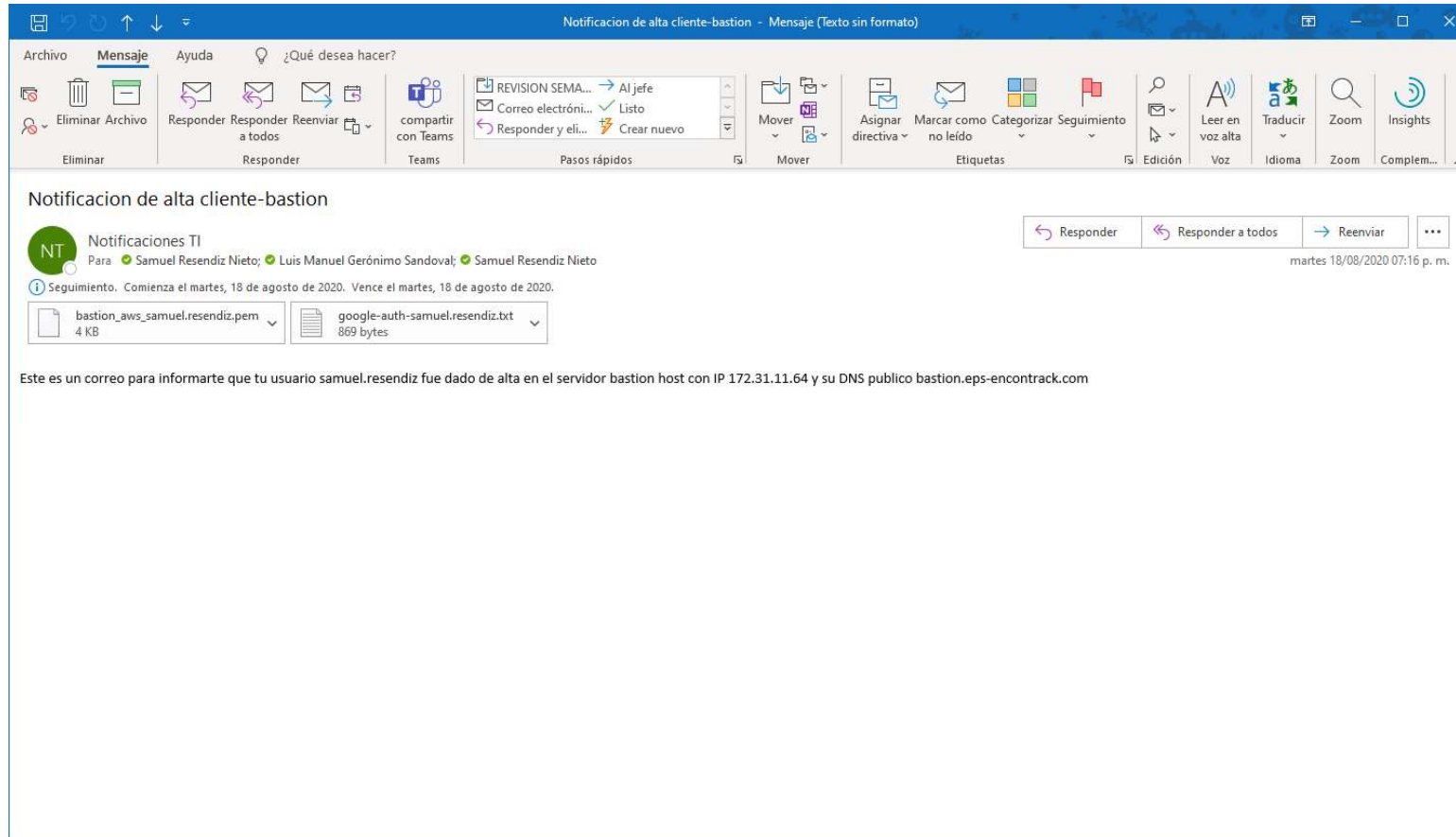


Manual de Acceso Bastion
(doble autenticación)



Recepción de correo

En tu bandeja de entrada recibirás un correo similar a la siguiente imagen:



- Cada colaborador recibirá dos archivos únicos para sus accesos (.pem y .txt) que en pasos posteriores utilizaremos.
- En el cuerpo del correo se encontrará el usuario, IP y DNS publico para el acceso al servidor.

