universidad SANJORGE
GRUPO SANVALERO

Protección del puesto de trabajo.

Curso 2018-2019

Departamento de Sistemas de Información USJ

✓ Protección de la información.

- El puesto de trabajo es clave para la protección de la información de la organización. Por ello, es necesario que apliquemos un conjunto de medidas de seguridad que nos garanticen que la información esté correctamente protegida.

Objetivo

- ✓ **Cumplimiento normativo.**

Ley Orgánica de Protección de Datos (LOPD)

Reglamento Europeo de Protección de Datos (25-5-18)

✓ Qué vamos a ver.

- ❑ Amenazas.
- ❑ Medidas de protección.
- ❑ Consejos útiles.
- ❑ Herramientas gratuitas.
- ❑ Guías de interés.

✓ Entorno tecnológico.

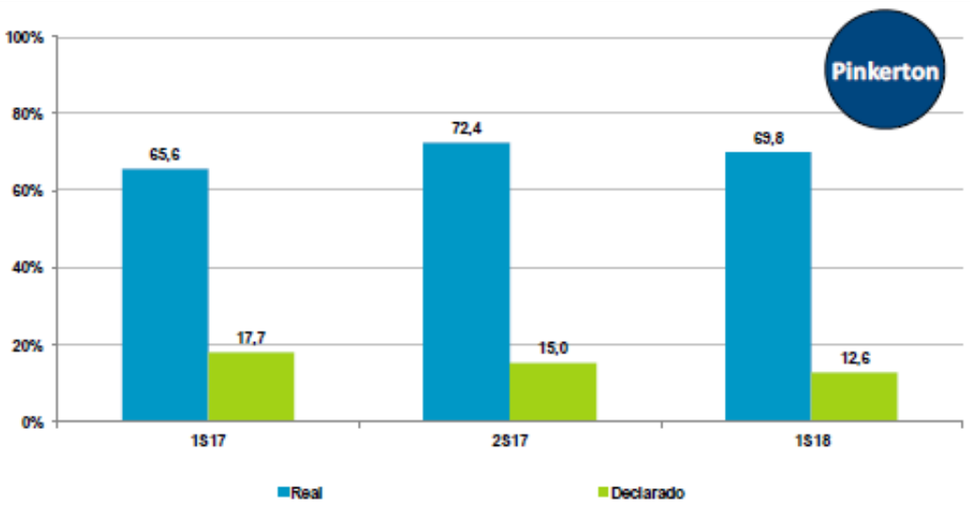
- Equipos informáticos (ordenadores, impresoras...).
- Redes cableadas.
- Redes WIFI.
- Dispositivos móviles.

✓ Amenazas - Malware.

- Phising. Ingeniería social. Conseguir información del usuario mediante engaños.
- Virus. Daña el equipo. Ejecución código maligno. Interviene usuario.
- Gusano. Se autopropaga. Consume recursos, ralentiza los sistemas.
- Troyano. Puerta trasera para otros programas. Difícil de detectar. ¡¡**Keylogers**!!.
- Adware. Publicidad no deseada. Molesto / Dañino (uso navegador).
- Spyware. Recopila toda la actividad del equipo.
- Ramsonware. Objetivo conseguir dinero cifrando información usuario.
- Rogueware. Alerta de virus con el fin de instalar un supuesto antivirus.

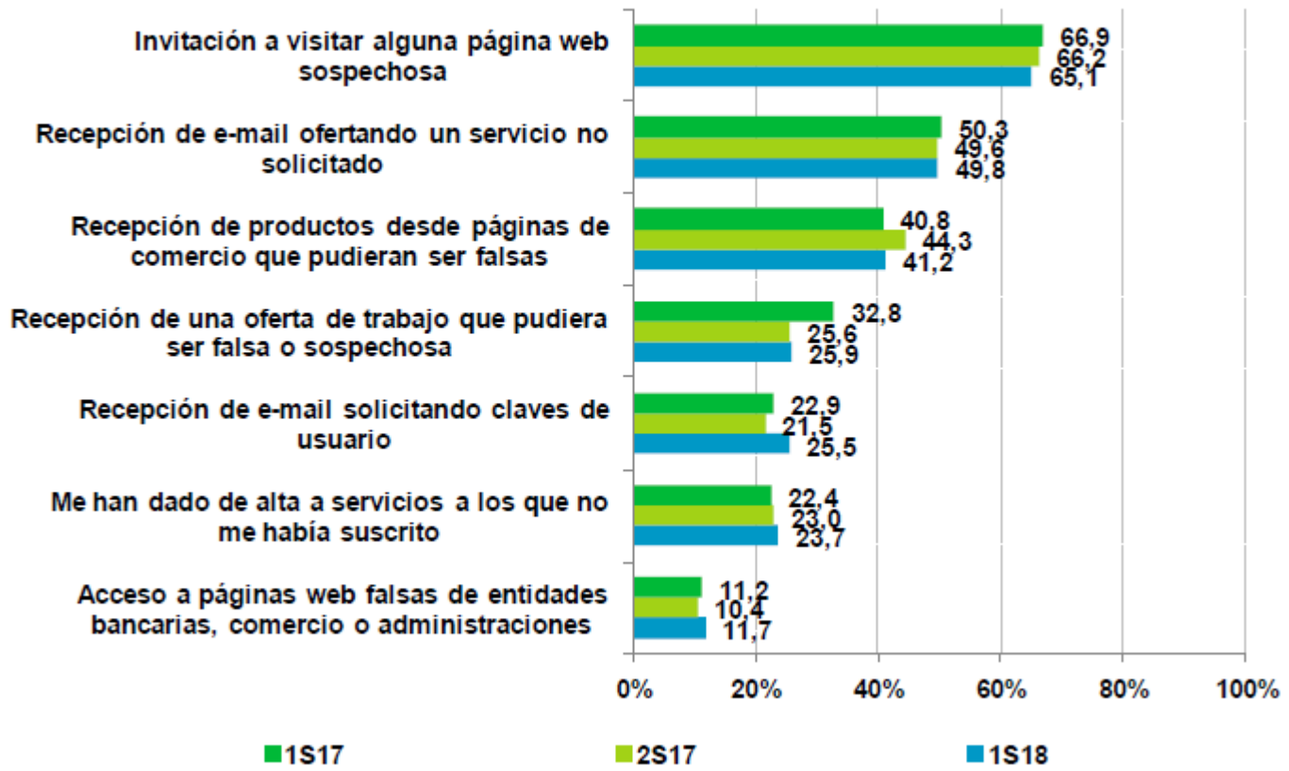
✓ Incidencia Malware.

