Linux Week 2012

Firma digital de documentos en Linux

Pablo Fonseca
Dirección de Informática Académica
PUCP

¿Para qué sirve?

- **Hacer trámites** del gobierno por internet.
- **Firmar contratos**.
- **Aprobar documentos**
  - Planos de ingeniería.
  - Presupuestos.
  - Autorizaciones.

Firma digital: ¿Qué se puede lograr?

- Garantizar **la identidad del que firma**.
- Garantizar **la integridad del documento**.

¿Válido legalmente?

LEY Nº 27269

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República
ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY DE FIRMAS Y CERTIFICADOS DIGITALES

2000

*"(...) **RENIEC** inauguró hoy en San Isidro la primera oficina de la Entidad de Registro Digital del Estado Peruano (EREP) "*

24 de febrero del 2012

http://www.reniec.gob.pe/portal/detalleNota.htm?nota=551

2012

Certificados digitales: ¿Confianza?

DELEGACIÓN DE CONFIANZA: Un usuario confía en la validez de una firma digital **si confía en la autoridad certificadora (CA) que emitió el certificado.**

En PERÚ

- RENIEC inauguró una **autoridad certificadora** en Febrero 2012.

- Para personas naturales: **DNI Electrónico.**

Firmando: lo que debemos saber (I)

- Un documento se firma con un **certificado digital.**
- Los certificados digitales se guardan en **contenedores.**

Firmando: lo que debemos saber (II)

- Un documento PDF puede tener **varias firmas digitales.**

- Las firmas pueden ser validadas por una **Autoridad de Sello de Tiempo (TSA).**

Tipos de firma digital

- **Asistida**

  -¿Quién lo usa? : Usuarios que aprueban documentos, firman contratos, etc.

- **Silenciosa**

  -¿Quién lo usa? : Aplicaciones web, firmado en batch, etc.

Contenedores: ¿Dónde guardo los certificados?

- PKCS #12 (*.p12 *.pfx)
- Java Key Store (JKS)
- WINDOWS-MY
- Otros

JSignPDF: Características

- Open source (MPL, LGPL).
- Firmas visibles.
- Estampa de tiempo.
- Validación CRL, OCSP
- Configuración del nivel de certificación
- Encriptación de PDF y derechos de acceso.
- Procesamiento en batch.

JSignPDF vs Software Comercial

- Las funcionalidades más importantes están soportadas.
- Costo por licencia: $ 0.00 vs 1000'$
- Código fuente disponible.
- Licencia permite desarrollar software comercial.
- Funciona como plugin para OpenOffice / LibreOffice.

Creando certificados de prueba

- **Crear root certificate**
  - /etc/pki/tls/misc/CA -newca
- **Crear certificado**
  - /etc/pki/tls/misc/CA -newreq
  - /etc/pki/tls/misc/CA -sign
- **Convertir PEM en x509 para usar el certificado en un Keystore**
  - openssl x509 -in /path/cacert.pem -out root_certificate.ca
- **Convertir a pfx**
  - openssl pkcs12 -inkey newkey.pem -in newcert.pem -export -out user_certificate.pfx
- **Importar certificado en JKS**
  - keytool -importcert -file /path/root_certificate.ca -keystore keystore.jks

Crear root certificate

/etc/pki/tls/misc/CA -newca

```
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            f3:f3:cf:4e:e2:f4:f7:1f
        Validity
            Not Before: Mar 13 14:59:06 2012 GMT
            Not After : Mar 13 14:59:06 2015 GMT
        Subject:
            countryName               = PE
            stateOrProvinceName       = Lima
            organizationName          = Palefo
            organizationalUnitName    = Technology
            commonName                = Palefo
            emailAddress              = pfonseca@pucp.edu.pe
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D3:4E:B4:85:C9:4D:FF:49:C4:88:83:B8:A0:28:C6:22:01:BB:C3:D0
            X509v3 Authority Key Identifier:
                keyid:D3:4E:B4:85:C9:4D:FF:49:C4:88:83:B8:A0:28:C6:22:01:BB:C3:D
0

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Mar 13 14:59:06 2015 GMT (1095 days)

Write out database with 1 new entries
```

Crear un certificado (I)

