ENERO 2020

Buenas prácticas en el uso seguro del correo electrónico

Seguridad de la Información de Castilla y León

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, solo 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 te fíes 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.**

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 **sistema 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.

Si eres empleado público de la Junta de Castilla y León el uso de medios digitales deberá realizarse conforme a la **política de seguridad** de la ACCyL, así como la política de **uso de los servicios de comunicaciones e informática** para todo usuario de los mismos.

Descubre más conceptos importantes para un buen uso del correo electrónico en la infografía de este mes.