FIGURA 13. EVOLUCIÓN DE LAS INCIDENCIAS DE MALWARE (DECLARADO VS. REAL) EN EL ORDENADOR DEL HOGAR (%)



Base: usuarios de PC
Fuente: Panel hogares, ONTSI

FIGURA 19. EVOLUCIÓN DE LA MANIFESTACIÓN DE LOS INTENTOS DE FRAUDE ONLINE (%)



Base: Usuarios que han sufrido un intento de fraude
Fuente: Panel hogares, ONTSI

✓ Phising - Ingeniería Social.

- Los ataques de ingeniería social tienen como objetivo a cualquier empleado, sin importar en el puesto que esté. A través de ellos un atacante puede obtener información confidencial de las propias víctimas, o utilizar a ésta para acceder a otras personas de la organización de manera inadvertida.

- Captan nuestra atención con alguna excusa con el fin de redirigirnos a páginas web fraudulentas que simulan ser las legítimas de un determinado servicio o empresa.

✓ Phising – Cómo detectarlo.

- Los mensajes suelen estar mal redactados.
- Piden cosas absurdas o algo que no has solicitado.
- Suelen notificar problemas de seguridad, desactivaciones de servicios…
- Suelen ser anónimos dirigidos a "Estimado cliente", ...
- Obligan a tomar una decisión en pocas horas.
- Suelen incorporar enlaces a dominios similares pero no originales.
- Los servicios de prestigio utilizan sus propios dominios para las comunicaciones.

✓ Phising - Casos reales.

De: ANDREA JACKELINE ALVARADO CHILLOGALLO [mailto:ajalvarado1@utpl.edu.ec]
Enviado el: lunes, 16 de julio de 2018 16:08
Para: ANDREA JACKELINE ALVARADO CHILLOGALLO
Asunto: RE: ¡¡¡Advertencia general!!!

¡¡¡Advertencia general!!!

Nuestra base de datos ha detectado un tráfico anormal y su cuenta se bloqueará en respuesta a la señal de protesta recibida por el protocolo de seguridad, que se intentó iniciar sesión / usar su cuenta de correo electrónico en actividades inusuales a través de una computadora desconocida. Para evitar perder su cuenta de correo electrónico, le recomendamos hacer **clic** para actualizar su correo electrónico dentro de las próximas 24 horas

2018. Todos los derechos reservados
WEB MAIL SECURITY DESK

De: Universidad-San-Jorge-Zaragoza [mailto:kdopacio@anlis.gov.ar]
Enviado el: miércoles, 18 de abril de 2018 10:21
Para: undisclosed-recipients:
Asunto: Verifica tu cuenta

MENSAJE IMPORTANTE DE ADMIN

Estimado usuario de Universidad-San-Jorge-Zaragoza,
Notamos que su cuenta de correo electrónico casi ha excedido su límite. Y es posible que no pueda enviar o recibir mensajes en cualquier momento a partir de ahora.
Haga clic en el enlace a continuación para renovar su cuenta;
http // abiluco.com / webauth / i /? webmail.usj.es
no renovar su cuenta Estará permanentemente discapacitado

Gracias,
Equipo de correo electrónico
© 2018 Universidad-San-Jorge-Zaragoza

✓ Phising - Casos reales.

De: [redacted]@usj.es [mailto:istiancalero@etb.net.co]
Enviado el: sábado, 22 de septiembre de 2018 10:15
Para: [redacted]@usj.es
Asunto: Su cuenta ([redacted]@usj.es) fue pirateada

¡Hola!

