Seminarios Web sobre Seguridad de la Información

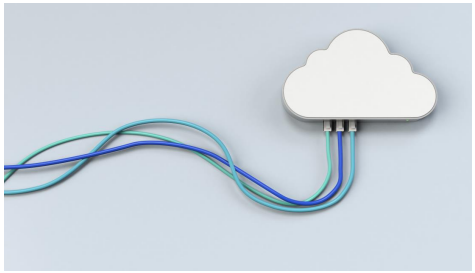
eclap

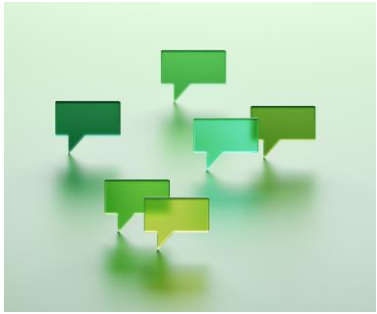
Junta de Castilla y León

Peligros en internet: Protégete a ti mismo y a la información que manejas

Objetivos

"Conocer las amenazas a las que se expone la información que tienen como origen en el uso de internet (navegación, correo electrónico y servicios en la nube) y la utilización de soportes de información, así como las medidas de seguridad a tener en cuenta"

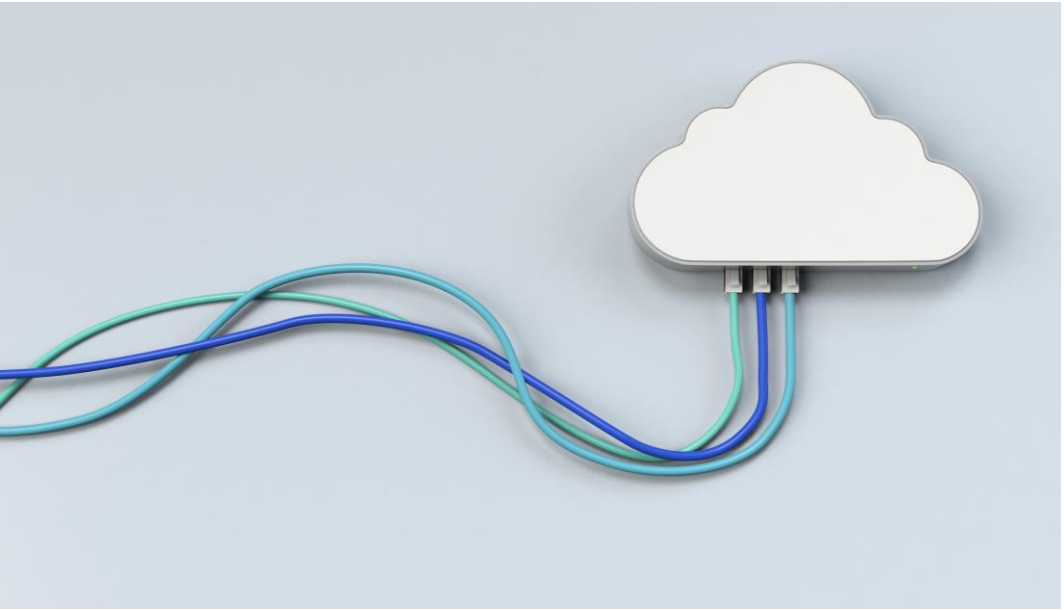




Índice del seminario

- Amenazas de la navegación en internet, correo electrónico y servicios en la nube
- Medidas de protección
- Buenas prácticas en el trabajo colaborativo
- Desinformación
- Buenas prácticas en el uso de las redes sociales
- Protección de los soportes de información (digitales o físicos)
- Prevención de fugas de datos
- Notificación de incidentes de seguridad

Amenazas de la navegación en internet, correo electrónico y servicios en la nube



La llegada de internet cambio por completo nuestra forma de trabajar e incluso de vivir pero también trajo consigo algunos peligros importantes

¿Qué amenazas puedo encontrarme cuando navego por internet y cómo puedo protegerme de ellas?

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Malware

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Malware

Virus

Programa cuyo objetivo es alterar el funcionamiento de un dispositivo. Para conseguirlo necesita la colaboración del usuario ejecutándolo en el equipo. Cuando se ejecuta infecta ficheros, toma el control y se propaga dañando el dispositivo. Cuidado con los ficheros .exe. Con nombre de otras aplicaciones para engañar.

Gusanos

El objetivo es el mismo que el del virus pero a diferencia de este no hace falta que lo ejecute el usuario ni modificar archivos para infectar el equipo. Se replica a sí mismo y se expande por las redes a las que está conectado el equipo. Difícil de detectar y provoca que ciertas tareas del equipo se vuelvan muy lentas. Otra forma de detectarlo es que se envían mensajes sin consentimiento.

Troyanos

Este tipo de malware se disfraza de archivos legítimos para que una vez se ejecutan se aprovechen de las vulnerabilidades de los equipos y puedan robar la información. No se propaga así mismo.

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Malware

Spyware

El objetivo es espiar y recolectar información de los usuarios o empresa sin su autorización. Suele actuar a escondidas y monitoriza y recopila datos sobre las acciones realizadas en el equipo, que tiene el disco duro, aplicaciones instaladas, historial de internet…

Adware

No daña al equipo sino que invade de publicidad el mismo. Lo habitual es que se presente mediante pop-up de ventanas emergentes mientras navegamos por internet. Podría considerarse spyware dado que puede recoletar y enviar datos personales.

Botnets

Programas de software creados para hacer operaciones de forma automática. Los robots webs o zombies cumplen las ordenes controladas por los ciberdelincuentes a distancia. Se forman redes de equipos infectados que pueden enviar spam, propagar malware o llevar a cabo ataques DDoS o criptominería.

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Malware

Criptominería

La criptominería o criptojacking son un tipo de código malicioso que secuestra el procesamiento inactivo del dispositivo víctima y lo usa para extraer criptomonedas. Una vez se secuestra el equipo víctima este es usado para hacer minado de criptomonedas mediante software de minería provocando una actividad del procesador muy alta.

Ramsonware

Secuestra los datos cifrándolos para pedir rescates económicos para poder ser liberados. Habitualmente pueden llegar al dispositivo a través de gusanos informáticos u otros software malicioso bloqueando el equipo mediante mensajes intimidatorios informando sobre ataque, cantidad solicitada y método de pago.

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Malware

Ramsonware

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Buenas prácticas para evitar ramsonware

Manual de buenas prácticas para evitar el ransomware

Uno de los mayores ataques a la disponibilidad es el ataque vírico conocido como ransomware, por el cual se nos cifran los datos y no se liberan hasta pagar un rescate, aunque actualmente no sólo se secuestran los datos, también los servicios. Y como novedad, este ataque se realiza simultáneamente con una filtración de datos hacia el exterior de la organización.

Copias de seguridad

Como **principal medida de prevención**, mantén regularmente una **copia actualizada de tus datos relevantes**. Puedes utilizar el espacio en red asignado a tu cuenta para posibilitar una copia regular de los documentos de tus sistemas de información, nunca en el mismo dispositivo.

Extensiones de fichero

Comprueba los **tipos reales de fichero** mediante la visualización completa de sus extensiones, para evitar ejecución de código dañino camuflado; en ocasiones los ficheros ejecutables se camuflan con icono de tipos de imagen o documentos ofimáticos.

Macros en documentos ofimáticos

No habilites las macros en los documentos de Microsoft Office y otras aplicaciones similares, y no desactivando la **vista protegida** de Office; como añadido, evita habilitar la edición si no es necesario.

Elementos sospechosos

No pinches en los **enlaces** ni descargues **adjuntos de correos spam o phishing**, prestando atención al remitente y contenido para verificar su legitimidad.

Fuentes confiables

Utiliza las **herramientas oficiales y los programas corporativos** a tu disposición, no instales programas desde fuentes no oficiales.

Navegación segura

Mantén una **conducta de navegación preventiva**, empleando los mínimos complementos y extensiones actualizadas, y no visitando webs sospechosas.

Antivirus

Comprueba que tu solución de antivirus corporativo se encuentra **activa y vigente**. También existen otras herramientas preventivas como microCLAUDIA que tendrás instaladas en tu puesto de usuario.

Ransomware

Del inglés *ransom* (rescate) y software; es un tipo de programa malicioso, de tipología virus, que al infectar un sistema encripta o bloquea los ficheros del mismo y solicita un rescate para liberarlos.

Tipología

Cifrador, encripta datos de usuario o incluso del sistema. Bloqueador, que impide el acceso a un dispositivo o un servicio online.

Clave de descifrado

Necesaria para el descifrado y conocida solo por el autor del *ransomware*, suele ser diferente para cada campaña de infección. Se solicita un pago, habitualmente en *criptomonedas*, aunque en gran parte de las ocasiones, no se libera la clave tras el pago.

Criptomonedas

Diferentes tipos de moneda digital, con mayor dificultad de rastreo, utilizadas en los secuestros de datos.

Actualizaciones

Verifica que el **sistema operativo se mantiene actualizado**; para ello, reinicia regularmente y así se aplicarán las actualizaciones aprobadas por la ACCyL. Igualmente con las aplicaciones y herramientas ofimáticas.

Dispositivo móvil

Si posees un **dispositivo móvil corporativo**, tanto de tipo iOS como Android, contempla las mismas buenas prácticas que en los puestos fijos de trabajo, con especial atención a las **unidades extraíbles**.

Incidencias

Ante procesos sospechosos de **cifrado de ficheros, desconecta tu puesto** de la red corporativa, para impedir la propagación del *ransomware* a las unidades de red y a otros puestos; y solicita una petición de incidencia código malicioso a tu **CAU**.

El uso de medios digitales deberá realizarse conforme a lo indicado en la política de seguridad de la ACCyL y la política de uso de los servicios de comunicaciones e informática

Junta de Castilla y León
Consejería de Fomento y Medio Ambiente
Dirección General de Telecomunicaciones y Transformación Digital

Ransoms más conocidos

CryptoLocker, Petya, NotPetya, CryptoWall, Jigsaw, TeslaCrypt, WannaCry, Mamba, Ryuk, REvil.

+ info

asista.jcyl.es
6116 (983 41 94 80)
www.jcyl.es/segurinfo
seguridadinformacion@jcyl.es

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Keyloggers

Tipo de software que se encarga de obtener y memorizar las pulsaciones que se realizan en un teclado consiguiendo así espiar de forma remota con el objetivo de obtener contraseñas de usuarios.

Hijackes o Secuestradores

Programa que secuestra a otro programa para usar sus derechos y modificar su comportamiento. El caso más habitual es el ataque a navegadores modificando la página de inicio y redireccionando las páginas sin que el usuario lo sepa. Pueden ser secuestros de IPs, páginas web, sesiones, navegadores…

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

¿Y cómo llegan estas amenazas a nuestros equipos?

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Navegación en internet

Correo electrónico

Junta de Castilla y León

Ingeniería Social

¿Qué es el la Ingeniería Social?

Conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

Este tipo de engaños pueden venir por diferentes medios como el correo electrónico, páginas web de internet, redes sociales, SMS, llamadas falsas…

La ingeniería social busca engañar al usuario de forma que una vez consigue la confianza del usuario lo manipula para que revele la información que necesita, instale un determinado software…

Existen diferentes ataques de ingeniería social que debemos conocer para poder prevenirlos. La mejor defensa ante los ataques de ingeniería social es el conocimiento y la educación para poder identificar estos ataques o sospechar ante cierta información recibida.

Junta de Castilla y León

Ingeniería Social

¿Cuáles son los principales ataques de Ingeniería Social?

Phishing

Comunicaciones disfrazadas de una fuente de confianza. Estos mensajes están diseñados para engañar a las víctimas y conseguir información personal, contraseñas, financiera… e incluso el poder instalar malware en nuestros equipos. El phishing por tanto es una suplantación de identidad para engañarnos y puede venir por correo electrónico, por SMS, llamadas telefónicas…

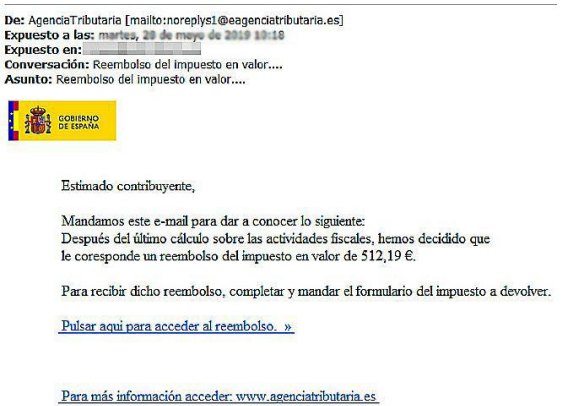
Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Ingeniería Social

¿Cuáles son los principales ataques de Ingeniería Social?

Phishing



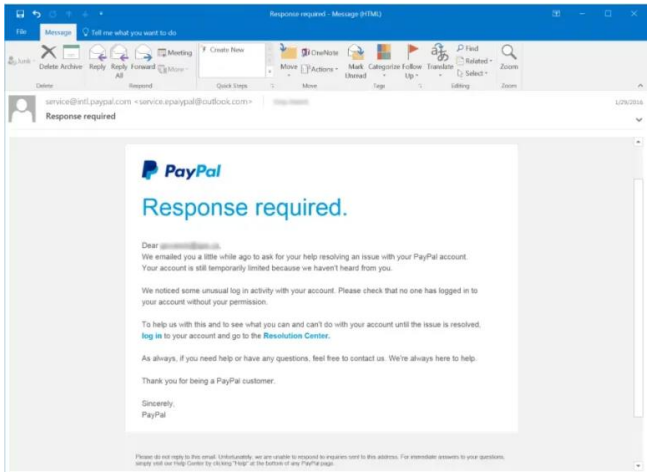
Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Ingeniería Social

¿Cuáles son los principales ataques de Ingeniería Social?