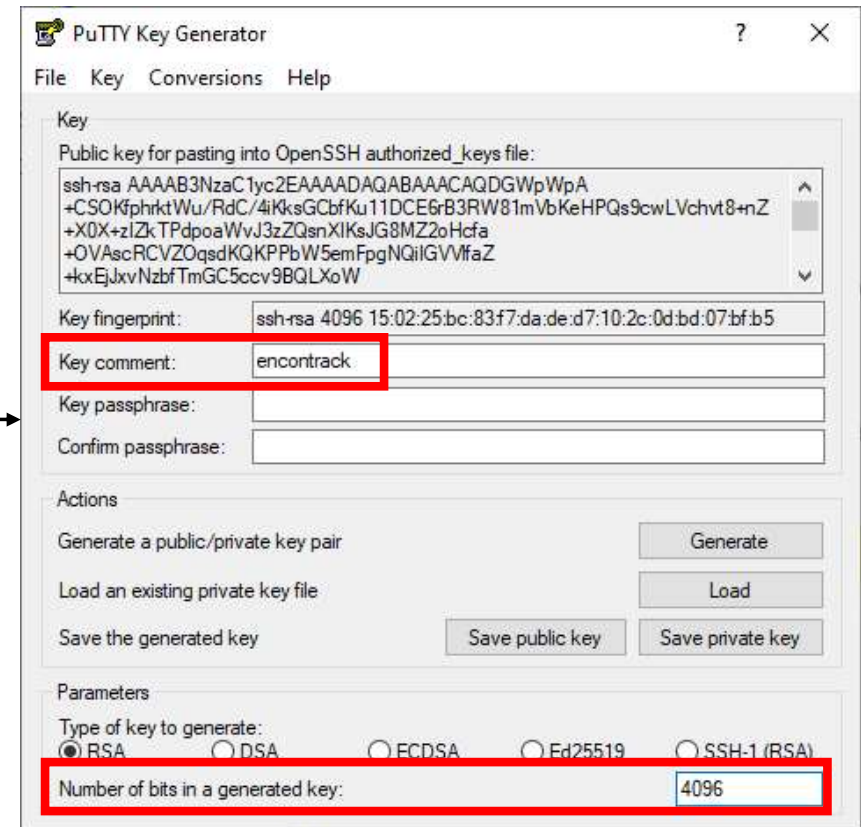
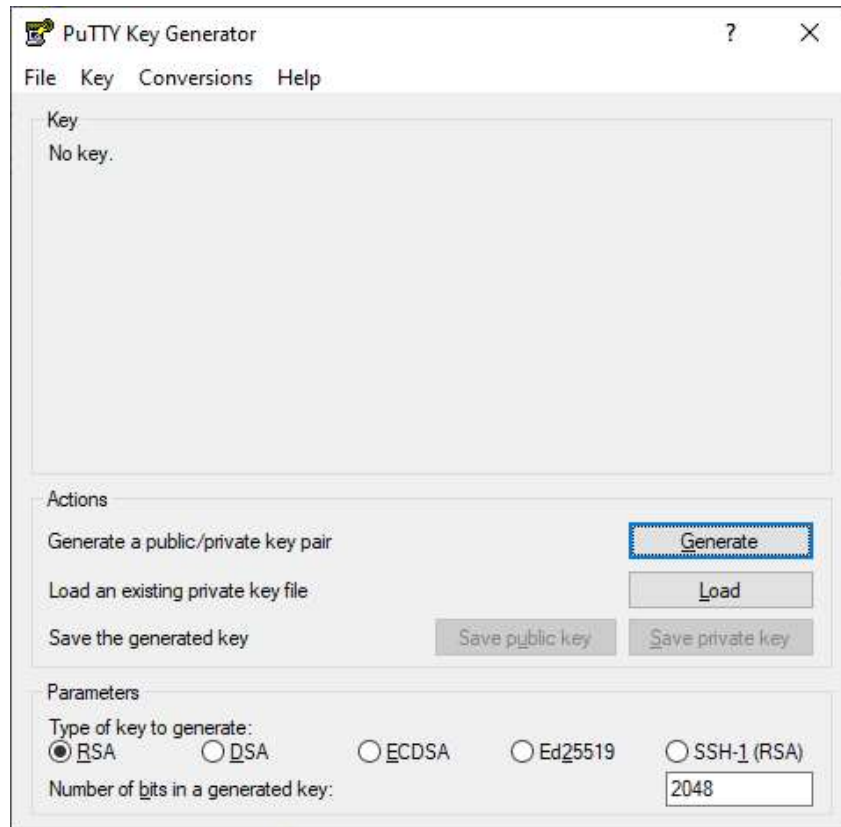
Nota: Descargar los archivos adjuntos en el correo y guardarlos en una localidad segura para su uso.



Transformar llave

Como prerequisite necesitamos tener el programa Puttygen para generar tu clave privada.

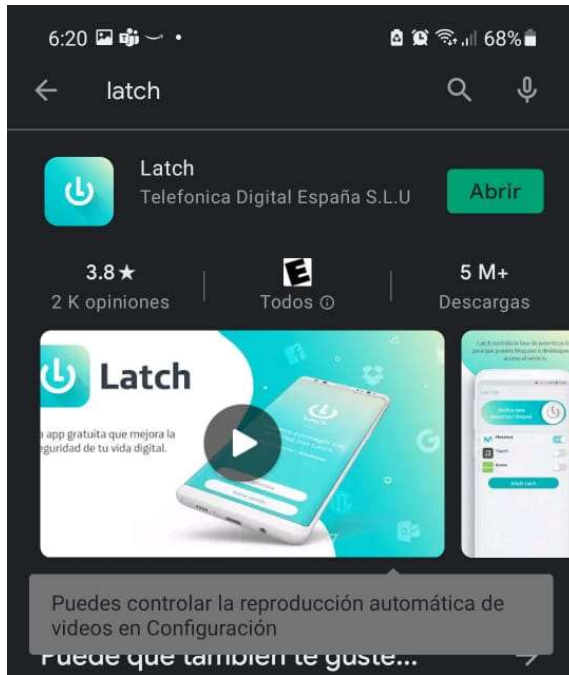
Abrir Puttygen → cargar la el archivo .pem descargado del correo → cambiar los datos a los señalados en la segunda imagen → guardar y nombrar como llave privada .ppk





Descargar aplicación “Latch “

Para poder implementar la doble autenticación es necesario descargar en un celular la aplicación Latch.