Puede que no me conozca y probablemente esté preguntándose por qué está recibiendo este correo electrónico, ¿correcto?
En este momento pirateé tu cuenta ([redacted]@usj.es). ¡Tengo pleno acceso a tu dispositivo! Te envio un correo electrónico desde tu cuenta !
De hecho, coloqué un malware en el sitio web de videos para adultos (material pornográfico) y usted sabe qué, usted visitó este sitio web para divertirse (ya sabe a qué me refiero).
Mientras estabas viendo clips de video,
su navegador de Internet comenzó a funcionar como un RDP (escritorio remoto) que tiene un registrador de teclas que me proporcionó acceso a su pantalla y también a su cámara web.
Inmediatamente después, mi programa de software reunió todos sus contactos desde su Messenger, redes sociales y correo electrónico.

¿Qué hice?
Hice un video de doble pantalla. La primera parte muestra el video que estabas viendo (tienes un buen gusto ya veces extraño), y la segunda parte muestra la grabación de tu cámara web.
¿Exactamente qué deberías hacer?

Bueno, creo que $250 es un precio justo para nuestro pequeño secreto. Realizará el pago con Bitcoin (si no lo sabe, busque "cómo comprar bitcoin" en Google).
Dirección de BTC: 1LK8rRhBTekN3Uxh8ib83FfmvMsX6EQnqL
(Es muy sensible, así que cópielo y péguelo)

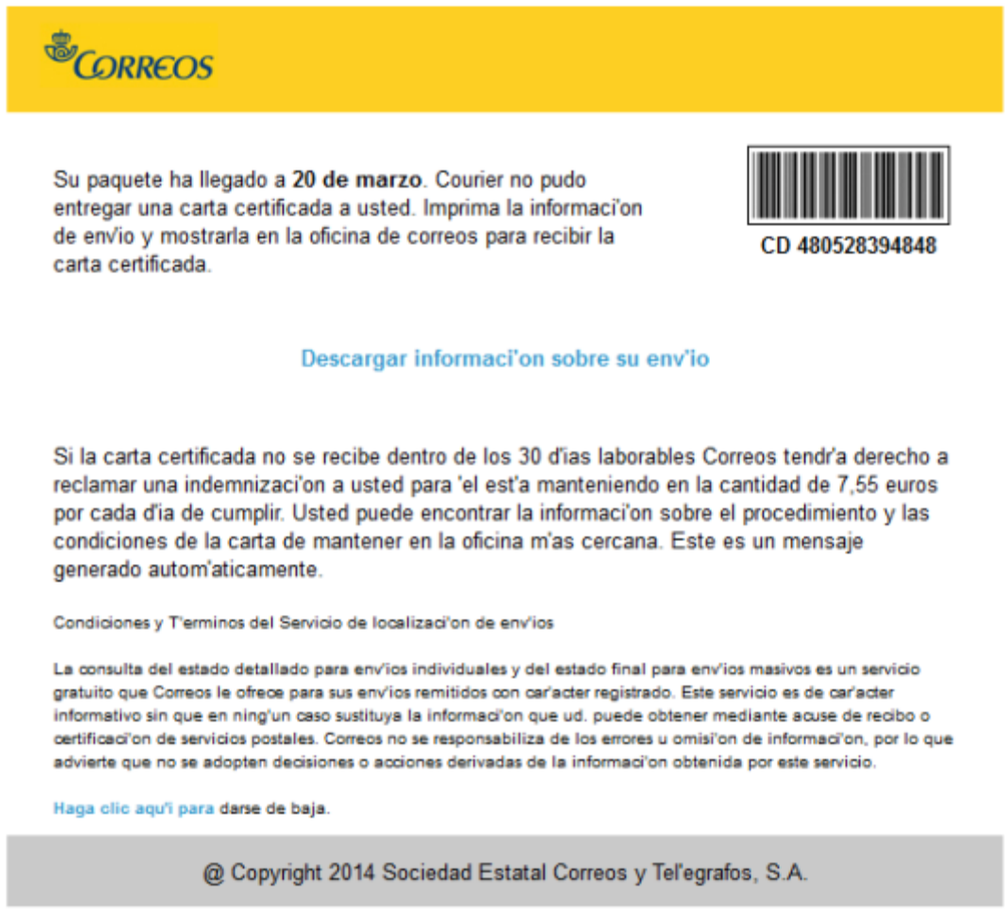
Nota:
Tienes 2 días para hacer el pago.
(Tengo un píxel específico en este mensaje de correo electrónico, y en este momento sé que ha leído este mensaje de correo electrónico).

Si no obtengo los BitCoins, definitivamente enviaré su grabación de video a todos sus contactos, incluidos familiares, compañeros de trabajo, etc.

Sin embargo, si pagas, destruiré el video inmediatamente.
Si desea pruebas, responda con "¡Sí!" y enviaré tu grabación de video a tus 3 amigos
Esta es la oferta no negociable, así que no pierda mi tiempo personal y el suyo respondiendo a este mensaje de correo electrónico.

La próxima vez, ¡ten cuidado!
¡Adiós!

✓ Ramsonware - Casos reales.



CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 480528394848

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

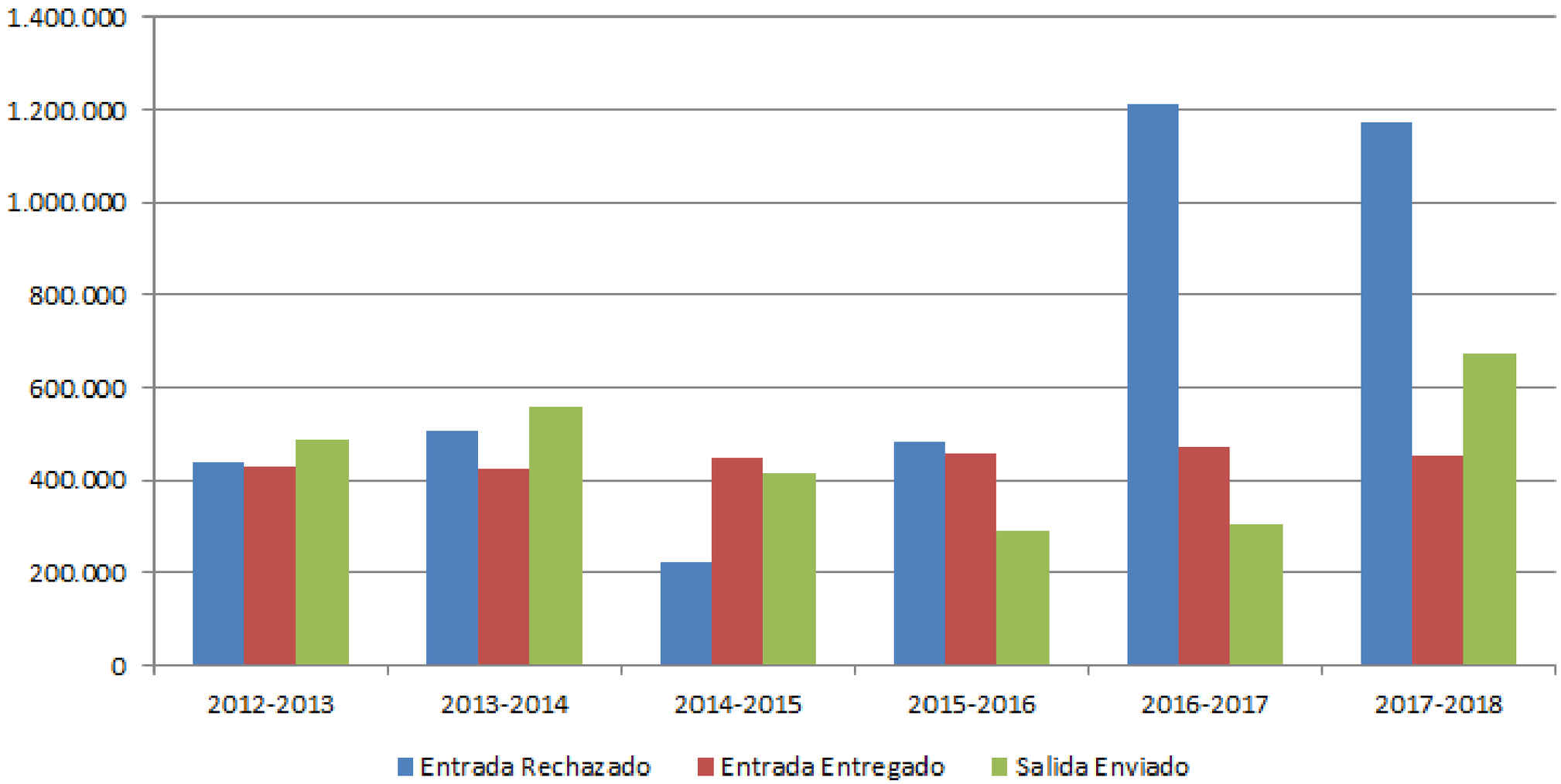
Condiciones y T'erminos del Servicio de localizaci'on de env'ios

La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede obtener mediante acuse de recibo o certificaci'on de servicios postales. Correos no se responsabiliza de los errores u omisi'on de informaci'on, por lo que advierte que no se adopten decisiones o acciones derivadas de la informaci'on obtenida por este servicio.

Haga clic aqu'i para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Tel'egrafos, S.A.

✓ Algunos datos.



✓ Medidas de protección.

- ❑ Utilización de contraseñas.
- ❑ Uso de redes seguras.
- ❑ Soportes de almacenamiento.
- ❑ Protección del equipo.
- ❑ Navegación segura.
- ❑ Copias de seguridad.
- ❑ Mesas limpias.