Phishing



Junta de Castilla y León

Ingeniería Social

¿Cuáles son los principales ataques de Ingeniería Social?

¿Cómo identificamos un ataque de Phishing?

- La oferta que recibimos es demasiado buena para ser verdad
- El mensaje suena aterrador, nos genera alarma o urgencia instándonos a actuar cuanto antes.
- Reconoce al remitente pero no suele interactuar con él o le pide algo inusual.
- Archivos adjuntos inesperados o extraños
- El mensaje contienen enlaces inesperados o extraños (pasa el curso por encima para ver la URL)

Junta de Castilla y León

Ingeniería Social

¿Cuáles son los principales ataques de Ingeniería Social?

¿Cómo nos protegemos del Phishing?

- No abrir mails de remitentes que no le sean familiares
- No haga clic en un enlace de un correo electrónico a menos que conozca a donde lleva exactamente
- Navegue manualmente hasta el enlace proporcionado escribiendo la dirección legítima en el navegador
- Busque el certificado digital de la web y asegúrese que si le pide información la web es HTTPS
- Selecciona parte del mail y busca en motor de búsqueda para ver si hay ataques parecidos

Junta de Castilla y León

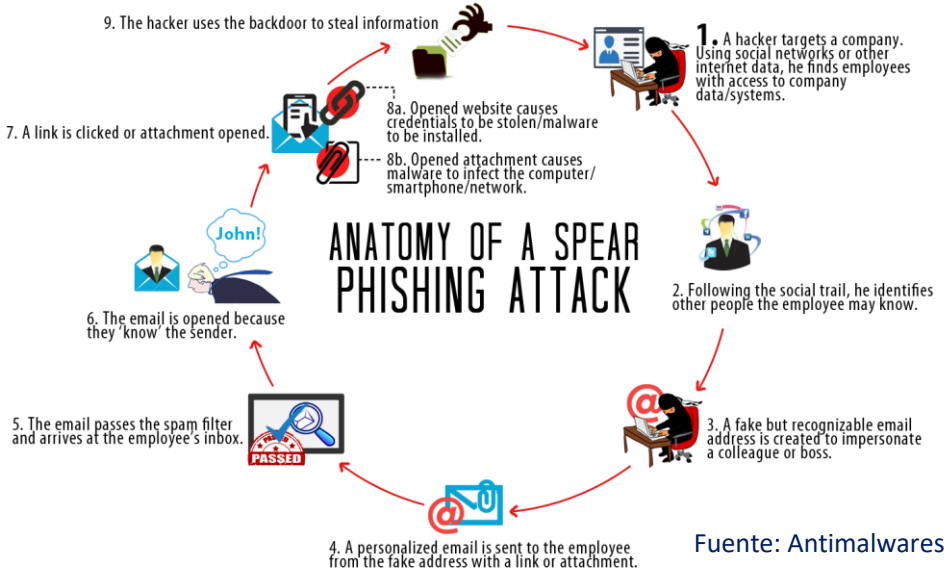
Ingeniería Social

¿Cuáles son los principales ataques de Ingeniería Social?

Spear Phishing

Es un tipo de phishing pero **dirigido a usuarios concretos o empresas concretas**. Están muy dirigidos y previamente han estudiado a quien recibe el mensaje para ser difícilmente detectables

Unido a este estaría el ***Whaling***, aún más dirigido hacia directivos u objetivos de alto valor y muy personalizado conociendo el sector.



Fuente: Antimalwares

Junta de Castilla y León

Ingeniería Social

¿Cuáles son los principales ataques de Ingeniería Social?

Smishing

El smishing es un tipo de ataque de phishing que llega en forma de **mensaje de texto o SMS**. Habitualmente, estos ataques piden a la víctima que realice alguna acción inmediata a través de enlaces maliciosos en los que hay que hacer clic o números de teléfono a los que hay que llamar. A menudo, solicitan a las víctimas que revelen información personal que los atacantes pueden usar en beneficio propio. Los ataques de smishing suelen transmitir una sensación de urgencia para que las víctimas actúen rápidamente y caigan en la trampa.

Junta de Castilla y León

Ingeniería Social

¿Cuáles son los principales ataques de Ingeniería Social?

Scareware

Malware que se vale del miedo de las personas para conseguir que descarguen falso software de seguridad o visiten un determinado sitio web. Puede aparecer en ventanas emergentes.

Pretexting

Crear un escenario falso o pretexto para engañar a las víctimas. Lleva una investigación previa para ser más creíble. Debemos tener especial cuidado con la información confidencial que compartimos y la urgencia.

Honey Trap

Es una situación en la que el atacante atrae a la víctima a una situación sexual vulnerable para realizar sextorsión u otro tipo de chantajes. Cuidado con los mensajes de que nos han estado observando a través de la cámara web.

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Spam

Consiste en el envío de correo electrónico publicitario de forma masiva a cualquier dirección de correo electrónico, cuya finalidad es vender sus productos. Los perjuicios que nos ocasionan es la saturación de los servicios de correo y la ocultación de otros correos maliciosos.

Junta de Castilla y León

Fraudes Online

¿Existen más fraudes online?

Tiendas online fraudulentas

Falsos préstamos

Falsos alquileres

Falsas ofertas de empleo

…

Existen diferentes situaciones en las que podemos acceder a fraudes online por lo que debemos estar realmente atentos a

- ¿Qué nos ofrecen? Desconfiar de bajos precios, intereses bajos…
- Revisar ortografía y gramática del anuncio y la web
- Investigar a quien nos ofrece el servicio y comprobar que los datos no han sido utilizados en otras estafas
- Cuidado con los métodos de pago y con las excusas o problemas

Junta de Castilla y León

Fraudes Online

¿Existen más fraudes online?

Falso soporte técnico

Habitualmente realizado a través de ventanas emergentes indicando que el equipo está infectado y llamemos a un número falso de soporte o bien por llamadas de falsos soportes por teléfono. Petición para instalar un programa para conectarse al ordenador y desinfestarlo remotamente.

- Actualizaciones de seguridad
- Restablecer el dispositivo
- Desinstalar apps que nos hayan indicado
- Cambiar contraseñas
- Reportar incidente

Junta de Castilla y León

Fraudes Online

¿Existen más fraudes online?

Perfiles falsos y suplantación de identidad en internet

Creación de perfiles falsos en redes sociales o plataformas haciéndose pasar por nosotros a través de datos obtenidos por internet.

- Cuidado con la información publicada en internet
- Hacer egosurfing periódicamente
- Recopilar pruebas
- Contactar con la red social o app y pedir el borrado de nuestros datos
- Gestionar adecuadamente la privacidad en redes sociales
- Cuidado con aceptar peticiones de desconocidos
- Denunciarlo

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Robos y Suplantación de Identidad

Los robos de identidad comienzan con la recopilación de información en internet que hemos ido añadiendo en diferentes plataformas y que pueden generar un perfil nuestro bastante detallado o bien obtenidos por técnicas de ingeniería social.

Retiros bancarios o compras que no se identifican

Faltan facturas o mails…

Cobros de deudas que no identificamos

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Buenas prácticas para evitar Suplantación de Identidad

Manual de buenas prácticas en prevención de suplantación de identidad

Una de las amenazas más frecuentes es la suplantación de entidades que pueden ser organizaciones o personas físicas, pudiendo ser suplantados nosotros mismos, y por ello debemos cuidar que nuestra información difundida sea mínima y sólo la necesaria.

Prevención

Utiliza la **seguridad y la prevención por defecto**, asegurando robustamente tus credenciales y contraseñas según la política de seguridad, y con varias capas de protección. Navega en sitios seguros. Evita redes wi-fi públicas. **Encripta la información** sensible en tus dispositivos.

Cuentas

No intercambies ni prestes tu cuenta de acceso de la ACCyL. No compartas las claves de acceso a tu ordenador ni a las aplicaciones para tu trabajo. Cada usuario es responsable de las acciones que se realicen con la cuenta que se le haya proporcionado o sus aplicaciones.

Políticas de seguridad y de uso

La ACCyL, al igual que las organizaciones con considerable tamaño y responsabilidad, tiene una **política de seguridad de la información**, y otros términos de servicio. Comprueba las políticas de la ACCyL así como las políticas de las empresas con las que te relaciones.

Reputación

Intercambia información sólo con **compañías y socios de reputación probada**. Antes de proveer cualquier información, como el correo o la cuenta ACCyL, el teléfono, etc. asegúrate de estar comunicándote con la entidad con la que debes hacerlo, sobre todo en comunicaciones de tipo informáticas o digitales.

Difusión controlada

Reduce la **información propia que publicitas**; no compartas datos de acceso o profesionales, u otros datos sensibles, en cualquier entorno no laboral. Usa **perfiles privados**.

Spoofing

Suplantación de características de una identidad, a través de la red, llevada a cabo por un intruso generalmente con fines de malware o de investigación. Los ataques, mediante falsas webs, a través de este tipo de técnicas ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

Phishing, vishing, smishing

Busca obtener la información personal o confidencial de los usuarios por medio del engaño la identidad digital de una entidad o persona de confianza en su medio de comunicación. Tipos: phishing (correo electrónico), vishing (llamada de voz), smishing (mensaje de texto SMS).

Scam

Tipo de fraude destinado a conseguir que una persona o grupo de personas entreguen patrimonio, utilizando suplantación junto con falsas promesas de beneficios económicos.

Diferenciación

Utiliza **diferente usuario y clave en tus cuentas personales**, como pueden ser redes sociales y otros sitios web. Esta información, la personal y la laboral, no debería ser utilizada de forma simultánea y será utilizada para distintos fines.

Actualizaciones y aplicaciones

Mantén **actualizado** y comprueba la **vigencia** de tu antivirus corporativo y los productos de seguridad análogos que tengas en tu equipo. Comprueba los permisos de aplicaciones.

Actividad y suscripciones

Comprueba tu actividad regularmente, revisando regularmente tu correo electrónico así como tus unidades de red para asegurar que no hay ninguna actividad sospechosa. Procura suscribirte y crear cuentas únicamente a los boletines y sitios web necesarios.

Identificación

Ante cualquier duda, **verifica el emisor** que te envía una información, llamada o correo, es quien dice ser, contactando por otro medio de comunicación. Puedes utilizar **firma digital** con certificado para asegurar la identidad tanto de emisor como de destinatarios.

Incidentes o situaciones anómalas

Si detectas algún **comportamiento sospechoso**, notifícalo a tu CAU; para los incidentes que conlleven una brecha de información y datos personales, informa adicionalmente al Responsable de Seguridad y al Delegado de Protección de Datos en tu organismo.

El uso de medios digitales deberá realizarse conforme a lo indicado en la política de seguridad de la ACCyL y la política de uso de los servicios de comunicaciones e informática

Junta de Castilla y León
Consejería de Fomento y Medio Ambiente
Dirección General de Telecomunicaciones y Transformación Digital

de beneficios económicos.

Pharming

Técnica mediante la que se envía, para un enlace web válido, la navegación de usuario a páginas falsificadas; bien mediante un malware en el puesto de usuario, o bien mediante modificación del servidor de los proveedores de servicio de red.

SIM swapping

Suplantación para solicitar duplicado de nuestra tarjeta SIM de telefonía, con la que pasan a recibir nuestras llamadas y mensajes de texto; utilizado sobre todo para los códigos de un solo uso en cuentas con doble autenticación.

+ info
asista.jcyl.es
6116 (983 41 94 80)
www.jcyl.es/segurinfo
seguridadinformacion@jcyl.es

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Suplantación de identidad y Fraude del CEO

Fraude del CEO

Técnica mediante la que se suplanta un alto cargo de la organización, con el objetivo de engañar a los empleados con acceso a los recursos económicos (Europol).

Business Email Compromise

Compromiso de correo electrónico de empresa. Suplantación de un tercero mediante la cual se nos modifica, o se nos da nueva, cuenta bancaria a la que tenemos que hacer un ingreso. Muy utilizado para suplantar proveedores.

Fraude de RRHH

En este caso se suplanta a un trabajador y se solicita un cambio de cuenta bancaria donde se produce el ingreso de la nómina

Ingeniería Social

Mecanismos, o esquemas de engaño, destinados a hacer que las personas lleven a cabo comportamientos que les van a perjudicar.

Scam

Estafa. Tipo de fraude destinado a conseguir que una persona o grupo de personas entreguen dinero, bajo falsas promesas de beneficios.

Phishing

Similares a correos *spam*, suplantan a entidades conocidas o también personas, y solicitan que el usuario proporcione datos personales o de credenciales.

Junta de Castilla y León

Fraude del SEO

¿Qué es el SEO?

El SEO (*Search Engine Optimization*) u *Optimización para motores de búsqueda* son una serie de técnicas y estrategias implementadas en una web o blog para que cuando busquemos en buscadores aparezcan en los primeros resultados.