Realizar el registro para el acceso a la aplicación de preferencia con los datos de la empresa.

6:24 67%

← Crear una cuenta nueva

Nombre

Email

Contraseña

Repetir contraseña

☐ Confirmando que he leído y que acepto el Acuerdo de licencia de usuario y la Política de privacidad. Asimismo, confirmo que soy mayor de edad de conformidad con las leyes del territorio en el que resido.

☐ Deseo recibir comunicaciones de Marketing y Promociones vía email.

[Acuerdo de licencia de usuario](#)

[Política de privacidad](#)

Enviar

Una vez registrado ingresar a la aplicación.

6:26 67%

Latch

samuel.resendiz@encontrack.com

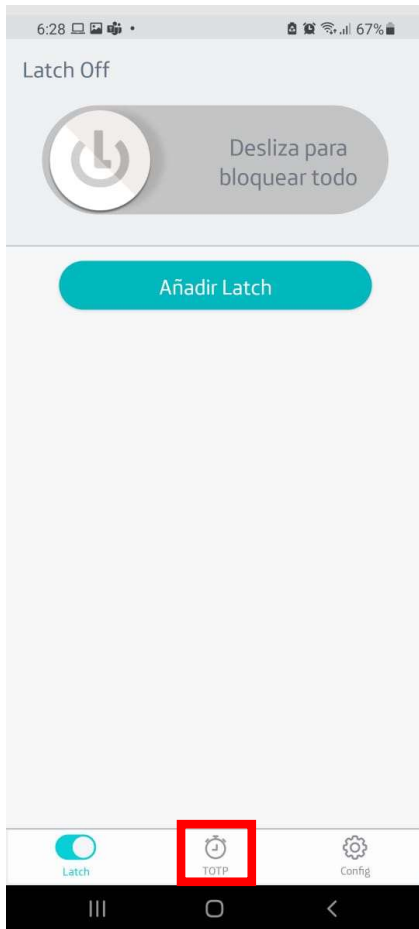
.....

Entrar

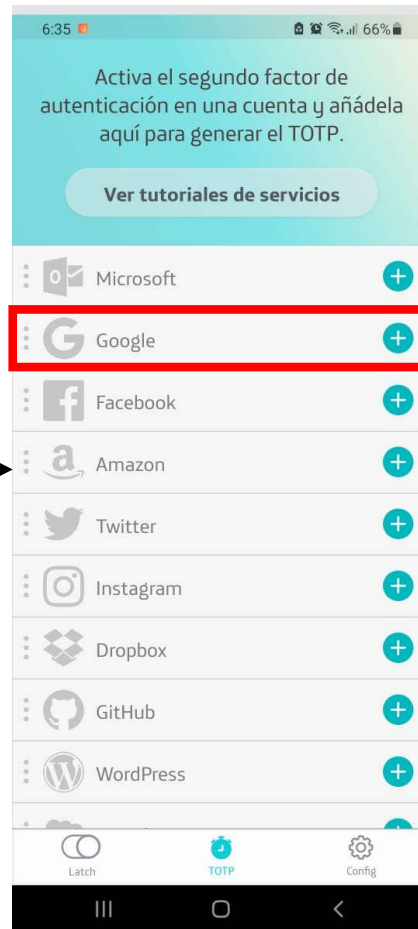
¿Olvidaste tu contraseña? [Restablecer](#)

¿No tienes cuenta? [Nuevo registro](#)

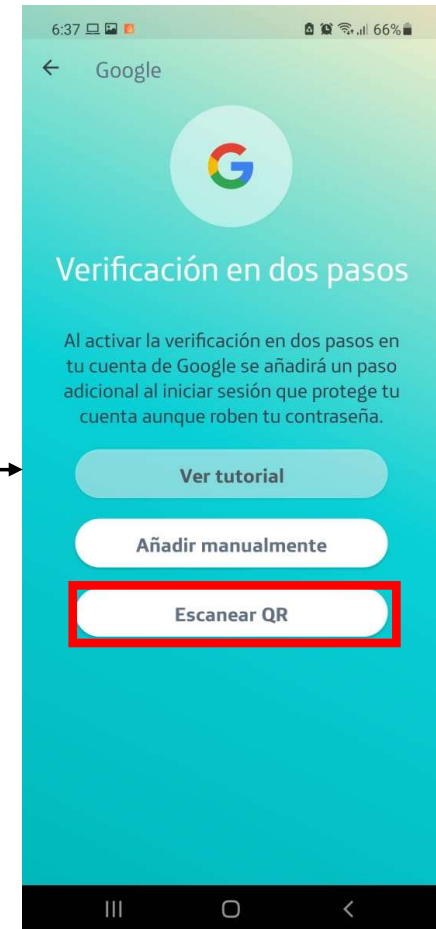
Una vez dentro de la aplicación favor de presionar la opción "TOTP"



Nos aparecerá el siguiente menú y nosotros elegiremos la opción de Google.