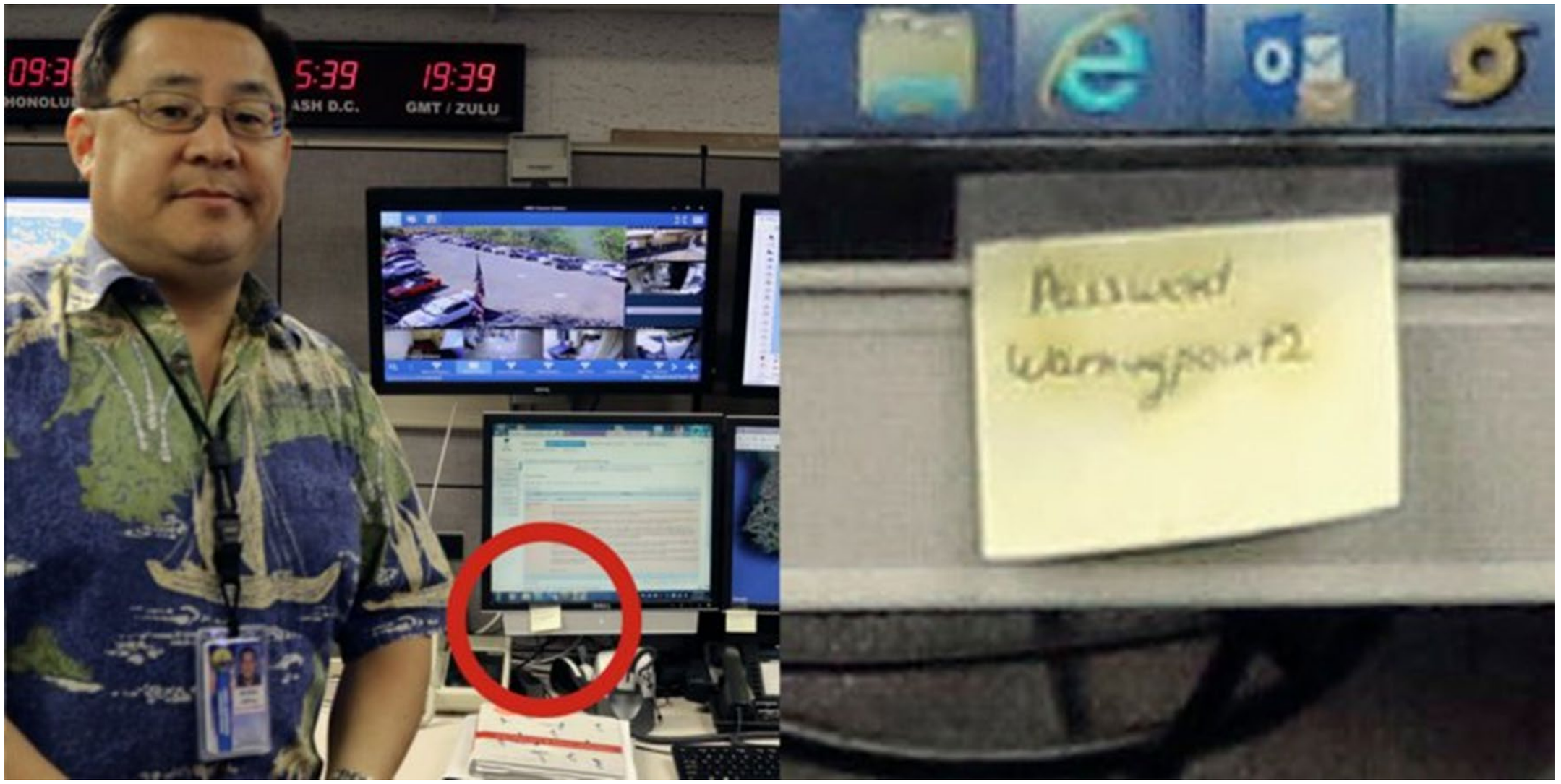
✓ Contraseñas robustas.