El fraude del SEO consiste en la aplicación de estas técnicas por parte de estafadores para posicionarse en los resultados por encima de las páginas reales para atraer a las víctimas

Los Administradores de páginas web deben tener esto en cuenta y posicionar bien sus webs para evitar ser "sobrepasados" por otras web y que usuarios entren en estas y puedan ser estafados

Como usuarios debemos estar siempre atentos a que web visitamos, su URL y que realmente sea la página web auténtica.

Junta de Castilla y León

QRishing

¿Qué es el QRishing?

El uso del los códigos QR son cada vez más habitualmente y más desde la pandemia que obligó en algún caso su uso para cartas de restaurantes, viajes, pasaportes COVID, conexión a WIFIs…

QRishing es la combinación de los códigos QR con el phishing. Así, se utilizan los códigos QR con el fin de engañarnos de diferentes formas:

- *Llevarnos a una web suplantando la identidad de una empresa y solicitando información.*
- *Descarga de malware o inyección de códigos maliciosos a través del escaneo de ese QR*
- *Ingeniería social par secuestrar cuentas que acepten la función de inicio por código QR. De esta forma capturan nuestras credenciales y la sesión de la víctima y pueden acceder a la información (QRLJacking)*

QRLJacking

Junta de Castilla y León

QRishing

¿Cómo podemos evitar el QRishing?

Comprobar la web a la que redirige el código QR. Utilicemos apps que permitan consultar la URL.

- *Deshabilitar apertura automática de enlaces al escanear el código QR.*
- *Estar muy atentos a qué nos facilita ese código QR y desconfiar*
- Como negocio comprobar que los códigos QR no han sido modificados.
- *Utilizar un generador de códigos con la suficiente seguridad*

Junta de Castilla y León

Acortadores URL

¿Qué son los acortadores URL y por qué debemos tener cuidado?

Un acortador de URLs nos permite que un enlace de muchos caracteres se pueda reemplazar por una dirección web con muchos menos que el original y nos dirige a la misma página web. Son muy utilizados en sistemas donde no se permiten muchos caracteres como SMS u otras apps.

Este tipo de enlaces está siendo utilizados para dirigirnos a webs diferentes de la original e intentar el fraude a través de esa página web de destino aprovechando que no sabemos la URL original

Junta de Castilla y León

Acortadores URL

¿Cómo podemos evitarlo?

- *Fijarnos bien en la fuente del mensaje en el que viene el enlace acortado*
- *Cuidado con los enlaces acortados e intentar utilizar servicios que nos permitan conocer la web original (getlinkinfo.com)*
- *Podemos analizar la URL a través de analizadores online o de los propios antivirus*
- *Existen también complementos de navegadores que nos permiten conocer las direcciones originales de enlaces acortados*
- *Abrirlo en un entorno seguro en el que no tengamos otras cuentas abiertas*

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Normas de navegación web

- Se podrán definir **diferentes perfiles de navegación web** teniendo acceso los usuarios a destinos concretos y requiriendo autorización el resto.
- Habrá **destinos no autorizados** por considerarse peligrosos o no relacionados con ACCyL.
- Desde el respeto a la intimidad y protección de datos del usuario, se podrá **acceder a la navegación web con riesgos de seguridad** con el fin de garantizar integridad y continuidad de prestación de servicios públicos.
- **Cuidado con las WIFI** abiertas
- **No olvidemos cerrar sesi**ón si hemos entrado en un sitio que nos ha requerido registro
- **Evita guardar contraseñas en el navegador** cuanto te da la opción de recordar contraseña

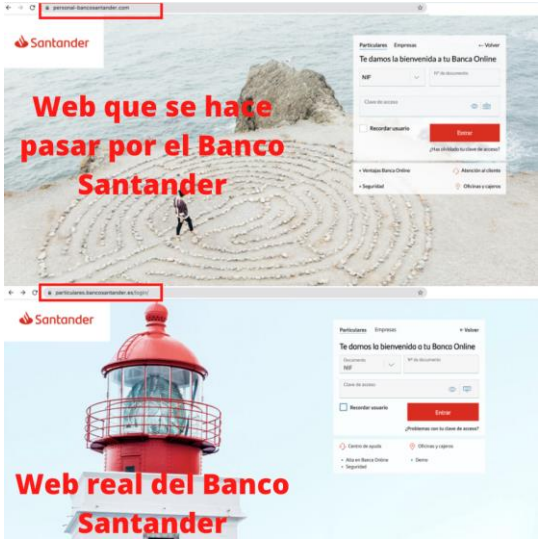
KeePass

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Normas de navegación web

- Siempre debemos **comprobar qué página web estamos visitando**. A través de phishing y otras técnicas nos intentarán engañar y llevarnos a webs que se hacen pasar por organismos y engañarnos
- Mantener **navegador actualizado** para evitar exploits al visitar webs
- Fijarnos siempre en la URL de la web que visitamos y que sea **HTTPS**
- Revisa periódicamente **plugins, extensiones y seguridad del navegador.** Cuidado con la instalación de complementos y extensiones, se debe evitar a no ser que sean de fuentes oficiales. Deshabilitar los sospechosos.
- Cuando se requiere autenticación de acceso priorizar **certificados electró**nicos en vez de usuario y contraseña
- Cerrar sesión al finalizar el trabajo.



Junta de Castilla y León

NOR 1220 – Seguridad de las Comunicaciones

8.3. Protección de la navegación web

El acceso de los usuarios internos a la navegación por Internet se protegerá frente a las amenazas que le son propias.

Podrán definirse **diferentes perfiles de navegación web**. Todos los usuarios tendrán acceso a unos destinos concretos. El acceso a destinos no incluidos entre los anteriores requerirá de autorización. **Habrá destinos no autorizados por considerarse peligrosos o no relacionados con la actividad de la ACCyL.**

Respetando el derecho a la intimidad de los trabajadores, la protección de los datos personales y el secreto de las comunicaciones, la ACCyL podrá **acceder a la navegación web con especiales riesgos de seguridad, incluidas las comunicaciones que estén cifradas, para garantizar la integridad y la continuidad en la prestación de los servicios públicos**. Con la misma finalidad, dichos contenidos podrán ser capturados y almacenados para su análisis posterior.

Se **formará y concienciará a los empleados** en el uso adecuado de la navegación web fomentando el uso seguro y alertando de usos incorrectos

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

¿Ya hemos visto varias amenazas relacionadas con el correo electrónico

También hemos visto buenas prácticas a tener en cuenta para evitar caer en estas amenazas

¿Existen reglas y normativas en ACCyL sobre el uso del correo electrónico?

Junta de Castilla y León

NOR 1110 – Condiciones de uso

(…)

5.12. Uso del correo corporativo

Las unidades competentes para la prestación de los servicios corporativos de informática y de comunicaciones suministrará a cada usuario una **dirección individual de correo electrónico asociada a su cuenta de usuario**. Cada usuario será responsable de las actividades realizadas a través de las cuentas de correo electrónico de las que es titular.

Únicamente podrán utilizarse **clientes de correo electrónico** autorizados por la ACCyL.

A los efectos de evitar que los servidores queden colapsados por su uso inadecuado o que puedan resultar dañados, los usuarios **deberán abstenerse de enviar mensajes masivos o con ficheros adjuntos de gran tamaño**.

No está autorizado el envío de correos que contengan información con datos sensibles o confidenciales sin proteger. En el caso de que sea necesario el envío de esta información y el usuario no tenga los conocimientos necesarios, el usuario deberá ponerse en contacto con su CAU o a los centros de servicios especializados que se habiliten, que le proporcionará el apoyo y los mecanismos necesarios para el envío de este tipo de información.

Junta de Castilla y León

NOR 1110 – Condiciones de uso

(…)

5.12. Uso del correo corporativo

Se **prohíbe a los usuarios el reenvío automático del correo corporativo a cuentas externas**, así como interceptar, leer, borrar, enviar, copiar o modificar el contenido de los mensajes de correo electrónico de otros usuarios.

Se **prohíbe el uso abusivo del correo electrónico**, propagación de cadenas de correos, envío de correos ofensivos y el intercambio no autorizado de contenidos protegidos por la legislación de propiedad intelectual. Asimismo, se prohíbe el envío de cualquier clase de código malicioso o dañino que puedan causar perjuicios en los sistemas de información

Junta de Castilla y León

NOR 1220 – Seguridad de las comuniones

8.1. Protección del correo electrónico

Se habilitará protección ante las amenazas más comunes del correo electrónico como spam, phishing, adjuntos con programas maliciosos y suplantación de identidad.

Mediante los mecanismos de control y protección adecuados, **se podrá limitar el envío y recepción de correos en base a detección de patrones anormales de comportamiento, uso abusivo o existencia de programas maliciosos.**

Se **formará y concienciará a los empleados** en el uso adecuado del correo electrónico.

Junta de Castilla y León

NOR 1230 - Normas de uso del correo electrónico

Uso de correo corporativo

- Las unidades competentes para la prestación de servicios corporativos de informática y comunicaciones suministrarán a cada usuario una **dirección de correo individual asociada a la cuenta de usuario**.
- Cada usuario es **responsable de sus correo electrónico y las actividades realizadas** con el mismo.
- Sólo podrán utilizarse **clientes de correo electrónico autorizados por ACCyL**.
- Se debe **evitar el envío de correos con adjuntos de gran tamaño o el envío de correos masivos así como el uso abusivo** (correo ofensivo, cadenas de correos…)
- **Prohibido el envío de correos con información sensible o confidencial sin proteger**.
- **Prohibido el reenvío automático de correo corporativo a cuentas externas así como leer, interceptar, borrar, enviar, copiar… el contenido de los correos de otros usuarios**.

Junta de Castilla y León

NOR 1230 - Normas de uso del correo electrónico

- Se deberán utilizar los clientes de correo autorizados y junto a los mensajes pueden transmitirse ficheros adjuntos a excepción de ejecutables y ficheros de código y scripts.
- Las **direcciones de correo de ACCyL son de ámbito laboral y para uso profesional únicamente**.
- La **cuenta de correo identificativa es individual y el usuario es responsable de las actividades realizadas**. El acceso externo mediante dispositivo móvil deberá ser autorizado.
- **Correos colaborativos tendrán protección adecuada** y sus miembros estarán identificados.
- Se deberá tener una **protección y credenciales suficientemente seguras y robustas**
- Se permite **recepción y envío de información sensible o confidencial con mecanismos de protección adecuadas (cifrado)**
- **Evitar almacenamiento excesivo de correos y cumplimiento de periodos de retención**

Junta de Castilla y León

NOR 1230 - Normas de uso del correo electrónico

➢ Cuando envío un Correo Electrónico

Antes de enviar un correo electrónico, **verifica los destinatarios** para comprobar que son los adecuados y mantén ocultas (CCO) aquellas direcciones que no implicadas directamente

➢ Cuando recibo un Correo Electrónico

Si recibes un mail, asegúrate de la **identidad del remitente** antes de abrir el mensaje

Elimina sin responder los correos spam, suplantación de identidad, sospechosos e ignora enlaces fuera de lo habitual o adjuntos sospechosos

➢ La **configuración del correo electrónico** se hará siempre primando seguridad y protección en la apertura

Junta de Castilla y León

NOR 1230 - Normas de uso del correo electrónico

Usos Prohibidos

- **Suscripción y comunicación** de correo electrónico corporativo a **servicios no relacionados con la actividad profesional**
- **Prohibido redirigir cuentas corporativas** de correo a correos externos de ACCyL salvo por autorización expresa
- Queda **prohibido interceptar, leer, borrar, enviar, copiar o modificar el contenido de los mensajes** de correo electrónico de otros usuarios. Se prohíbe en especial la suplantación de identidad tanto en el envío como en la gestión de mensajes de correo electrónico.
- **Prohibida la conexión a servidores de correo no corporativos**
- **Prohibida la utilización de herramientas o sistemas que intenten ocultar la identidad del emisor**
- **Prohibido el uso abusivo de correo electrónico**, envíos masivos, exceso de adjuntos, envío de malware, contenidos ofensivos o propagación de cadenas de correos.

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Junta de Castilla y León

Manual de buenas prácticas para el uso seguro del correo electrónico

El correo electrónico es hoy el principal punto de entrada en cualquier organización para los enlaces y software dañino, y con el que extraer información de forma no autorizada. Su uso adecuado es muy dependiente de la concienciación en seguridad de la información.

Procedencia

No confíes únicamente en el nombre del remitente y verifica si el propio **@dominio del correo** recibido es de confianza, como 'jcyl.es'. Ante dudas, por otro medio de comunicación, **verifica la legitimidad** de un correo aunque sea de un contacto conocido o de la organización.

Indicios sospechosos

Desconfía si presenta cualquier **síntoma o patrón fuera de lo considerado estándar** o habitual. Por ejemplo, sólo deberá proceder de una única dirección de correo, no solicitar información inusual o la descarga/ejecución de un adjunto sospechoso de forma excesiva.

Enlaces

Comprueba a qué web apunta, **evitando hacer clic directamente** desde el propio cliente de correo; escribe de forma manual en la barra del navegador. Si el enlace es de una web sospechosa o desconocida, es recomendable buscar antes información web relacionada.

Ficheros adjuntos

No descargues un fichero adjunto procedente de un correo con remitente desconocido, o con indicios sospechosos. Guarda manualmente el adjunto y analízalo con la **solución antivirus** en primer lugar. Asegúrate de su extensión (Word, Excel, etc.), no sólo por el icono visualizado.