/etc/pki/tls/misc/CA -newreq

```
Generating a 2048 bit RSA private key
.....................................................................................................................+++
.................................+++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:PE
State or Province Name (full name) []:Lima
Locality Name (eg, city) [Default City]:Lima
Organization Name (eg, company) [Default Company Ltd]:Palefo
Organizational Unit Name (eg, section) []:Technology
Common Name (eg, your name or your server's hostname) []:Pablo Fonseca
Email Address []:user@server.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request is in newreq.pem, private key is in newkey.pem
```

Crear un certificado (II)

/etc/pki/tls/misc/CA -sign

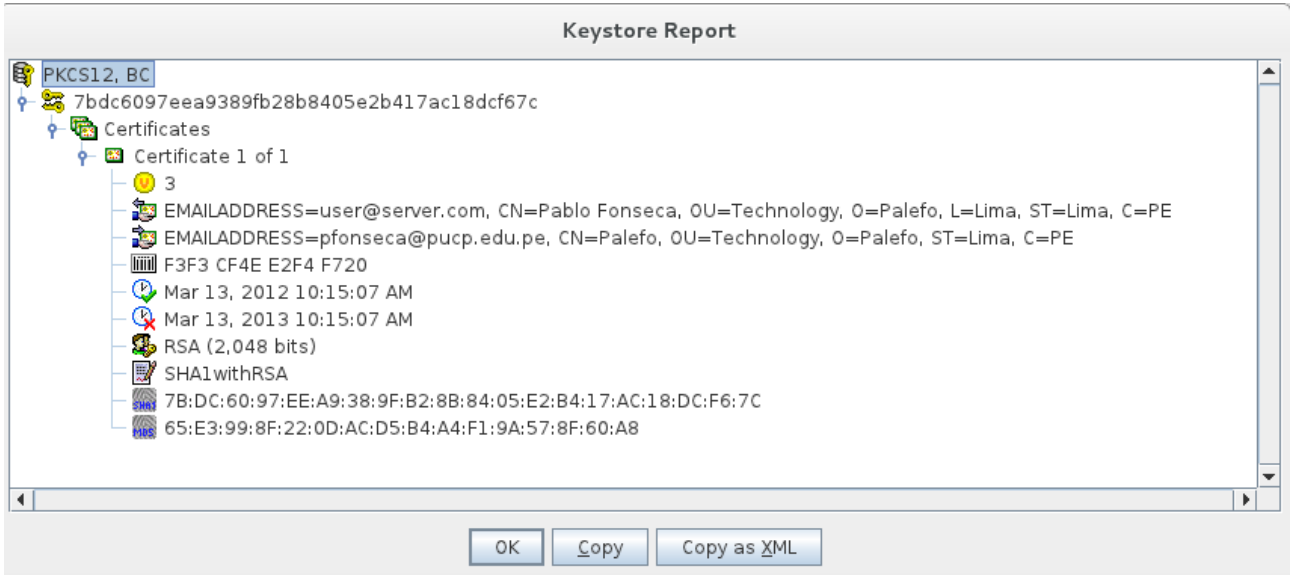
```
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            f3:f3:cf:4e:e2:f4:f7:20
        Validity
            Not Before: Mar 13 15:15:07 2012 GMT
            Not After : Mar 13 15:15:07 2013 GMT
        Subject:
            countryName               = PE
            stateOrProvinceName       = Lima
            localityName              = Lima
            organizationName          = Palefo
            organizationalUnitName    = Technology
            commonName                = Pablo Fonseca
            emailAddress              = user@server.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                25:06:E6:59:34:2D:42:8C:C3:82:E6:9A:9D:DC:38:1E:35:2E:61:07
            X509v3 Authority Key Identifier:
                keyid:D3:4E:B4:85:C9:4D:FF:49:C4:88:83:B8:A0:28:C6:22:01:BB:C3:D0

Certificate is to be certified until Mar 13 15:15:07 2013 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
```

Exportar un certificado a PFX

openssl pkcs12 -inkey newkey.pem -in newcert.pem -export -out user_certificate.pfx

```
Enter pass phrase for newkey.pem:
Enter Export Password:
Verifying - Enter Export Password:
```

Se necesitará usar el "Export Password" para poder usar el certificado.