Cambia tus contraseñas periódicamente – http://micuenta.usj.es

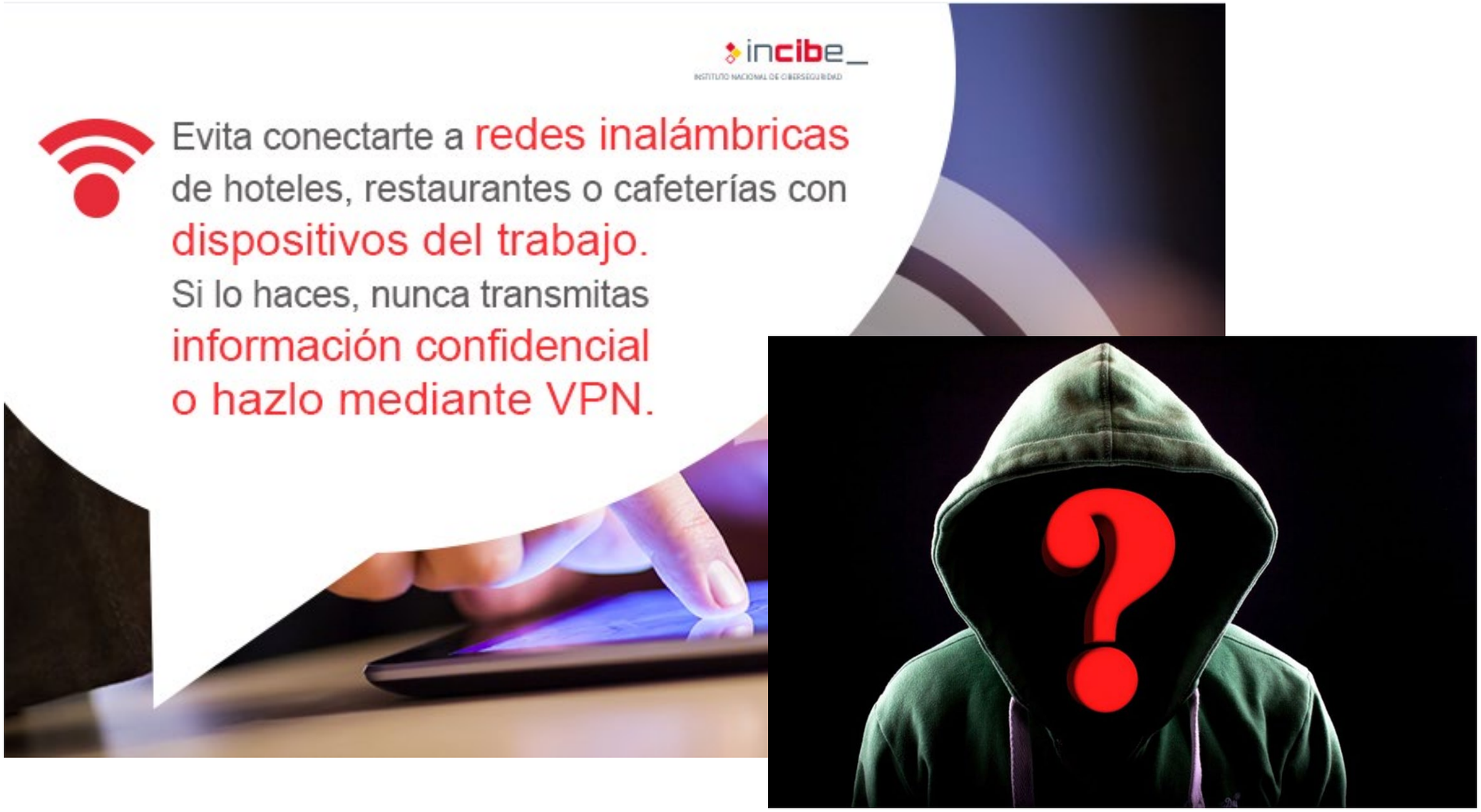
✓ Cómo crear una contraseña robusta.

- Deberán tener una longitud igual o superior a 8 caracteres e inferior a 13 caracteres.
- Deberán contener al menos una letra mayúscula, una minúscula, un número y un carácter especial de los siguientes: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~
- No deberá estar formada por un grupo de letras y otro grupo de números de forma consecutiva (ej. Carlos2018).
- La contraseña no deberá ser igual a ninguna de las 3 últimas contraseñas usadas.
- La contraseña deberá cambiarse periódicamente, o siempre que se entienda que haya podido ser comprometida.
- Utilizaremos la aplicación https://micuenta.usj.es.

✓ No anotes tus contraseñas en papel.



✓ Utiliza redes seguras.



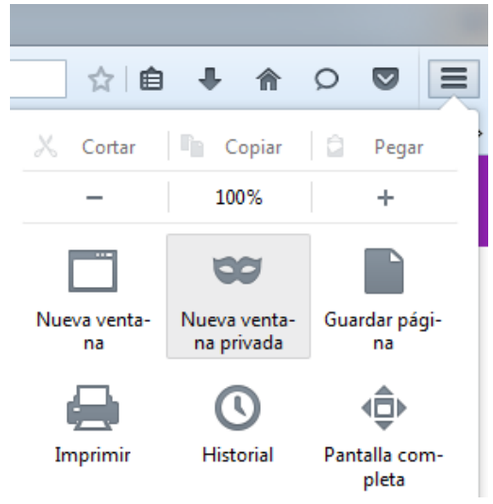
✓ Qué es una VPN.

✓ Soportes de almacenamiento.

✓ Protege tu equipo.

- Mantén actualizado el Sistema Operativo.
- Bloquea la pantalla de tu equipo cuando no estés en tu puesto: **Windows** + **L**
- Cuidado con la descarga de ficheros y el acceso a enlaces que lleguen a través del correo electrónico.
- Utiliza el cifrado de datos.
- Notifica cualquier incidente de seguridad.

✓ Navegación segura.



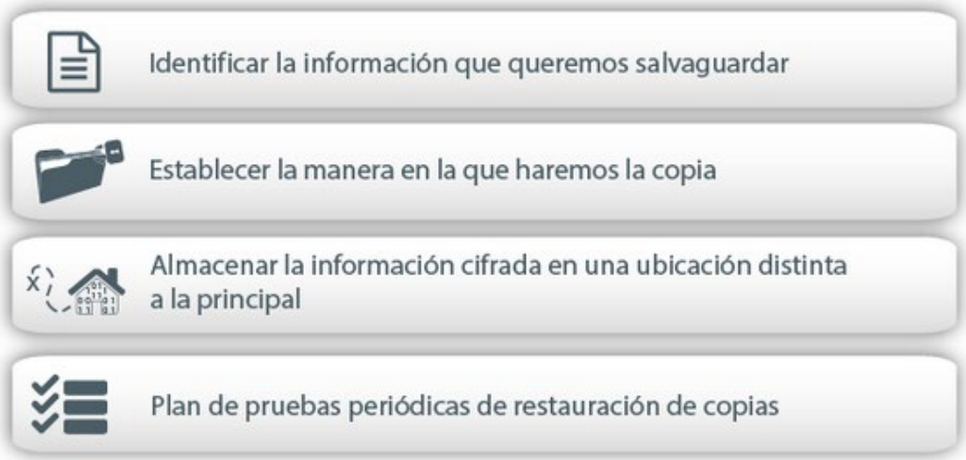
- Mantén el navegador actualizado.
- Elige complementos y plugins de confianza.
- Borra el historial de navegación periódicamente.
- Elimina las cookies.
- Navega en modo incógnito y por páginas seguras.