Envíos y respuestas

No respondas a **comunicaciones sospechosas** ni proporciones datos personales o de tu cuenta de acceso. Utiliza **CCO** 'Con Copia Oculta' para comunicaciones a varios destinatarios.

Macros de productos *office*

No habilites las macros de documentos ofimáticos sospechosos, incluso si el propio fichero así lo solicita desde el visor incluido en la aplicación cliente de correo. Habilitando el **modo edición** sin necesidad, anulamos la primera protección que nos ofrece la propia herramienta.

Almacén de correos PST, OST

Archivos de datos de correo que se almacenan en el equipo (PST) o en el servidor de correo (OST), conteniendo mensajes y otros elementos.

Spam

Correo propaganda o basura. Son mensajes no deseados procedentes de remitentes desconocidos. Si solicitas ser borrado de los destinatarios, lo único que haces es confirmar que la dirección de correo existe; no se debe responder nunca a un mensaje de este tipo.

Phishing

Correos en los que se suplanta a entidades conocidas, también personas, y solicitan que el usuario proporcione datos personales o de credenciales tanto de cuentas laborales como personales, mediante enlace a página web falsa para verificar algún dato.

Ingeniería social

Conjunto de técnicas psicológicas que permiten engañar y persuadir a personas aprovechando la buena voluntad, para conocer cualquier clase de información, como credenciales, o conseguir que realice alguna acción.

Previsualización del contenido

Para una mayor seguridad, **desactiva la visualización automática de correos**, habitualmente en la configuración de Vista del Panel de Lectura. La previsualización de adjuntos, habitualmente en configuración del Centro de confianza para Tratamiento de datos adjuntos.

Cifrado de información y contraseña del almacén de correo

Cifra los mensajes de correo que contengan **información clasificada o sensible**, dependiendo del sistema origen y nivel del Esquema Nacional de Seguridad al que pertenezca. Utiliza **contraseñas robustas** para el acceso al correo electrónico si has creado tus 'Archivos de datos' locales; las contraseñas deberán ser periódicamente renovadas.

Actualizaciones

Reinicia el equipo regularmente para que se apliquen las **actualizaciones corporativas aprobadas**, teniendo así siempre actualizado el sistema operativo, las aplicaciones ofimáticas incluido el gestor correo y el navegador (con sus extensiones), y activo el antivirus corporativo.

Correos en las incidencias

Cuando abras una incidencia en tu CAU recuerda **adjuntar el correo sospechoso recibido**, en consonancia con el procedimiento corporativo de notificación de incidentes.

Lista masiva de direcciones

Listas semipúblicas de información reunida a través de rastreo en Internet, las redes sociales, los foros, así como brechas de datos de empresas. Para la mayoría no se puede solicitar la eliminación de nuestros datos y desaparecen solas.

+ info

asista.jcyl.es
6116 (983 41 94 80)
www.jcyl.es/segurinfo
seguridadinformacion@jcyl.es

El uso de medios digitales deberá realizarse conforme a lo indicado en la política de seguridad de la ACCyL y la política de uso de los servicios de comunicaciones e informática

Junta de Castilla y León
Consejería de Fomento y Medio Ambiente
Dirección General de Telecomunicaciones y Transformación Digital

Amenazas de la navegación en internet, correo electrónico y servicios en la nube

Buenas prácticas en el trabajo colaborativo

¿Cómo colaboro o trabajo con terceros si estoy llevando a cabo teletrabajo?

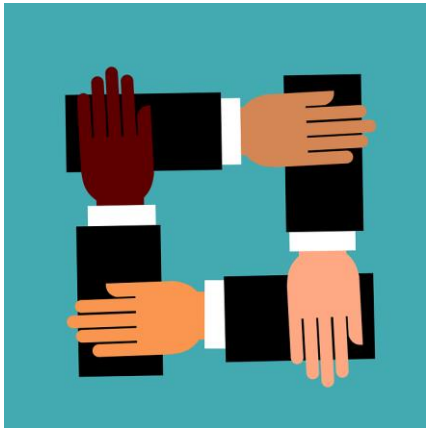
¿Qué aspectos debo tener en cuenta cuando llevo a cabo trabajo colaborativo?

Las herramientas colaborativas son fundamentales y debemos conocerlas y aprender a utilizarlas

Junta de Castilla y León

Buenas prácticas en el trabajo colaborativo

- No debemos compartir nuestras cuentas con otros terceros para poder hacer trabajo colaborativo.
- Se dispone de diferentes **unidades de red** para trabajar en equipo dentro de tu Servicio o edificio.
  - Unidad de Departamento: Unidad G:
  - Unidad de Consejería o Edificio: Unidad J:
- La unidad individual es la Unidad N y sobre ella se hacen copias de seguridad. No debemos introducir información personal en las mismas. El trabajo colaborativo no se ubicará en esta unidad.
- Para no parar procedimientos se puede añadir **respuesta automática al correo** durante ausencias programadas o redirigir los correos a compañeros. En Copia compañeros que intervengan en trámites.



Buenas prácticas en el trabajo colaborativo

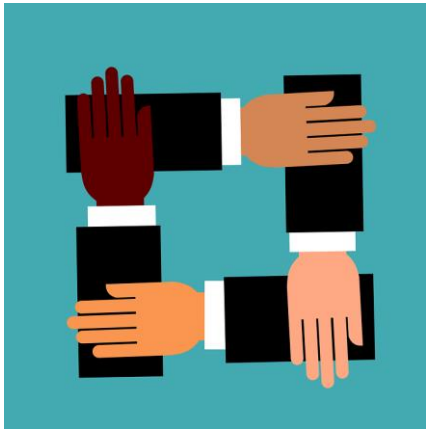
- Para la distribución de correos con información que deba ser rápidamente gestionada se dispone de las **listas de distribución**. Se debe tramitar a través del Dpto la petición.

- Utiliza las impresoras, escáneres… evitando aquellos conectados directamente a un equipo concreto pudiéndose acceder así desde cualquier puesto. Con las credenciales de JCYL podemos iniciar sesión en cualquier equipo.

- Debemos utilizar únicamente **herramientas colaborativas de ACCyL como JCYL Transfer, mensajería corporativa… Evitar herramientas no autorizadas**

- Las videoconferencias se llevarán a cabo por la **herramienta propia y los enlaces se compartirán sólo a los participantes**. Toda reunión tendrá un moderador y debemos cuidar el fondo de imagen.

- **Evitemos guardar información laboral en soportes extraíbles y no conectes USBs sospechosos no proporcionados por ACCyL**



Buenas prácticas en el trabajo colaborativo

Junta de Castilla y León

Transferencia de archivos pesados de forma segura

JCyL Transfer

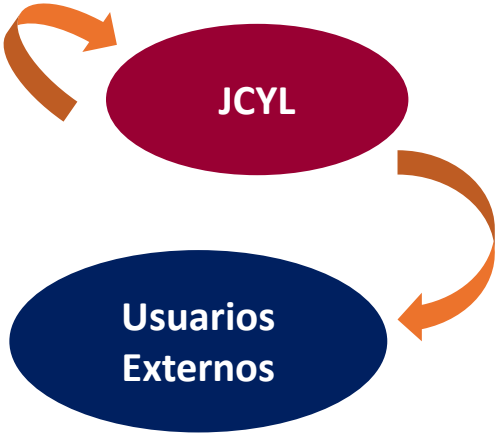
Si alguna vez necesitamos enviar archivos de gran tamaño podemos hacerlo a través de la herramienta JCylTransfer a la cual se puede acceder a través de https://jcyltransfer.jcyl.es

Esta herramienta está basada una herramienta generalista como We Transfer si bien, sólo pueden SUBIR contenidos a la misma usuarios de Junta de Castilla y León

Nos servirá para intercambiar información:

- Entre diferentes unidades administrativas de JCYL
- Con usuarios o empresas externas (sólo descargar la información)

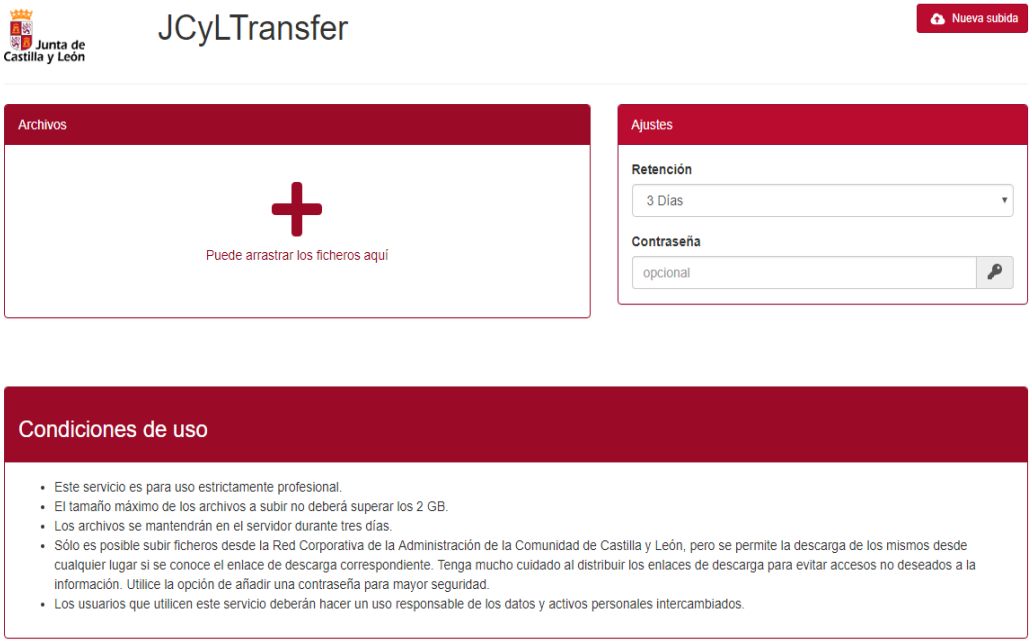
Accesible desde Internet Explorer, Chrome, Firefox y Edge.



Junta de Castilla y León

Transferencia de archivos pesados de forma segura

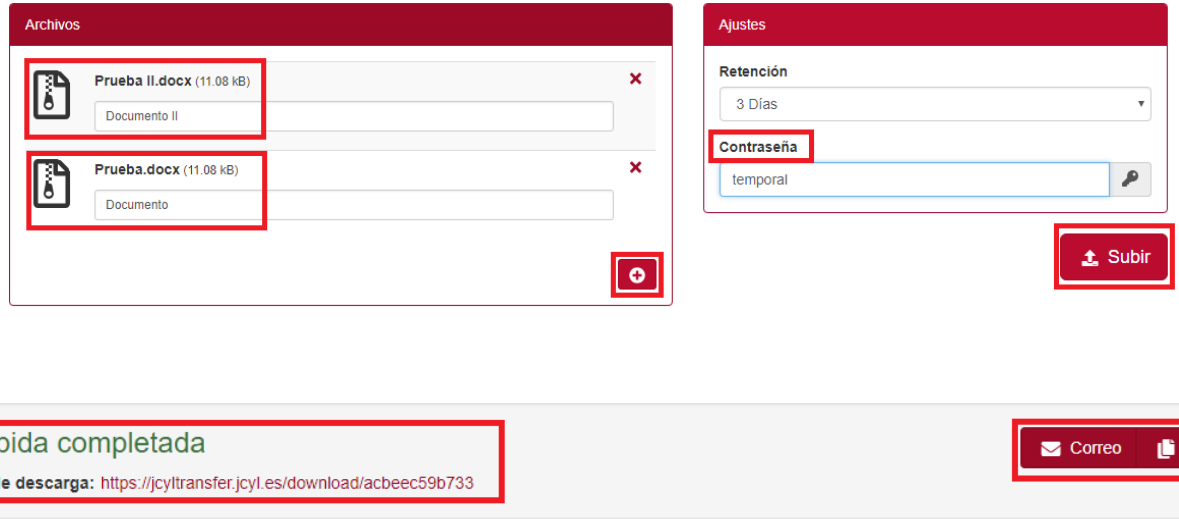
JCyL Transfer



Junta de Castilla y León

Transferencia de archivos pesados de forma segura

JCyL Transfer



Junta de Castilla y León

Transferencia de archivos pesados de forma segura

JCyL Transfer

Se genera un enlace que proporcionamos al destinatario y al que cualquiera podrá acceder. Así sólo debemos enviárselo a los destinatarios.

Tamaño máximo de archivos: 2GB

Pueden protegerse las descargas con contraseña

Los ficheros se mantendrán 3 días, luego se borran automáticamente

Sólo se pueden subir ficheros desde la Red Corporativa JCYL.