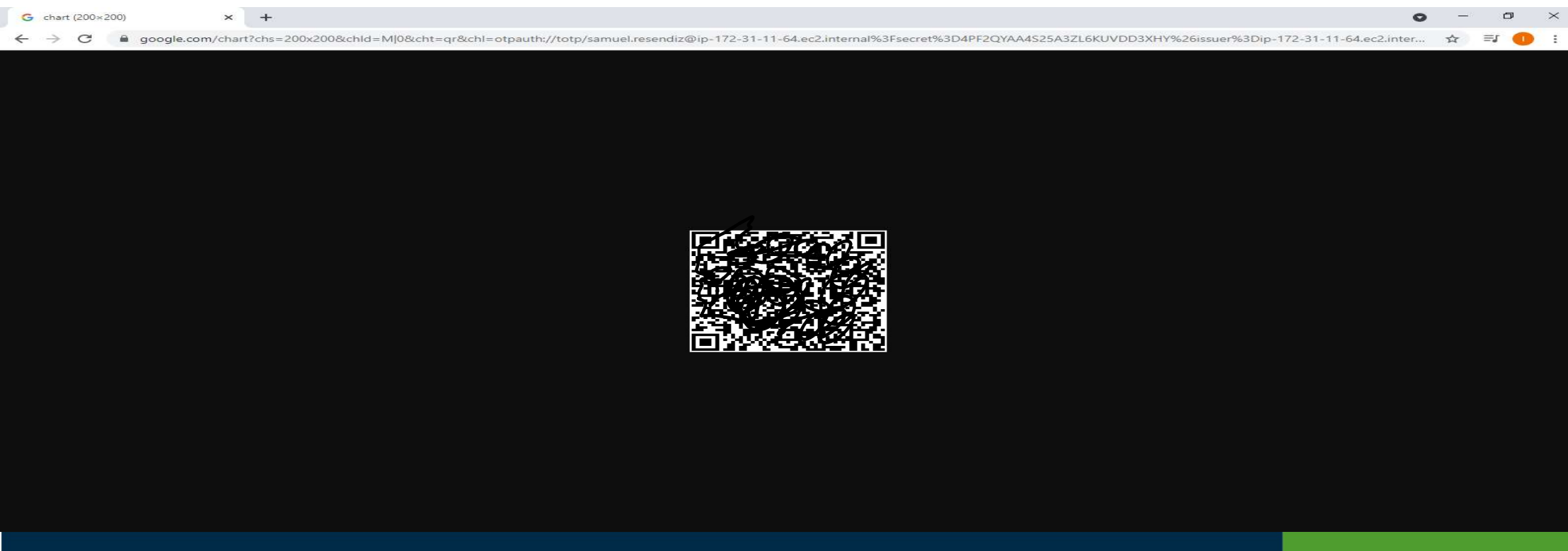
Elegimos la opción de Escanear QR



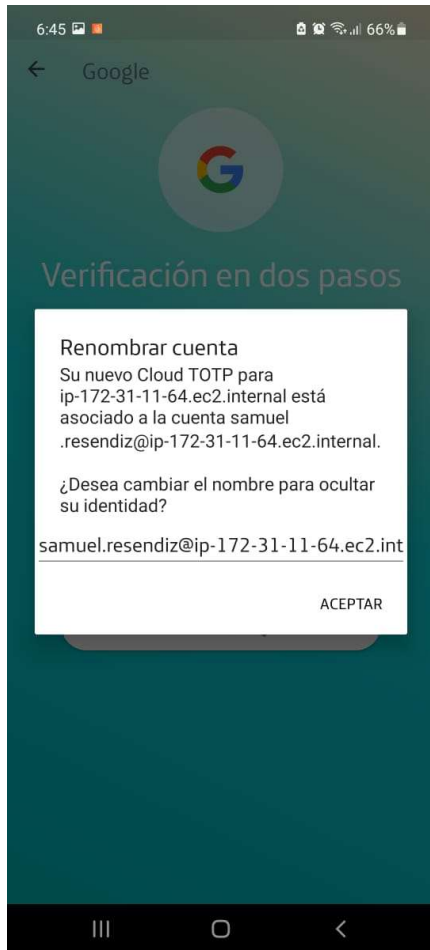
A continuación abriremos el archivo .txt que se envió en el correo inicial y nos aparecerá algo similar a la siguiente imagen:

```
*google-auth-samuel.resendiz: Bloc de notas
Archivo Edición Formato Ver Ayuda
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/samuel.resendiz@ip-172-31-11-64.ec2.internal%3Fsecret%3D4PF2QYAA4S25A3ZL6KUVDD3XHY%26issuer%3Dip-172-31-11-64.ec2.internal
Your new secret key is: 4PF2QYAA4S25A3ZL6KUVDD3XHY Your verification code is 016299 Your emergency scratch codes are: 
Línea 2, columna 199 100% UNIX (LF) UTF-8
```

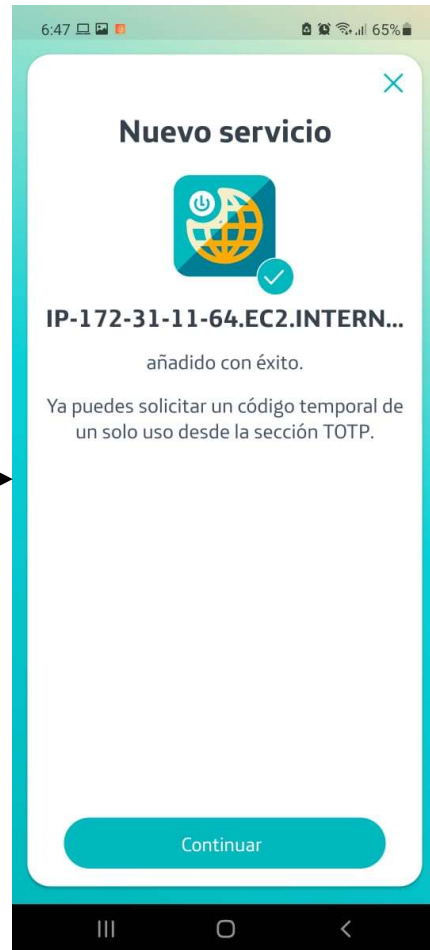
Copiamos la URL completa y la pegamos en un navegador