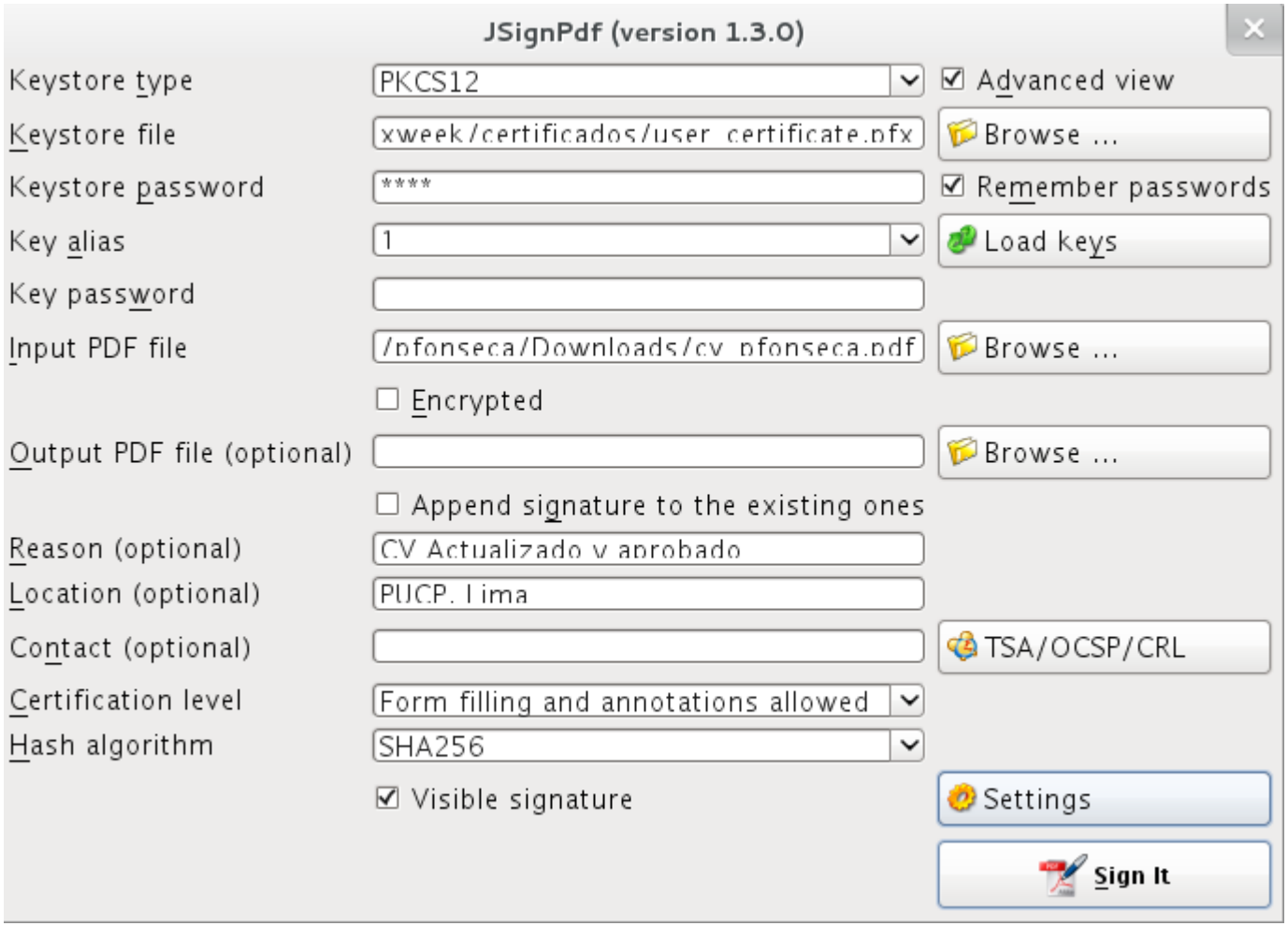


**Portecle*

Exportar el root certificate

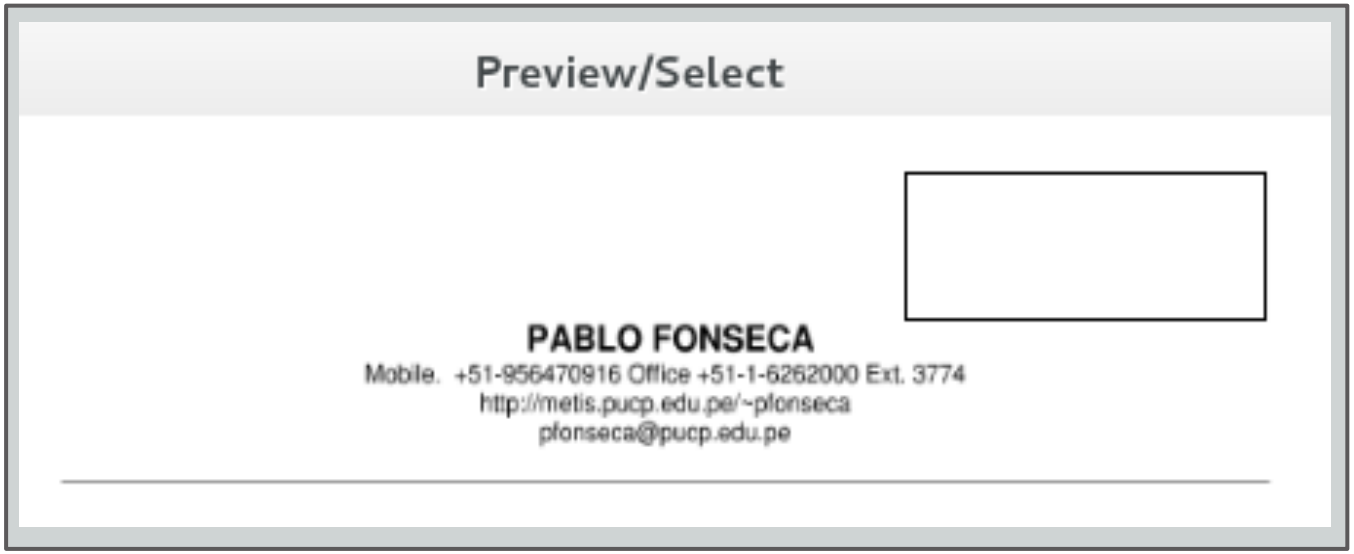
openssl x509 -in cacert.pem -out root_certificate.cer

Firmar el PDF (I)