Sólo se puede utilizar con fines profesionales

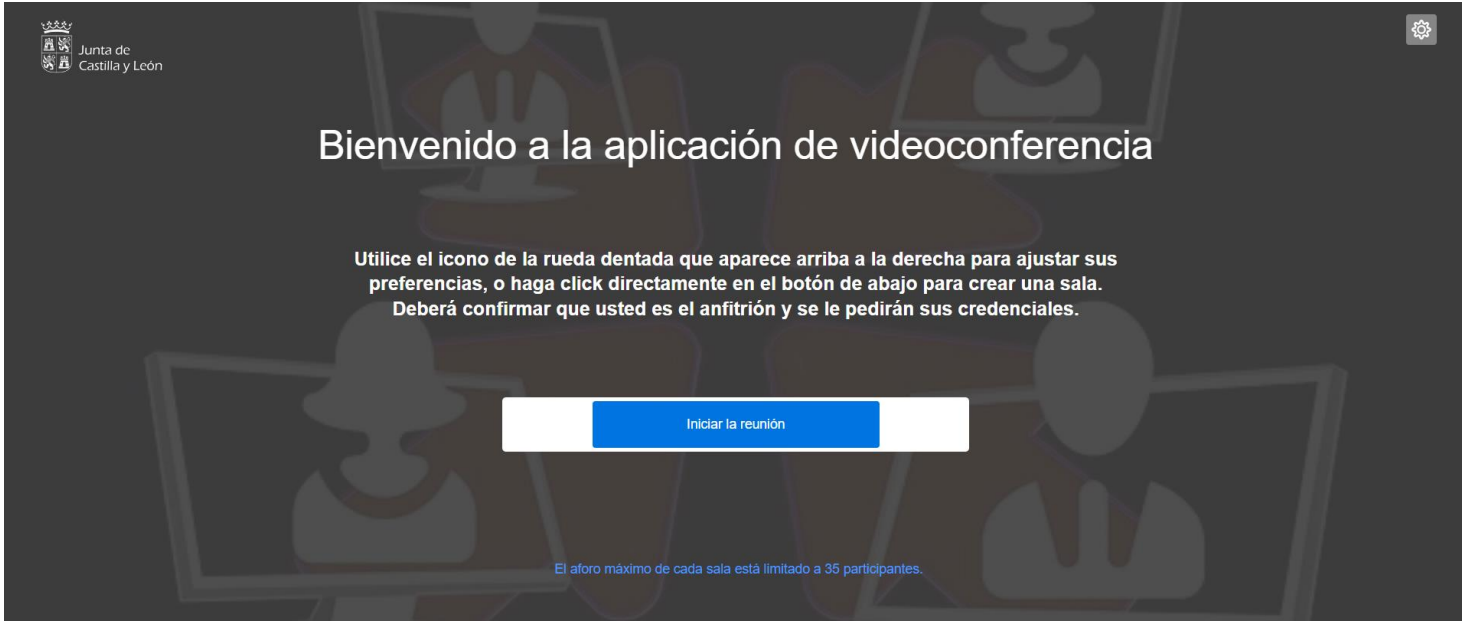
VER VIDEO

Buenas prácticas en el trabajo colaborativo

Junta de Castilla y León

Videoconferencias

JCyL Meet



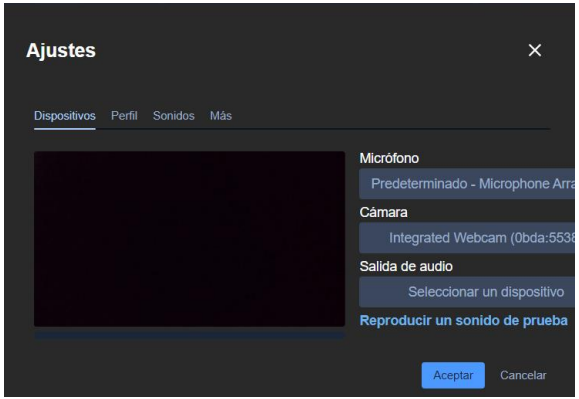
https://vconf.jcyl.es

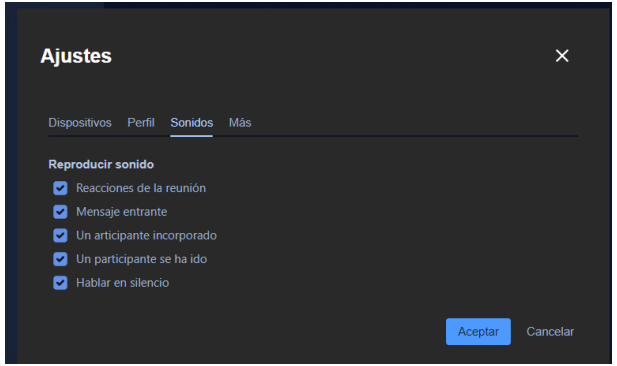
Buenas prácticas en el trabajo colaborativo

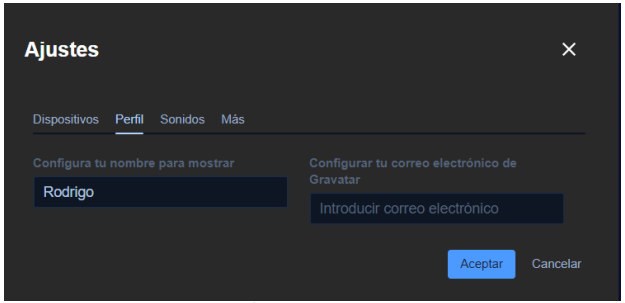
Junta de Castilla y León

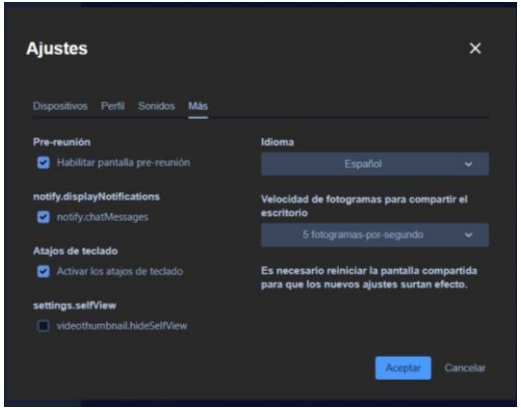
Videoconferencias

JCyL Meet







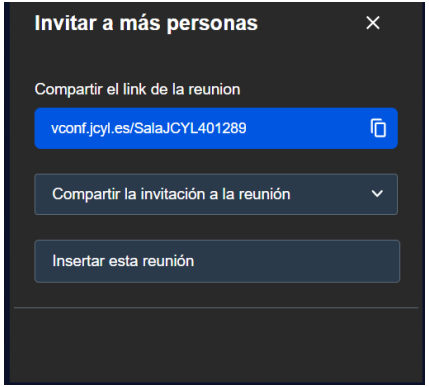


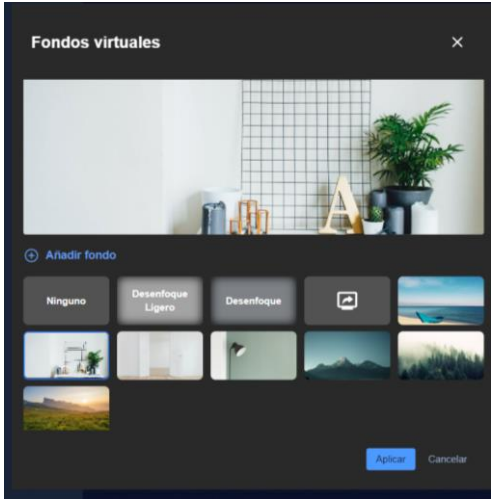
Buenas prácticas en el trabajo colaborativo

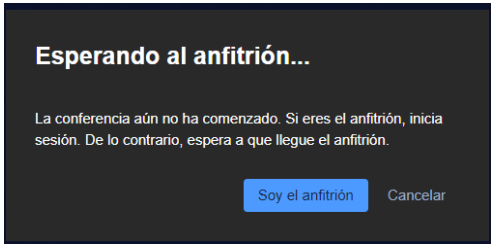
Junta de Castilla y León

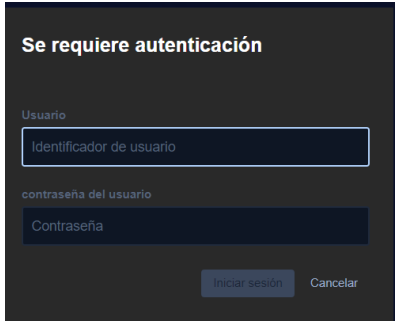
Videoconferencias

JCyL Meet









Junta de Castilla y León

Videoconferencias

JCyL Meet

Accesible desde Google Chrome o Microsoft Edge

Está basado en la herramienta generalista Jitsi

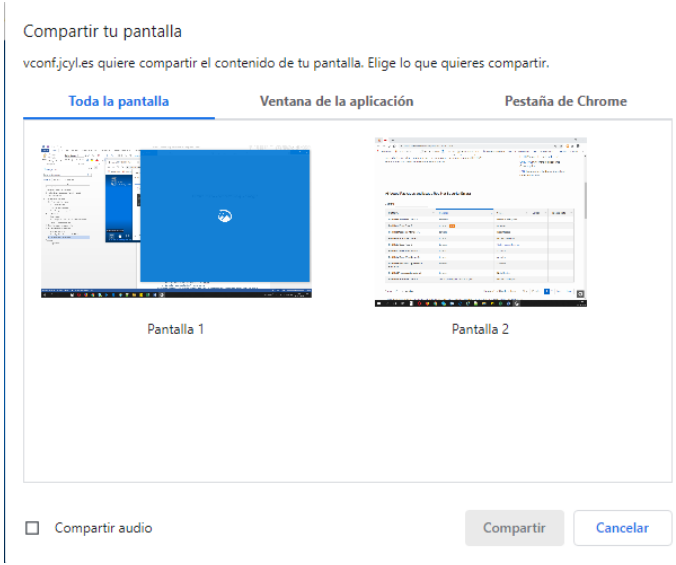
Se puede instalar también como aplicación y así poder unirse a conferencias si bien, no podremos crear Salas de Reunión. Las descargas se hacen a través de https://jitsi.org/downloads

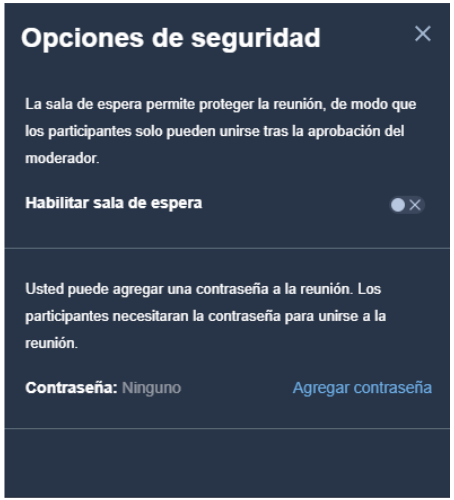
Junta de Castilla y León

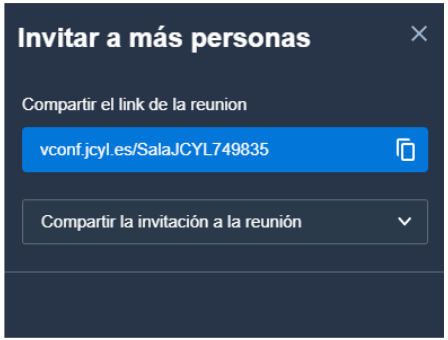
Videoconferencias

JCyL Meet

Compartir pantalla y opciones de seguridad







Junta de Castilla y León

Videoconferencias

JCyL Meet

Crear una nueva Sala de Videoconferencia

Como anfitrión que he creado la videoconferencia debo:

1. Entrar minutos antes de la reunión
2. Esperar a que todos los participantes hayan entrado en la sala
3. Agregar contraseña para evitar la entrada de otros usuarios por error