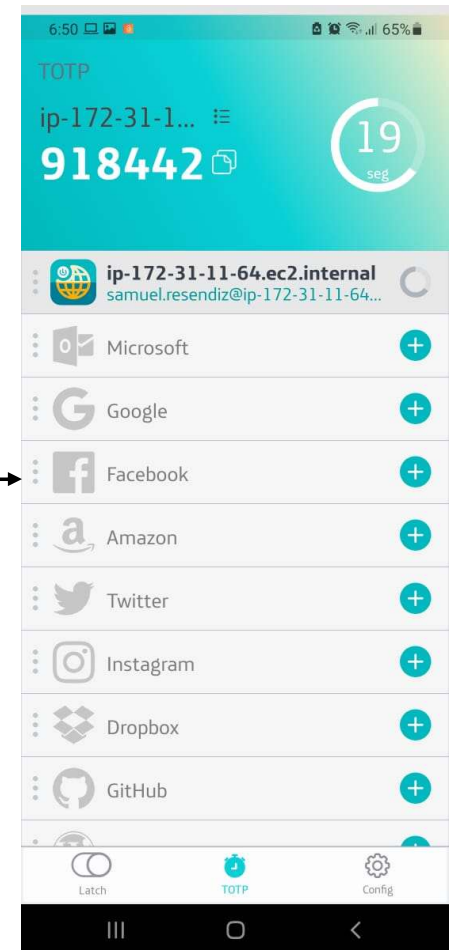
Una vez escaneado el QR nos aparecerá la siguiente imagen:



Aceptamos el alta del TOTP y aparecerá la siguiente imagen:



Pasado el registro ya tenemos activo nuestro código de verificación para el acceso a Bastion



Como siguiente paso configuraremos el acceso por ssh

Session settings

SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL

Warning: you have reached the maximum number of saved sessions for the personal edition of MobaXterm.
You can start a new session but it will not be automatically saved.

Basic SSH settings

Remote host * **bastion.eps-encontr** ☐ Specify username Port **22**

Please support MobaXterm by subscribing to the Professional edition here: <https://mobaxterm.mobatek.net>

Advanced SSH settings Terminal settings Network settings Bookmark settings

☒ X11-Forwarding ☒ Compression Remote environment: **Interactive shell**

Execute command: ☐ Do not exit after command ends

SSH-browser type: **SFTP protocol** ☐ Follow SSH path (experimental)

