Buenas prácticas en el uso del correo electrónico

PROCEDENCIA: No confíes únicamente en el nombre del remitente. Verifica si el propio **dominio del correo** recibido es de confianza (dominio del organismo que envía el correo es la parte que sigue a la '@'), como por ejemplo '**jcyl.es**'.
Si el contenido de un correo procedente de un **contacto conocido** nos genera sospechas o desconfianza, contacta con el mismo por otra vía de comunicación para verificar la legitimidad.

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 demasiado explícita.

ENLACES: No pinches en enlaces de correos sospechosos, y evita hacer clic directamente en cualquier enlace desde el propio cliente de correo. Verifica su ortografía y **tecléala de forma manual en la barra del navegador**.

Si el **enlace es de una web desconocida**, es recomendable buscar antes información en motores de búsqueda reconocidos.

FICHEROS ADJUNTOS: No descargues un fichero adjunto procedente de un correo con remitente desconocido; deberás tener **seguridad de su procedencia** y que no presente indicios sospechosos.

Guarda manualmente el adjunto y analízalo con la solución antivirus en primer lugar. Antes de abrir cualquier fichero descargado mediante correo, asegúrate de su tipo (Word, Excel, etc.) y no se fíe sólo por el icono asociado al mismo. Revisa el **nombre completo del fichero incluida la extensión**; algunos nombres son muy largos y solo se puede visualizar una parte.

ENVÍOS Y RESPUESTAS: Utiliza la **funcionalidad CCO 'Con Copia Oculta'** para comunicaciones a varios destinatarios.

No respondas a comunicaciones sospechosas ni realices ninguna acción que proporcione datos personales o de tu cuenta de acceso. **Nunca se solicitan datos de credenciales por correo electrónico**.

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

O correo basura.
Son mensajes no deseados procedentes de remitentes desconocidos. Las direcciones de los destinatarios suelen proceder de listas masivas de correos filtrados.
Con frecuencia si uno solicita ser borrado de los destinatarios, lo único que hace es confirmar que tu dirección de correo existe; no se debe responder nunca a un mensaje de este tipo.

Phishing

Similares a correos *spam*, suplantan a entidades conocidas o también personas, y solicitan que el usuario proporcione datos personales o de credenciales tanto de cuentas laborales como personales. Suelen ofrecer la posibilidad de conectarse a alguna página web falsa para verificar el correo o algún dato concreto.

MACROS DE OFFICE: No habilites las macros de los documentos ofimáticos, incluso si el propio fichero así lo solicita desde el visor incluido en la aplicación cliente de correo.

No habilites el modo edición; con esta acción nos saltaríamos la protección que nos ofrece la propia herramienta ofimática.

PREVISUALIZACIÓN: Para mayor seguridad **desactiva la visualización automática de correos**, habitualmente en la configuración de Vista del Panel de Lectura.

La **pre-visualización de ficheros adjuntos** se desactiva habitualmente en las opciones y herramientas del Centro de confianza para el Tratamiento de datos adjuntos.

CIFRADO DE INFORMACIÓN: Cifra los mensajes de correo que contengan información clasificada o sensible, así como dependiendo del si**stema origen y nivel del Esquema Nacional de Seguridad** al que pertenezca.

CONTRASEÑA DEL CORREO: Utiliza **contraseñas robustas** para el acceso al correo electrónico si has creado tus 'Archivos de datos' locales, que contienen mensajes de correo.
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.

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

Ingeniería Social

Se asocia el concepto 'hackear (acceder) a la persona'.

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.

Lista masiva de direcciones filtradas de correo

Listas semipúblicas de información reunida a través de rastreo en Internet, las redes sociales, los foros, así como brechas de datos de empresas; no se tiene que realizar ninguna acción concreta e intencionada para aparecer en ellas.

Recogen la dirección de correo electrónico así como otros datos asociados a la misma. Para la mayoría no se puede solicitar la eliminación de nuestros datos y desaparecen solas.

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