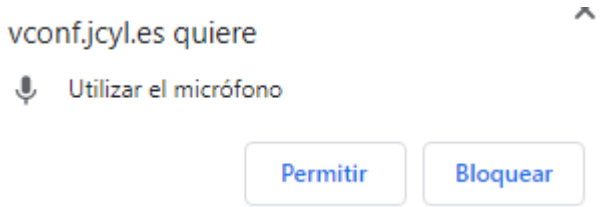
Junta de Castilla y León

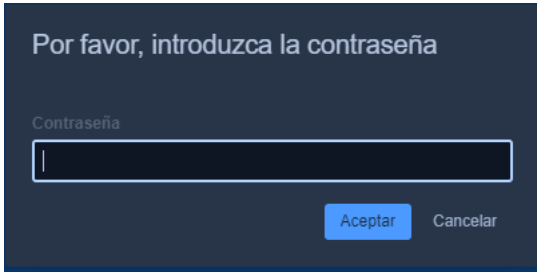
Videoconferencias

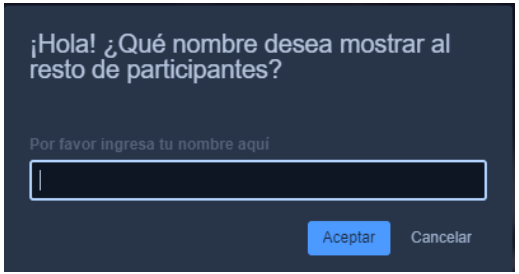
JCyL Meet

Videoconferencia como invitado

Copiamos el enlace enviado en la barra del navegador Chrome o Edge





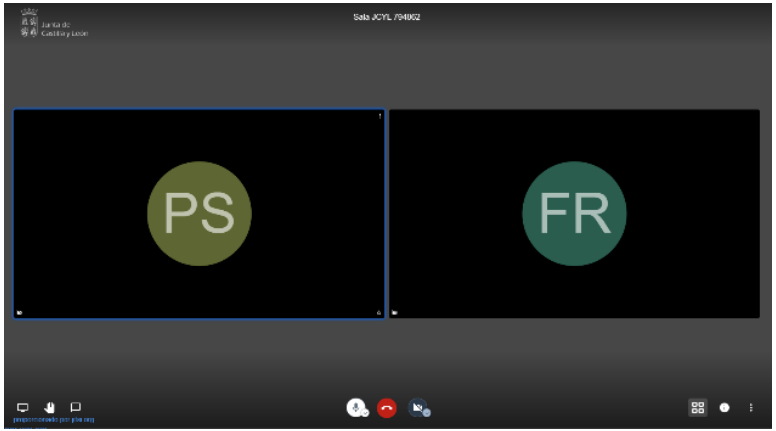


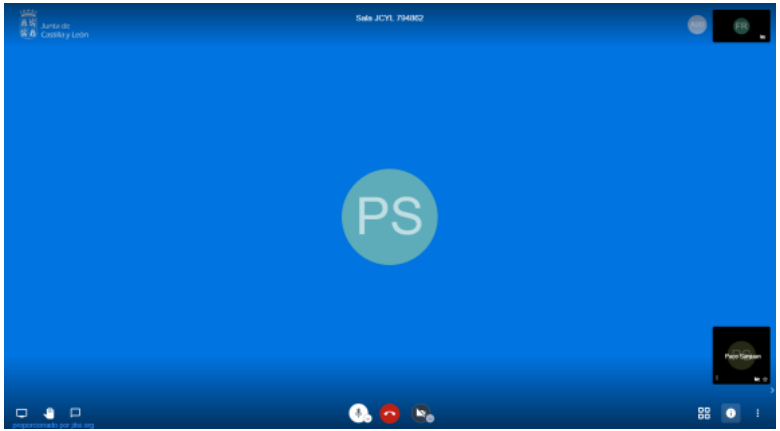
Junta de Castilla y León

Videoconferencias

JCyL Meet

Utilización de la sala de conferencia



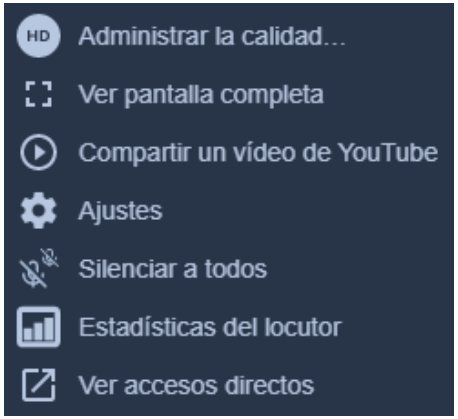


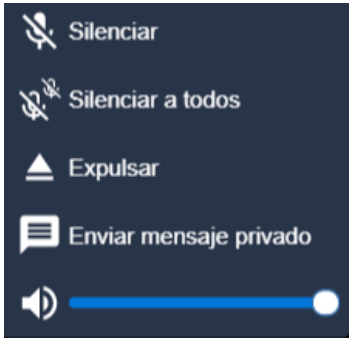
Junta de Castilla y León

Videoconferencias

JCyL Meet

Utilización de la sala de conferencia





Preferiblemente utilizar cascos

Utilizar indicador de mano para solicitar turno y sea respetuoso con los turnos

Por regla general micrófono desconectado si no vamos a participar

Si se detectan problemas de conexión es preferible bajar la calidad de imagen

De forma externa cuida tu entorno y lo que pueda aparecer en él

Junta de Castilla y León

Videoconferencias

JCyL Meet

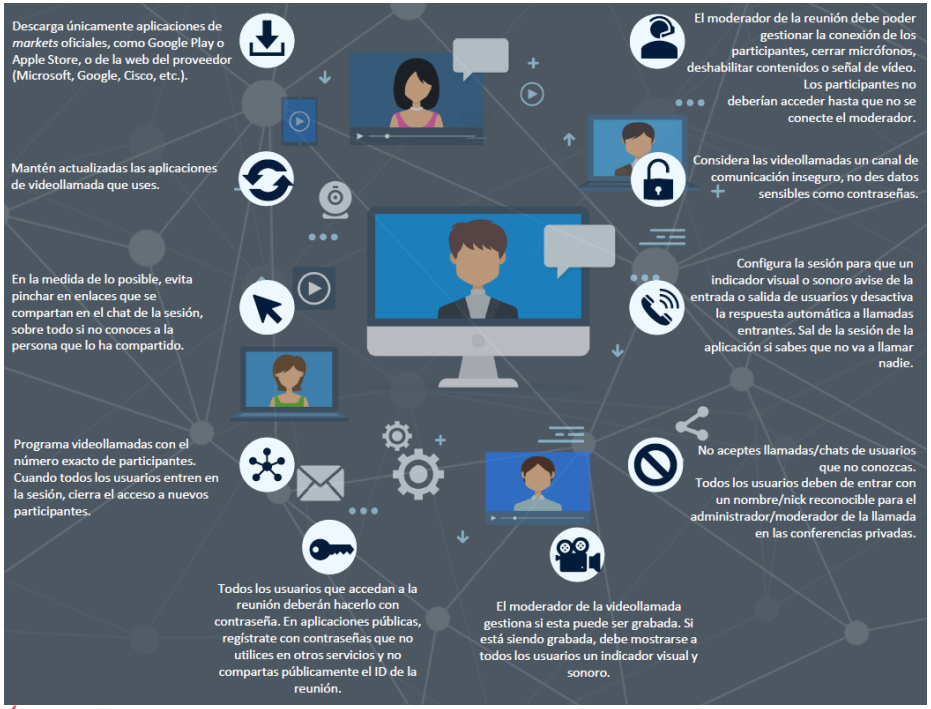
Utilización en dispositivos móviles

Buenas prácticas en el trabajo colaborativo

Junta de Castilla y León

Videoconferencias

JCyL Meet



Buenas prácticas en el trabajo colaborativo

Junta de Castilla y León

Otras herramientas colaborativas de ACCyL

Urbion — *Listín telefónico y acceso a datos*

Portafirmas — *Portafirmas de la ACCyL*

Hermes — *Comunicaciones y notas interiores entre servicios*

Desinformación

Las noticias falsas se han convertido en uno de los peligros más habituales en internet buscando en todo momento desinformar con la intención de engañar, manipular, desprestigiar…

"Una mentira repetida 100 veces se convierte en realidad"

Joseph Goebbels

Desinformación

Categorías de desinformación de Claire Wardle

Desinformación

Junta de Castilla y León

Desinformación							
Categorías → Motivaciones	Sátira o parodia	Conexión falsa	Contenido engañoso	Contexto falso	Contenido impostor	Contenido manipulado	Contenido inventado
Periodismo deficiente		✓	✓	✓			
Parodia	✓				✓		✓
Provocación					✓	✓	✓
Pasión				✓			
Partidismo			✓	✓			
Provecho económico		✓			✓		✓
Poder o influencia política			✓	✓		✓	✓
Propaganda			✓	✓	✓	✓	✓

Categorías de desinformación de Claire Wardle y Motivaciones de Eliot Higgins

Desinformación

Falso

Este vídeo con nubes ondulantes muestra el ojo del huracán Ian en Florida.

1938 Falso

1 nuevo

140 Engañoso

Newtral es miembro de la red del IFCN. Ésta es nuestra metodología de trabajo.

BULO

Desinformación

Junta de Castilla y León

Buenas prácticas ante la desinformación en internet

- Revisar el origen de la noticia (fuentes)
- Desconfiar de titulares llamativos y contenidos polémicos. Comprobar el contenido completo y a poder ser en varias fuentes adicionales de referencia.
- Formatos con medias verdades, errores lingüísticos, pantallazos
- Cuidado con el contenido patrocinado e influencers. Procura contrastar la información con expertos contrastados.
- Comprobar las fechas y que el contexto no coincide con algún tipo de campaña
- No contribuir a difundir información no contrastada ni trazable
- Comprueba siempre el contenido completo de una información. No te quedes sólo con el titular que puede ser engañoso y lee la noticia completa
- Si detectas alguna información de tu organización que se ha comunicado de forma incorrecta, debemos notificar al responsable para subsanar esa comunicación

Desinformación

Junta de Castilla y León

Buenas prácticas ante la desinformación en internet

- **Maldita.es**
- **Newtral**
- **Salud sin Bulos**
- **Fast Check Explorer**

Buenas prácticas en el uso de las redes sociales

Junta de Castilla y León

Para muchas personas se han convertido en plataformas fundamentales en nuestro ocio y en algunos casos también profesionalmente

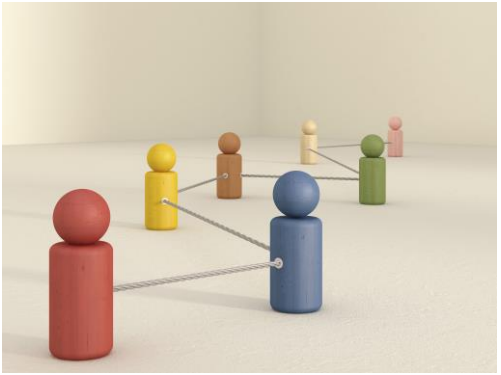
¿Qué aspectos debemos tener en cuenta en el uso de las redes sociales?

Buenas prácticas en el uso de las redes sociales

Junta de Castilla y León

Buenas prácticas de seguridad en redes sociales

- Revisa la **privacidad de las redes sociales**, conoce cómo funciona y elige la privacidad más adecuada
- Muy atento al ámbito del **contenido compartido** diferenciando entre publicaciones públicas o privadas
- **Evita difundir información sensible por redes sociales** tanto a nivel laboral como personal. Esta información puede ser utilizada para suplantar la identidad
- Divide información publicitada que pueda vincularte con el puesto de trabajo y **no compartas datos del puesto de trabajo**
- **No proporciones información privada sobre terceros** y **desactiva la geolocalización** por defecto
- **Evita la apertura de contenidos con indicios sospechosos**. Cuidado con los enlaces acortados
- **Lista de contactos debe mantenerse privada**
- Contraseñas fuertes y doble factor de autenticación
- Mantén tu **reputación y cuida tu imagen digital** que es parte de tu identidad



Buenas prácticas en el uso de las redes sociales

Buenas prácticas de Seguridad en Redes Sociales

Protección de los soportes de información (digitales o físicos)

“Debemos evitar en la medida de lo posible la utilización de dispositivos extraíbles para manejar información ya que son un riesgo para la seguridad de los sistemas y de la propia información”

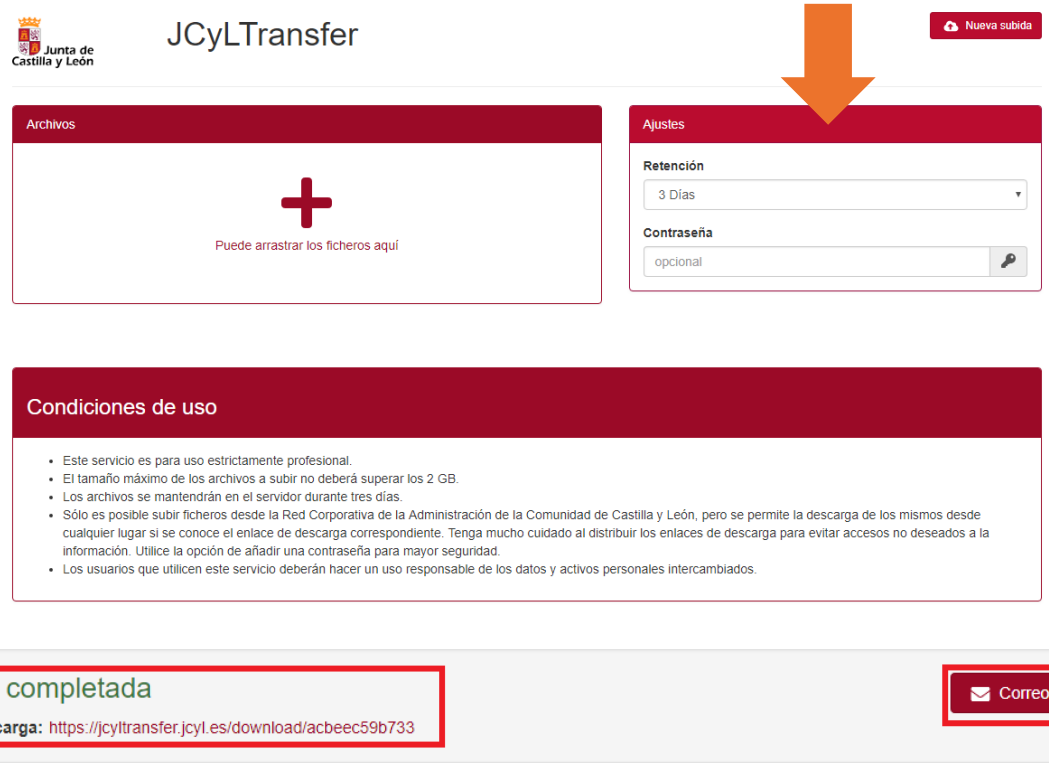
Protección de los soportes de información (digitales o físicos)

Junta de Castilla y León

Normas en el uso de soportes digitales

- No debemos conectar dispositivos sospechosos a nuestros equipos ya que pueden ser un riesgo. En caso de tener que conectarlos utilizaremos el antivirus sobre ese dispositivo. Está relacionado con el llamado ***baiting*** y la posibilidad de encontrar USBs en lugares públicos.
- Si necesitamos enviar información de gran tamaño, podemos utilizar JCYL Transfer
- Los soportes etiquetados no deben revelar el contenido pero sí el nivel de seguridad
- Si debemos utilizar los mismos, este dispositivo deberá ser cifrado o la información que contenga deberá ser cifrada (recomendable para todos y obligatorio para información de nivel medio y alto del ENS)
- Una vez cumplido su objetivo deberemos borrar la información de forma segura (Ccleaner, Eraser… y otras herramientas pueden ser utilizadas).