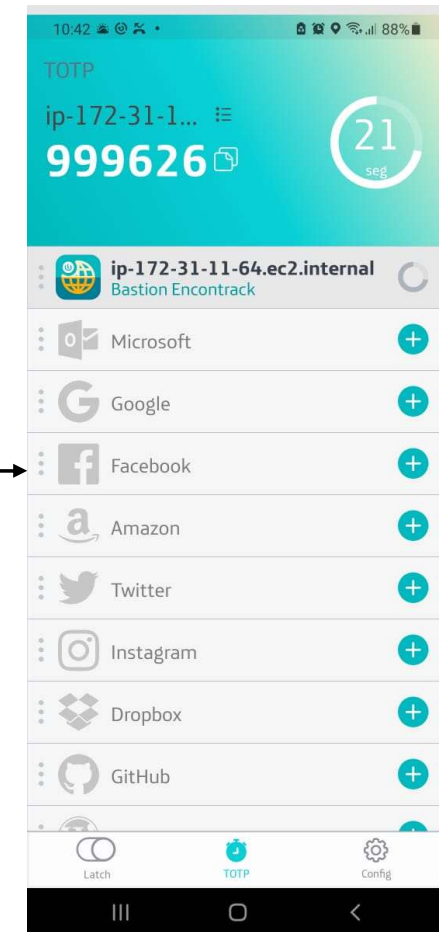
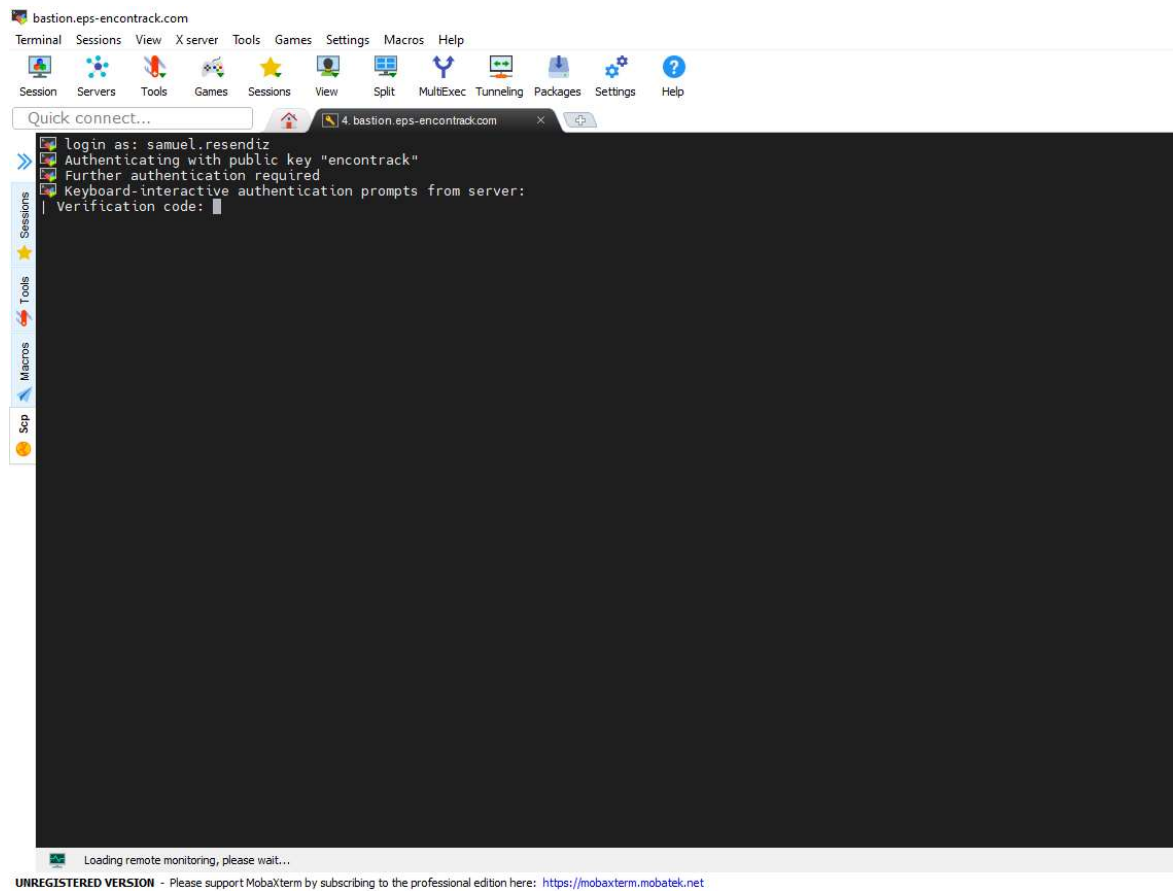
☒ Use private key **C:\Users\Samuel Resendiz\OneDr** ☐ Adapt locales on remote server