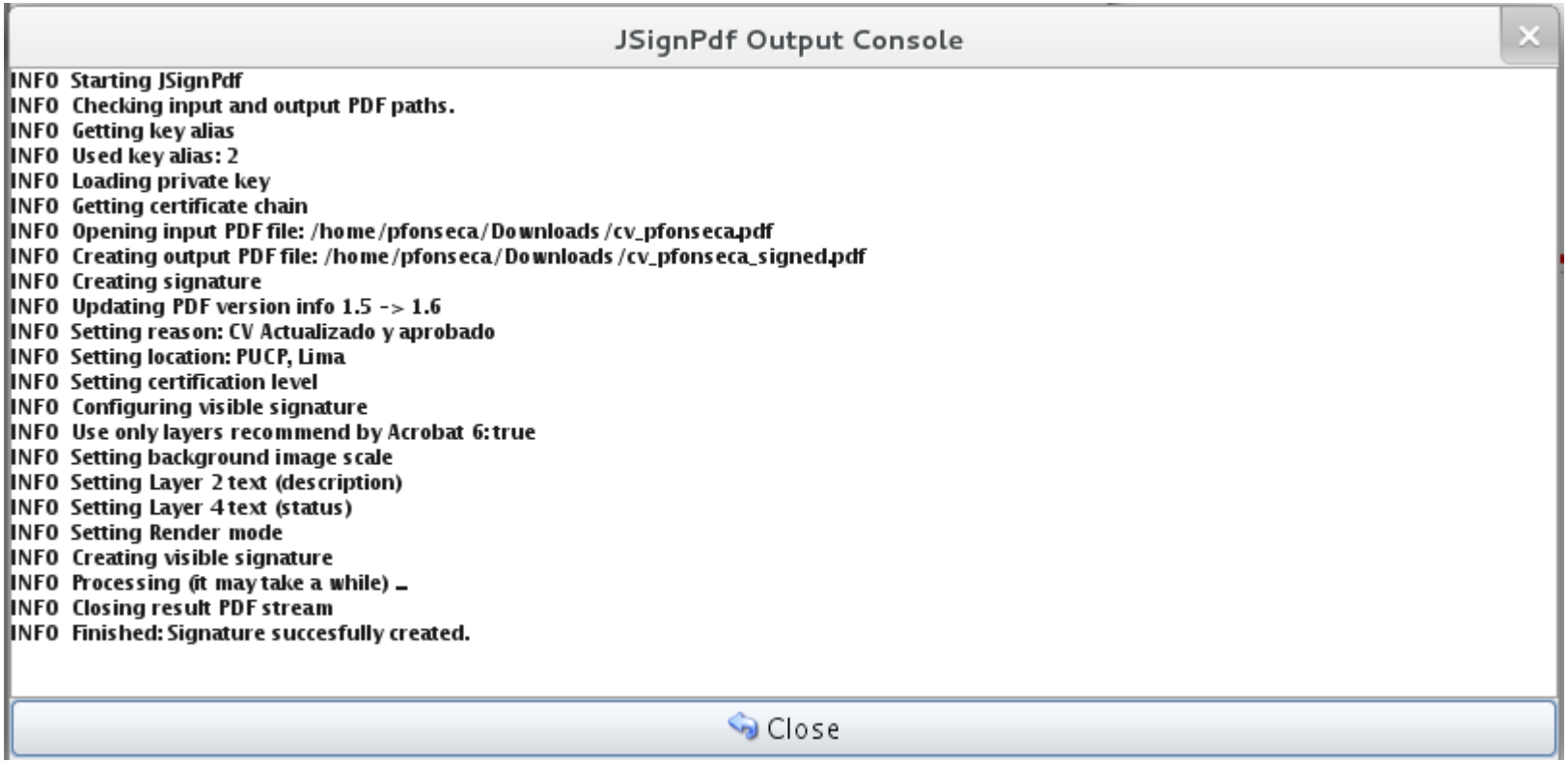


Firmar el PDF (II)

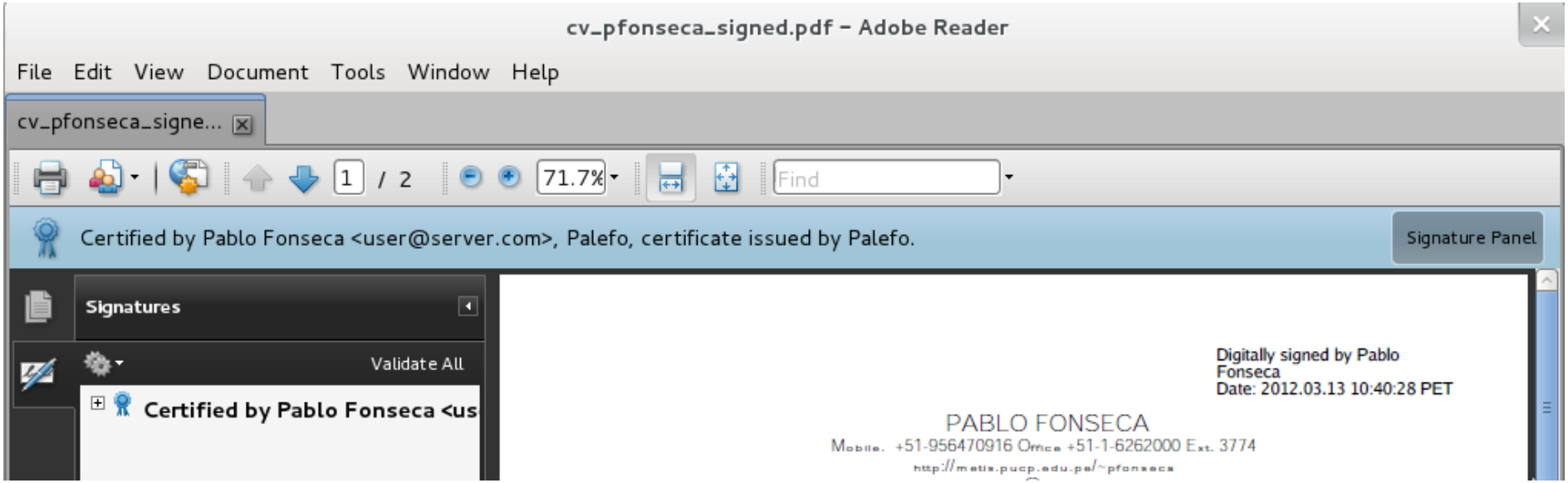
Seleccionar el área donde se firmará.



Firmar el PDF (III)



Firmar el PDF (IV)



Siguiente paso:

- Usar JSignPDF como librería.
- Usar JSignPDF para firma en batch.

Conclusiones

- Momento ideal en el Perú para desarrollar software que incluya posibilidad de firma digital.

- JSignPDF es muy completo y se podría usar como librería o como aplicación.

Referencias útiles

- RENIEC: http://www.reniec.gob.pe/portal/principalPKI.htm

- JSIGNPDF:
  http://jsignpdf.sourceforge.net/

¿Preguntas?

Gracias!

Contacto:
Pablo Fonseca
Email: pfonseca@pucp.edu.pe
Twitter: @palefo