Protección de los soportes de información (digitales o físicos)



Protección de los soportes de información (digitales o físicos)

Junta de Castilla y León

Normas en el uso de soportes físicos (archivos en papel)

- **Oficina sin papeles** eliminando en la medida de lo posible el papel en el flujo de trabajo
- La **custodia de los documentos** es igualmente importante en la oficina y en el trabajo a distancia. Debemos procurar las mismas medidas de seguridad que en la oficina
- Si **imprimes documentación** y no hay medidas de impresión segura con código, r**ecógelo inmediata**mente dado que la información puede tener información sensible.
- **Mesa despejada**: evita mantener documentos visibles encima de la mesa cuando no se está trabajando.
- **Destrucción de papel sensible o con información personal** debe hacerse mediante destructoras de papel disponibles. Si hay contenedores de reciclaje, revisa que no se puede extraer el documento
- **Borra las pizarras al finalizar las sesiones de trabajo y recoge los documentos utilizados**.

Evita imprimir lo que no sea necesario

Prevención de fugas de datos

Uno de los grandes riesgos que tenemos en las organizaciones son la pérdida de datos que debemos procurar evitar a través de medidas de prevención adecuadas

Prevención de fugas de datos

Junta de Castilla y León

Buenas prácticas para prevenir la fuga de datos

- Debemos procurar **revisar siempre con quien compartimos** la información y que estos remitentes sean personas autorizadas para poder acceder a la misma.
- ***¿Por qué medios compartimos la información?*** El medio es igualmente importante que el remitentes dado que si no compartimos la información por medios seguros y autorizados podemos provocar pérdidas de datos
- La **información debe estar siempre almacenada en recursos de ACCyL** evitando almacenamientos locales o en clouds o USBs no autorizados
- Cuidado con el **transporte de soportes en papel o USBs** con datos de nuestra organización
- En caso de llevar a cabo transmisión o transporte de datos confidenciales o de relevancia para nuestra organización deberemos procurar hacer **cifrado de esta información** por medios recomendados

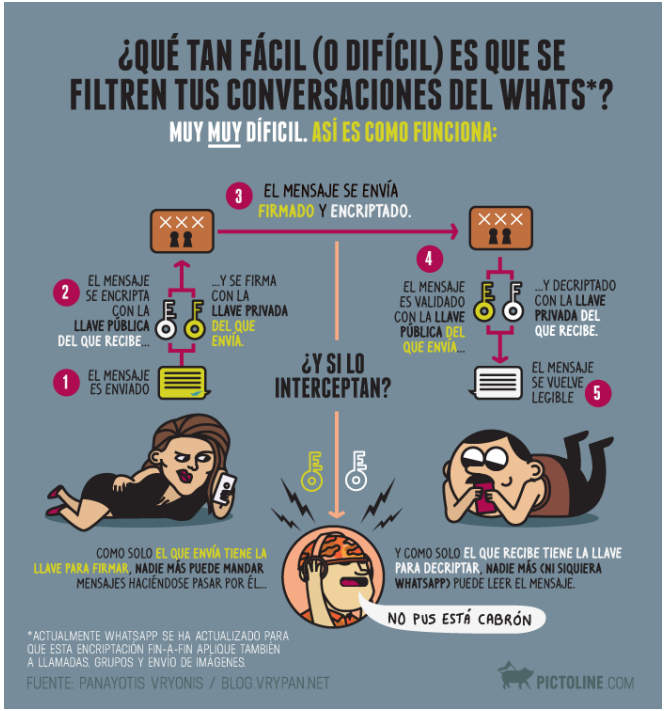
Prevención de fugas de datos

Junta de Castilla y León

Buenas prácticas para prevenir la fuga de datos

Gpg4win
GnuPG for Windows

7ZIP



Prevención de fugas de datos

Junta de Castilla y León

Buenas prácticas para prevenir la fuga de datos

- Mucho cuidado con los intentos de engaño por **ingeniería social** y con los datos que aportamos por internet. Cuanto más datos aportamos más fácil son los robos de identidad

- Cuando compartimos documentos, sobre todo si son públicos, debemos llevar a cabo limpieza de **metadatos** de estos documentos previamente para no desvelar información no necesaria. Los metadatos son información asociada sobre propósito, estructura, descripción, administración…

- Debemos tratar los documentos de acuerdo a las **directivas de clasificación** existentes en nuestra organización y, en base a esto, establecer los diferentes permisos de acceso con **política de mínimo privilegio**

- Las **credenciales corporativas no se usarán en otros servicios no laborales** y finalizaremos sesión al acabar.

- **Contraseñas diferentes** en diferentes sitios o servicios

Notificación de incidentes de seguridad

Junta de Castilla y León

Buenas prácticas para prevenir la fuga de datos

- Uso de **VPN** en dispositivos portátiles.
- Habilita doble factor de autenticación (**2FA**) si se permite
- **Elimina regularmente la información obsoleta** si no se debe conservar. Comprueba periódicamente unidades locales y de red.
- **No uses la dirección de ACCyL como correo alternativo** a otros servicios no laborales.
- Se **monitorizan listas públicas de internet desde ACCyL** con el fin conocer que direcciones corporativas pueden tener más afectación posterior de spam o phishing

Si, a pesar de todas estas precauciones, detectamos una fuga de datos, debemos notificarlo como un incidente de seguridad

Junta de Castilla y León

¿Qué es un incidente de seguridad?

"Un incidente de seguridad en un sistema de información es cualquier situación o eventualidad en la que pueda verse amenazada la información y pueda, en consecuencia, dar lugar a una degradación o pérdida de su confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad"

Notificación de incidentes de seguridad

Junta de Castilla y León

¿Qué NO es un incidente de seguridad?

Medidas de mitigación sin necesidad de notificar incidente de seguridad	
Se recibe un correo marcado como [SPAM] o [POSIBLE SPAM], redactado con una gramática muy burda, en un idioma extranjero, al que no se contesta, ni se pincha en ningún enlace.	Eliminar y bloquear remitente.
Se reciben correos sospechosos de un remitente conocido.	Informar a remitente de los mismos
Se ha perdido o destruido un dispositivo cifrado con datos de los que hay copia.	Informar responsable de tratamiento. Restaurar la información de la copia de seguridad.
El antivirus indica que ha realizado una serie de tareas que no requieren atención.	Reiniciar equipo si se indica.
Fallo en una aplicación	Generar petición de aplicación, no de seguridad

¿Qué SÍ es un incidente de seguridad?

Incidente	Resolución	Categoría petición Seguridad
Correo basura, spam	Eliminar y opcionalmente bloquear remitente. Si se ha respondido adjuntando datos o se ha accedido a un enlace o fichero adjunto, generar petición.	Correo spam o publicitario
Correo suplantación, phishing	Eliminar y opcionalmente bloquear remitente. Si se ha respondido adjuntando datos o se ha accedido a un enlace o fichero adjunto, generar petición.	Correos sospechosos o sondeo de información. Phishing
Nuestros contactos nos informan de envíos propios de correos sin ser conscientes de los mismos	Notificar a remitente de la situación y de la precaución en dichos correos. Generar petición.	Código dañino o malicioso, malware
Visualización del propio correo en lista pública externa ACCyL	Eliminar el correo corporativo del servicio ajeno no laboral con brecha de seguridad. Generar petición.	Política de seguridad. Incumplimiento de normativa.
El dispositivo de puesto de usuario se comporta de forma errática Aparecen elementos que no se han instalado de forma consciente	Generar petición.	Código dañino o malicioso, malware.
Se cifran archivos y documentos en el equipo o unidad de red	Desconectar cable de red del equipo, y desactivar red inalámbrica en su caso. Generar petición.	Código dañino o malicioso, malware.
Pérdida o robo de dispositivo no cifrado con datos personales o confidenciales Fuga o brecha de datos personales en un sistema de la ACCyL	Notificar al responsable del tratamiento y al Delegado de Protección de Datos. Generar petición.	Compromiso de información. Acceso no autorizado o fuga de información. Mal uso de sistemas de información
Préstamo entre empleados o uso de credenciales ajenas	Modificar clave, no prestar ni usar cuenta de terceros. Generar petición	Suplantación identidad. Intento de fraude o uso de recursos no autorizados.
Imposibilidad de actualización de antimalware, antivirus	Reiniciar equipo. Si no se actualiza, generar petición.	Antivirus o sistema no actualizado, vulnerable.

Junta de Castilla y León

¿Cómo se detectan los incidentes?

Automatizadamente

A través de herramientas o recursos informáticos como Servicios de Alerta Temprana (sondas SAT-SARA, SAT-INET, SAT-ICS).

Notificación de Usuarios

Como usuarios podemos detectar incidentes que pueden estar ocurriendo y puede haber diferentes aspectos que nos hagan detectar estos incidentes:

- **Pérdida o robo** de un dispositivo no cifrado con datos personales
- **Notificación de terceros** (compañeros, usuarios, proveedores…) de que han recibido algún mail no enviado por nosotros.
- **Correos sospechosos** solicitando información a los que se ha respondido o se ha introducido información (phishing)

Junta de Castilla y León

¿Cómo se detectan los incidentes?

Notificación de Usuarios

- **Comportamientos erráticos del equipo** como
  - Aparición de mensajes, pop-ups, mucha publicidad, barras de tareas o extensiones en navegador
  - Falsos antivirus, falsas aplicaciones de soportes técnicos
  - Bloqueo o reinicio del equipo o comportamientos no habituales
  - Lentitud del ordenador. tarda mucho en arrancar o el disco duro trabaja sin cesar
  - Aplicaciones que no funcionan o ejecución de otras sin permisos
  - Demasiado correo basura
  - Desaparición de archivos

- Se **cifran archivos y documentos**. Probablemente sea un ramsonware por lo que deberemos
  - Desconectar inmediatamente el cable de red y desactivar la red inalámbrica
  - Generar petición en ASISTA3

- Adware / Spyware
- Troyanos
- Botnet
- Gusanos
- Minería o criptominado
- Ramsonware

Notificación de incidentes de seguridad

Junta de Castilla y León

¿Y si detecto estos síntomas?

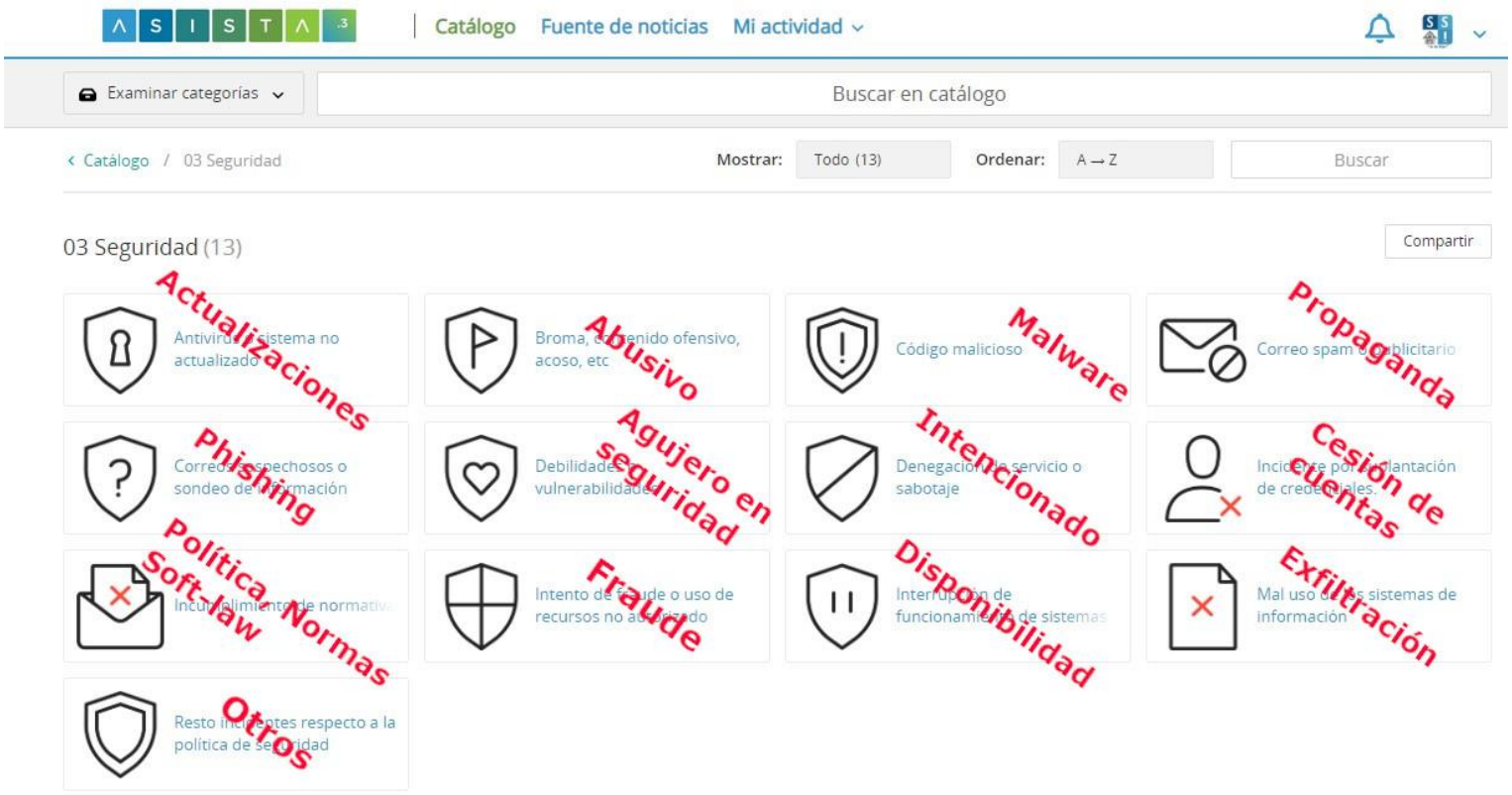
¿Cómo debo actuar?