- Utiliza un gestor de contraseñas, no las almacenes en el navegador.
- Cierra siempre la sesión cuando salgas de una página en la que te hayas autenticado con usuario contraseña.

✓ Copias de seguridad.

- Microsoft OneDrive: https://portal.office.com/
- En dispositivos extraíbles. Cifrado.
- En recursos compartidos de la Universidad.
  - Servidor de Ficheros.
  - Vibox.

LOS RIESGOS más habituales que puede sufrir un soporte son pérdida, robo, rotura, destrucción o avería.



✓ Política de mesas limpias.

✓ Destrucción de documentación.

✓ Seguridad en el móvil.

- Habilita un sistema de bloqueo robusto. Doble factor.
- No descargues Apps desde sitios no oficiales.
- Evita la utilización de redes WIFI públicas.
- Habilita la protección antivirus y la encriptación.
- En caso de pérdida o robo comunícalo de inmediato al DSI. Lo bloquearemos.
- Encontrar mi teléfono: *Find my Android* - *Find my iPhone*.

✓ Consejos útiles.

No facilites credenciales através de correos electrónicos. Nosotros nunca te las pediremos.

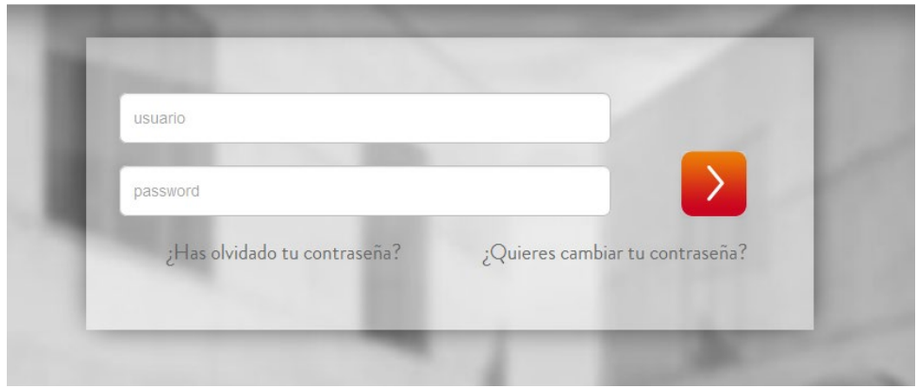
No respondas a correos sospechos. Si lo haces estás revelando tu identidad.

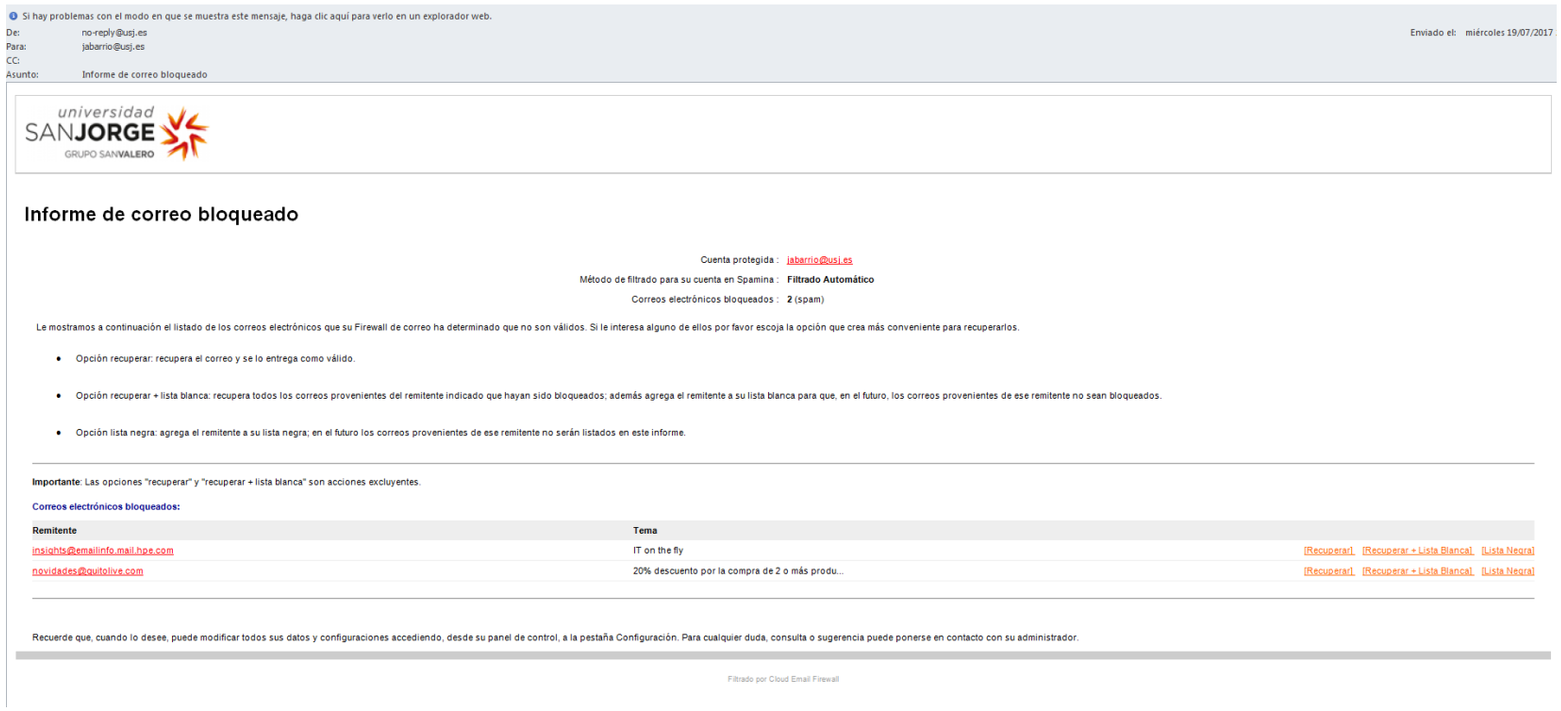
Cuidado con los enlaces que parecen de confianza (Google, Dropbox...)

