetado y la alerta de asaltantes violentos basado en geolocalización. Es un mecanismo abierto de gestión automática y distribuída. Ofrece datos de geolocalización de eventos y actores para el desarrollo de herramientas de prevención de delitos violentos en espacios públicos y/o asistencia a víctimas.

No es una herramienta para la recuperación de objetos robados.

El presente documento describe las características generales del modelo.

# **2. CONSIDERACIONES**

A. La mayoría de los asaltos violentos realizados en espacios públicos tienen como propósito el hurto.

B. Uno de los elementos hurtados más comunes son los teléfonos celulares. (\* VALIDAR)

C. Una de cada N (\*CONSULTAR) personas cuenta con un teléfono inteligente con soporte GPS y de acceso a internet.

**3. CASO DE USO**

**3.1 Instalación de la aplicación**

Los ciudadanos instalarán en sus *smartphones* la aplicación SCARLATA. Al activar la aplicación, se le asignará al ciudadano una clave numérica de 8 dígitos. Cuando desee, el *ciudadano* podrá solicitar una nueva clave, que siempre será generada por la propia red SCARLATA. El ciudadano deberá recordar su clave.

La aplicación SCARLATA enviará coordenadas de posición geográfica del dispositivo periódicamente en ciclos de entre 5 y 10 minutos. A la información geográfica transmitida acompañará el código de 8 dígitos del *ciudadano* y nada más. Ninguna información extra del dispositivo o del *ciudadano* será solicitada ni transmitida a través de la red SCARLATA.

**3.2 Etiquetado de asaltantes**

Si el *ciudadano* se torna víctima de un atraco, cederá su *smartphone* al asaltante como botín. Una vez el *ciudadano* esté seguro, ejecutará el procedimiento de etiquetado del *asaltante*. El *ciudadano* buscará un medio de comunicación y declarará el evento mediante alguno de los siguientes métodos:

1. Llamará a un número toll-free e ingresará a través de un IVR los ocho (8) dígitos de su código de *ciudadano*.
2. Enviará un SMS a un número corto con los ocho (8) dígitos de su código de *ciudadano*.

Con cualquiera de estas acciones, el *ciudadano* autorizará la publicación – siempre anónima – de las coordenadas geográficas actualizadas de su dispositivo móvil a través de la aplicación ESCARLATA. Con esto, el *ciudadano* “etiquetará” al *asaltante* como ciñéndole una marca.

**3.3 Señalización de *asaltantes***

Se mostrará la posición geográfica de los *asaltantes* etiquetados en google maps a través de la web y de la propia aplicación móvil de ESCARLATA.

**3.4 Alertas de proximidad**

La aplicación móvil de ESCARLATA emitirá una alerta sonora o vibrante si un *asaltante* etiquetadose encuentra en un radio de 200 mts. de un *ciudadano*.

**3.5 Reconocimiento del *asaltante***

El *ciudadano* alertado tomará los recaudos necesarios para su protección y advertirá del peligro a las personas alrededor suyo. Si le resulta seguro, intentará un reconocimiento visual del *asaltante* etiquetado, su móvil o cualquier otro elemento que facilite su identificación por los demás *ciudadanos*. Añadirá todos los elementos y características reconocibles al perfil del *asaltante* etiquetado en la red ESCARLATA. El usuario podrá ingrear características o votar por características previamente asociadas al *asaltante* etiquetado. La red ESCARLATA ordenará las características según recurrencia en los reportes. Naturalmente se irá afinando la descripción del sospechoso, que será pública.

**4. ARQUITECTURA**

**4.1 Elementos de la red**

1. *Gateways*: Aplicación de código abierto que procesará los requests de la red ESCARLATA de forma distribuída. Los *Gateways* recepcionarán y almacenarán los datos de información geográfica de los *sensores* por espacio de 24 horas. No publicará tales datos hasta que el *ciudadano* lo autorice a través del protocolo de etiquetado.
2. *Sensores*: Aplicación de código abierto para dispositivos móviles con funciones de geolocalización y transmisión de datos de etiquetas.
3. Monitores: Interfaces de usuario para el monitoreo, rastreo, auditoría y alerta de etiquetas.

**4.2 Implementación y Propagación de Gateways**

Podrá existir más de un *Gateway* administrado por distintas organizaciones públicas o privadas. La propagación de los *Gateways* se realizará mediante registros DNS SRV, administrados por una tercera parte de confianza.

**4.3 Certificación de Gateways**

La correcta implementación de los *Gateways* será certificada por un organismo convenido (Quién define este organismo y cómo) antes de poner los dispositivos en producción.

**5. API**

Los nodos de la red ESCARLATA ofrecerán un API basado en REST o un Web Service SOAP que permitirá la creación de nuevos tipos de sensores y monitores.

**6. REQUERIMIENTOS**

**6.1 Gratuidad de la transmisión de datos**

Se solicitará a las operadoras de telefonía móvil la gratuidad de un tráfico de datos mínimo para cada dispositivo móvil contra un set determinado de hosts que harán de *gateways* de entrada para los mensajes de geolocalización.

**6.2 Número corto**

Para activación de etiquetas via SMS.

**6.2 Linea toll-free**

Para activaciones de etiquetas via IVR..

**7. RIESGOS PREDECIBLES**

**7.1 Pánico o Síndrome de Cuco**

….

**7.2 Uso irresponsable**

….

**8. POSIBLES INVALIDADORES**

**8.1 Tiempo de tracking insuficiente**

Es posible que en muchos casos el tiempo en que el *smartphone* (sensor) quede encendido y conectado a partir del evento no sea suficiente para realizar un *tracking* útil, dado que la primera acción del *asaltante* luego de la fuga podría ser apagar el dispositivo y remover su batería. (@GisseJo)

Es posible determinar un umbral de tiempo promedio mediante consultas a víctimas de hurto de celular. Es de suponer que la mayoría de las víctimas realizó al menos una llamada al número de móvil hurtado luego del evento. Es necesario determinar el tiempo transcurrido entre los eventos y las llamadas, y si los teléfonos continuaban o no encendidos.

**8.2 Estado de shock de las víctimas**

Es posible que las víctimas del atraco puedan entrar en estado de shock luego del episodio, y esto las incapacite para la ejecución del protocolo de etiquetado a tiempo.