¿A quién se lo notifico y por qué medios?

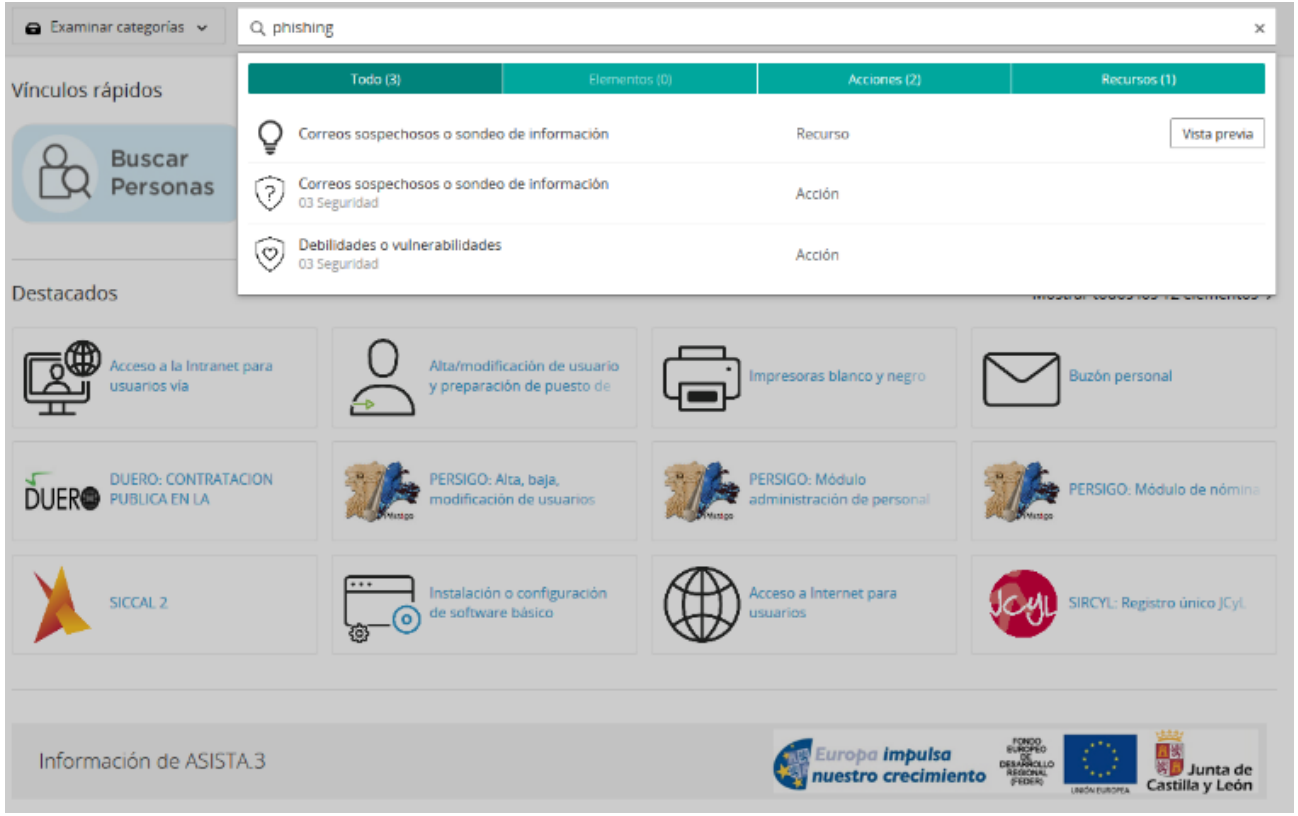
- **Entorno web ASISTA.3**. En primer lugar, se podrá comunicar mediante el enlace a **ASISTA.3** https://asista.jcyl.es/ durante las 24 horas del día. Seleccionar la categoría **SEGURIDAD**.
- **Asistencia telefónica**: 6116 (interno) y 983 41 94 80 (público y externo). Se presta atención continua durante la jornada de trabajo: de lunes a jueves de 8:00 a 19:00, viernes de 8:00 a 15:00.
- **Usuarios externos**: forma de contacto a través del **012**
- **Interfaz técnico web**: Se trata de una sección sólo para técnicos.

Notificación de incidentes de seguridad

Notificación de incidentes de seguridad

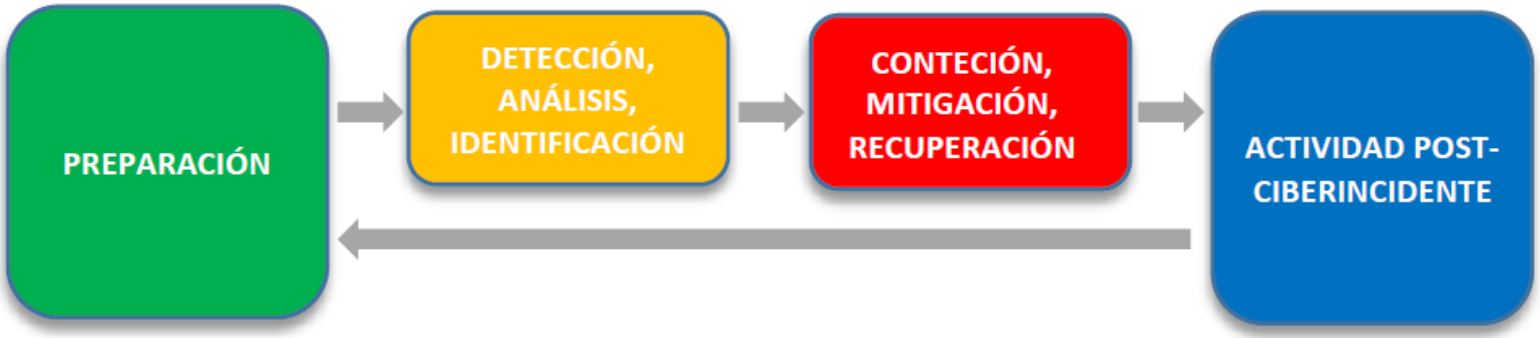


Notificación de incidentes de seguridad



Junta de Castilla y León

¿Y cómo se responde ante ciberincidentes?



Ciclo de vida de la Respuesta a Ciberincidentes

Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

Decreto 22/2021
Política de Seguridad de la Información y Protección de Datos (**PSIPD**)

Boletín Oficial de Castilla y León BOCYL

Núm. 192 Lunes, 4 de octubre de 2021 Pág. 47003

I. COMUNIDAD DE CASTILLA Y LEÓN

A. DISPOSICIONES GENERALES

CONSEJERÍA DE ECONOMÍA Y HACIENDA

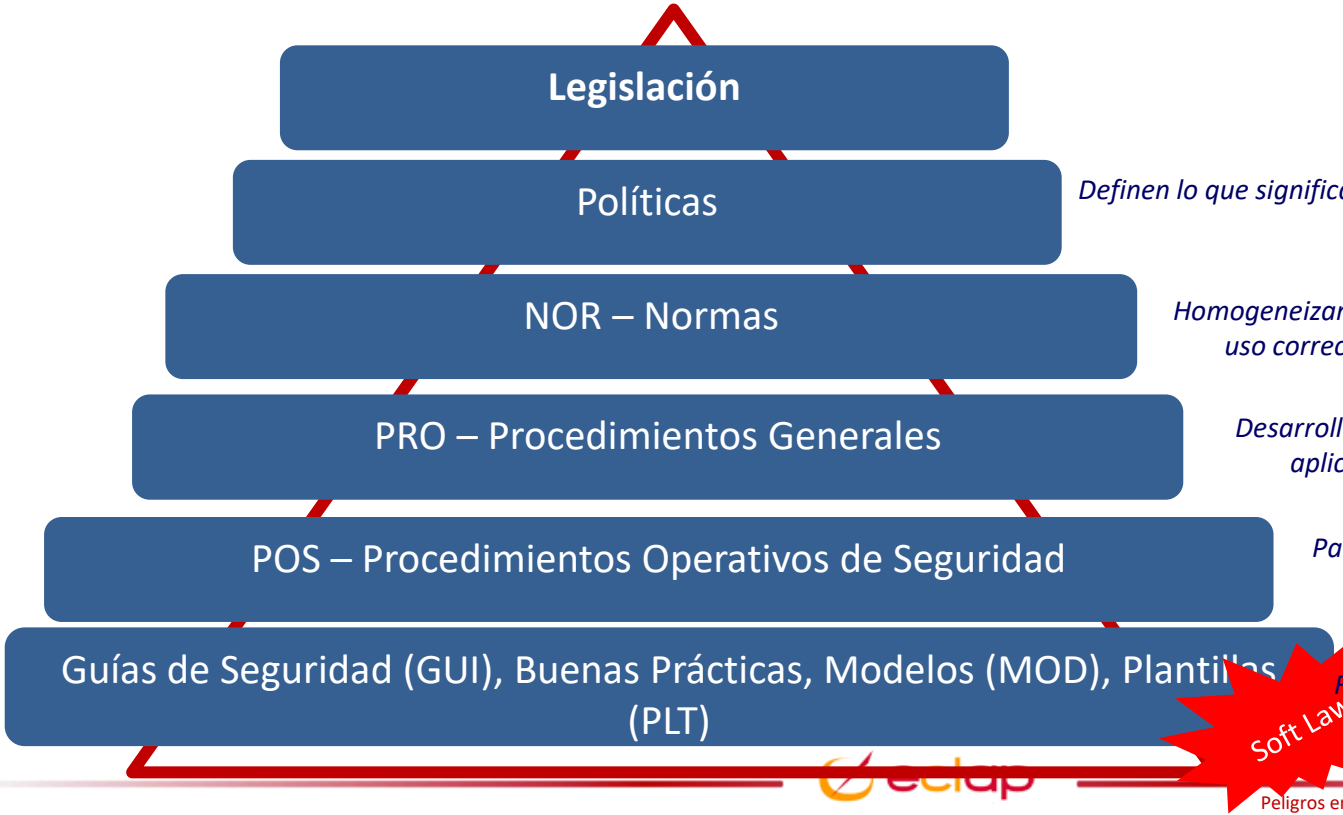
DECRETO 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece, en su artículo 13, el derecho de los ciudadanos a la protección y confidencialidad de sus datos y a la seguridad de los mismos cuando figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

Desarrollo de la PSIPD



Definen lo que significa la Seguridad de la Información en una organización

Homogeneizan el uso de aspectos concretos, indican el uso correcto y responsabilidades. Obligatorias

Desarrollan las Normas en aspectos que sean de aplicación transversal y sea obligatorio

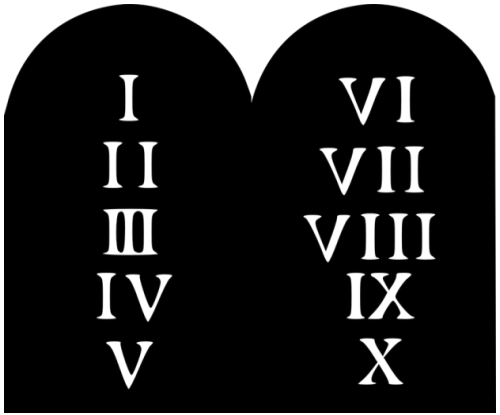
Para tareas concretas indicando qué hacer en cada caso paso a paso (día a día)

Recomendaciones pero que pueden tener responsabilidades

Obligaciones del Personal

El personal de la Administración de la Comunidad que tenga acceso a datos personales deberá colaborar en la implementación de la PSIPD y cumplir lo previsto en los instrumentos que la desarrollan.

Los empleados públicos cumplirán asimismo las obligaciones establecidas en la normativa de protección de datos personales y en particular las siguientes:



Política de Seguridad. Normas y Condiciones de Uso

Junta de Castilla y León

Obligaciones del Personal

Sólo accederemos a los datos personales cuando tengamos autorización y a la información que necesitamos para llevar a cabo nuestras tareas asignadas

Guardaremos deber de confidencialidad con la información que tratamos

No divulgaremos las contraseñas de acceso a los sistemas y aplicaciones informáticas que contengan datos de carácter personal

Custodiaremos con diligencia los documentos en soporte papel con datos personales e información confidencial

Solicitar las autorizaciones necesarias para grabar en dispositivos portátiles o tratar fuera de las dependencias administrativas los datos personales

No utilizar con fines diferentes a los propios del servicio los medios digitales puestos a su disposición

Turno de preguntas

Junta de Castilla y León

eclap