Execute macro at session start: **<none>**

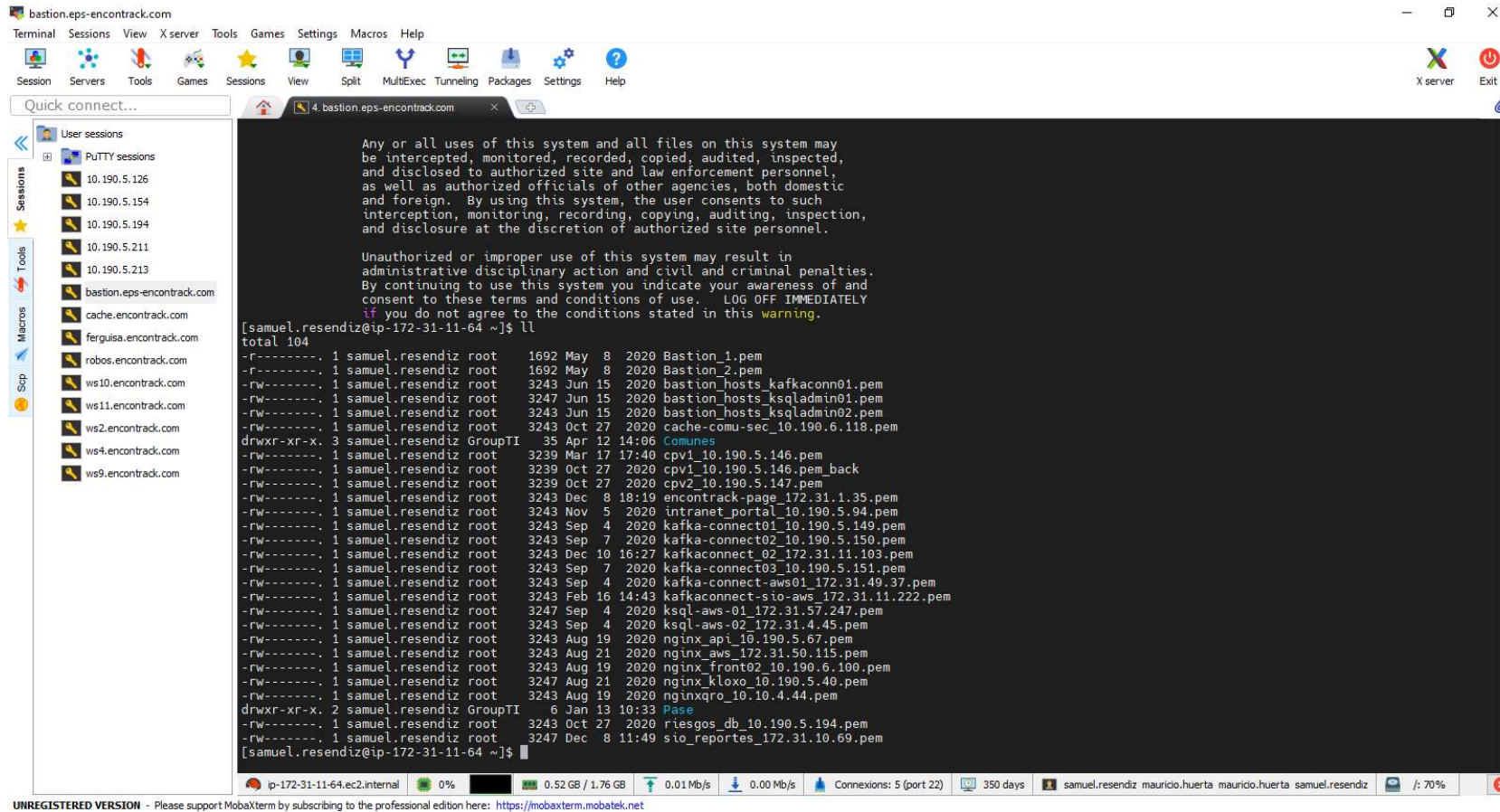
OK Cancel

- Ponemos el nombre del host que se muestra en el correo inicial:
bastion.eps-encontrack.com
- Seleccionar la llave transformada .ppk para crear la primer forma de autenticación.

Para el login se utilizará el usuario que se les envió en el correo y utilizaran el código verificador proporcionado por la aplicación "Latch"