Si tienes alguna duda consulta con el servicio de Soporte Técnico.

✓ Herramientas de seguridad USJ.

- ❑ Acceso seguro a las aplicaciones (https).
- ❑ Se requiere autenticación.
- ❑ Antivirus - Antimalware.
- ❑ Antispam.
- ❑ Cortafuegos.





Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

De: no-reply@usj.es
Para: jabarrio@usj.es
CC:
Asunto: Informe de correo bloqueado

Enviado el: miércoles 19/07/2017

Informe de correo bloqueado

Cuenta protegida : jabarrio@usj.es
Método de filtrado para su cuenta en Spamina : **Filtrado Automático**
Correos electrónicos bloqueados : **2** (spam)

Le mostramos a continuación el listado de los correos electrónicos que su Firewall de correo ha determinado que no son válidos. Si le interesa alguno de ellos por favor escoja la opción que crea más conveniente para recuperarlos.

- Opción recuperar: recupera el correo y se lo entrega como válido.
- Opción recuperar + lista blanca: recupera todos los correos provenientes del remitente indicado que hayan sido bloqueados; además agrega el remitente a su lista blanca para que, en el futuro, los correos provenientes de ese remitente no sean bloqueados.
- Opción lista negra: agrega el remitente a su lista negra; en el futuro los correos provenientes de ese remitente no serán listados en este informe.

Importante: Las opciones "recuperar" y "recuperar + lista blanca" son acciones excluyentes.

Correos electrónicos bloqueados:

Remitente	Tema	
insights@emailinfo.mail.hpe.com	IT on the fly	[Recuperar] [Recuperar + Lista Blanca] [Lista Negra]
novidades@quitolive.com	20% descuento por la compra de 2 o más produ...	[Recuperar] [Recuperar + Lista Blanca] [Lista Negra]

Recuerde que, cuando lo desee, puede modificar todos sus datos y configuraciones accediendo, desde su panel de control, a la pestaña Configuración. Para cualquier duda, consulta o sugerencia puede ponerse en contacto con su administrador.

Filtrado por Cloud Email Firewall

✓ Herramientas gratuitas.

- OSI - https://www.osi.es/es/herramientas-gratuitas
- INCIBE - https://www.incibe.es/protege-tu-empresa
- Algunas herramientas útiles:
  - Descubre si han hackeado tu cuenta de correo - https://breachalarm.com/
  - Servicio Antibotnet para tu red doméstica - https://www.osi.es/es/servicio-antibotnet
  - Detección de aplicaciones maliciosas en el móvil - https://www.osi.es/es/conan-mobile
  - Antivirus Online - http://www.virscan.org/language/en/
  - Gestor de contraseñas – Keepass - https://keepass.es/
  - Cifrado de Archivos/USB/Discos – Veracrypt - https://www.veracrypt.fr/en/Home.html

✓ Referencias y Guías de ayuda.

- OSI: Guía de Privacidad y Seguridad en Internet
  https://www.osi.es/sites/default/files/docs/guiaprivacidadseguridadinternet.pdf.

- INCIBE: Kit de Concienciación
  https://www.incibe.es/protege-tu-empresa/kit-concienciacion

Departamento de Sistemas de Información

www.usj.es

universidad SANJORGE GRUPO SANVALERO

Campus Universitario Villanueva de Gállego
Autov. A-23 Zaragoza - Huesca, Km 299
50830 • Villanueva de Gállego • Zaragoza
T. (34) 976 060 100 • F. (34) 976 077 581