Una vez dentro del Bastion solo tendrán acceso al home asignado y ahí se encontraran los archivos .pem de los servers a los que tienen acceso únicamente.



```
bastion.eps-encontrack.com
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
User sessions
PUTTY sessions
10.190.5.126
10.190.5.154
10.190.5.194
10.190.5.211
10.190.5.213
bastion.eps-encontrack.com
cache.encontrack.com
fergusa.encontrack.com
robos.encontrack.com
ws10.encontrack.com
ws11.encontrack.com
ws2.encontrack.com
ws4.encontrack.com
ws9.encontrack.com

Any or all uses of this system and all files on this system may
be intercepted, monitored, recorded, copied, audited, inspected,
and disclosed to authorized site and law enforcement personnel,
as well as authorized officials of other agencies, both domestic
and foreign. By using this system, the user consents to such
interception, monitoring, recording, copying, auditing, inspection,
and disclosure at the discretion of authorized site personnel.

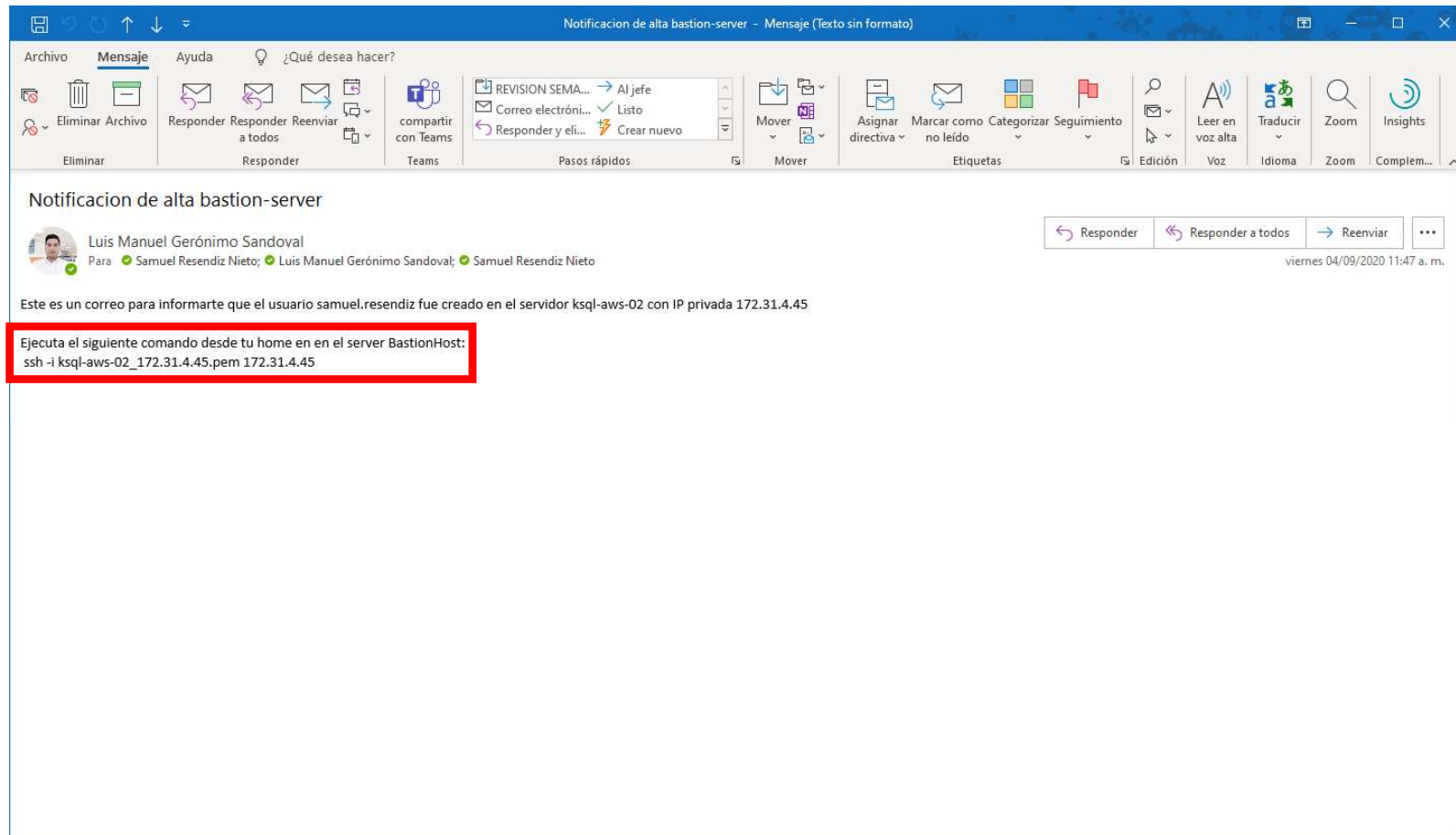
Unauthorized or improper use of this system may result in
administrative disciplinary action and civil and criminal penalties.
By continuing to use this system you indicate your awareness of and
consent to these terms and conditions of use. LOG OFF IMMEDIATELY
if you do not agree to the conditions stated in this warning.

[samuel.resendiz@ip-172-31-11-64 ~]$ ll
total 104
-r----- 1 samuel.resendiz root 1692 May 8 2020 Bastion_1.pem
-r----- 1 samuel.resendiz root 1692 May 8 2020 Bastion_2.pem
-rw----- 1 samuel.resendiz root 3243 Jun 15 2020 bastion_hosts_kafkaconn01.pem
-rw----- 1 samuel.resendiz root 3247 Jun 15 2020 bastion_hosts_ksqladmin01.pem
-rw----- 1 samuel.resendiz root 3243 Jun 15 2020 bastion_hosts_ksqladmin02.pem
-rw----- 1 samuel.resendiz root 3243 Oct 27 2020 cache-comu-sec_10.190.6.118.pem
drwxr-xr-x 3 samuel.resendiz GroupTI 35 Apr 12 14:06 Comunes
-rw----- 1 samuel.resendiz root 3239 Mar 17 17:40 cpv1_10.190.5.146.pem
-rw----- 1 samuel.resendiz root 3239 Oct 27 2020 cpv1_10.190.5.146.pem_back
-rw----- 1 samuel.resendiz root 3239 Oct 27 2020 cpv2_10.190.5.147.pem
-rw----- 1 samuel.resendiz root 3243 Dec 8 18:19 encontrack_page_172.31.1.35.pem
-rw----- 1 samuel.resendiz root 3243 Nov 5 2020 intranet_portal_10.100.5.94.pem
-rw----- 1 samuel.resendiz root 3243 Sep 4 2020 kafka-connect01_10.190.5.149.pem
-rw----- 1 samuel.resendiz root 3243 Sep 7 2020 kafka-connect02_10.190.5.150.pem
-rw----- 1 samuel.resendiz root 3243 Dec 10 16:27 kafkaconnect_02_172.31.11.103.pem
-rw----- 1 samuel.resendiz root 3243 Sep 7 2020 kafka-connect03_10.190.5.151.pem
-rw----- 1 samuel.resendiz root 3243 Sep 4 2020 kafka-connect-aws01_172.31.49.37.pem
-rw----- 1 samuel.resendiz root 3243 Feb 16 14:43 kafkaconnect-sio-aws_172.31.11.222.pem
-rw----- 1 samuel.resendiz root 3247 Sep 4 2020 ksql-aws-01_172.31.57.247.pem
-rw----- 1 samuel.resendiz root 3243 Sep 4 2020 ksql-aws-02_172.31.4.45.pem
-rw----- 1 samuel.resendiz root 3243 Aug 19 2020 nginx_api_10.190.5.67.pem
-rw----- 1 samuel.resendiz root 3243 Aug 21 2020 nginx_aws_172.31.50.115.pem
-rw----- 1 samuel.resendiz root 3243 Aug 19 2020 nginx_front02_10.190.6.100.pem
-rw----- 1 samuel.resendiz root 3247 Aug 21 2020 nginx_kloxo_10.190.5.40.pem
-rw----- 1 samuel.resendiz root 3243 Aug 19 2020 nginxqro_10.10.4.44.pem
drwxr-xr-x 2 samuel.resendiz GroupTI 6 Jan 13 10:33 Pase
-rw----- 1 samuel.resendiz root 3243 Oct 27 2020 riesgos_db_10.190.5.194.pem
-rw----- 1 samuel.resendiz root 3247 Dec 8 11:49 sio_reportes_172.31.10.69.pem
[samuel.resendiz@ip-172-31-11-64 ~]$
```

ip-172-31-11-64.ec2.internal 0% 0.52 GB / 1.76 GB 0.01 Mb/s 0.00 Mb/s Connexions: 5 (port 22) 350 days samuel.resendiz mauricio.huerta mauricio.huerta samuel.resendiz /: 70%

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

Para los accesos a los servidores recibirán un correo como el que se muestra a continuación y ahí se describe la forma de como ingresar a los servidores asignados





Gracias por su atención y para cualquier duda, favor de comunicarse con Luis Manuel y/o Samuel Reséndiz.