



COMITÉ DE EMPRESA DE LA UNIVERSIDAD DE BURGOS

A LA ATENCIÓN DEL PLENO DEL COMITÉ DE EMPRESA

ASUNTO: Protocolo de gestión, seguridad y custodia de la cuenta de correo electrónico institucional del Comité.

1. EXPOSICIÓN DE MOTIVOS

El uso de las tecnologías de la información por parte de la representación legal de los trabajadores debe conciliar el derecho a la información de todos sus miembros con el estricto cumplimiento de la normativa vigente en materia de Protección de Datos y la seguridad jurídica de las comunicaciones institucionales.

La cuenta de correo cempresa@ubu.es actúa como el canal oficial de comunicación del Comité de empresa. Por ello, es imperativo establecer un protocolo que **garantice la integridad** de la información y **la autenticidad** de los mensajes emitidos.

2. TITULARIDAD Y CUSTODIA

De acuerdo con las funciones de representación y fe pública interna:

La Presidencia: Es la figura encargada de la emisión de comunicaciones oficiales en nombre del órgano.

La Secretaría: Es la figura encargada de la custodia de la documentación, archivos y la gestión del correo entrante.

Por razones de seguridad técnica y jurídica, las claves de acceso serán de uso exclusivo de la Presidencia y la Secretaría, evitando el acceso multivariante que impida la trazabilidad de las acciones realizadas en la cuenta.

3. FUNDAMENTOS JURÍDICOS PARA EL ACCESO RESTRINGIDO

Trazabilidad y Responsabilidad: El acceso compartido por múltiples usuarios impide identificar al autor de un envío, eliminación o modificación de correos. Ante una posible demanda o conflicto legal, la responsabilidad recae en quienes ostentan los cargos, por lo que el control debe ser coherente con dicha responsabilidad.

Reglamento General de Protección de Datos: El Comité maneja datos de carácter sensible (nóminas, procesos de incapacidad temporal, expedientes sancionadores). El acceso a estos datos debe regirse por el principio de minimización, limitando el acceso solo a las personas estrictamente necesarias.

Seguridad de la Información: El riesgo de borrado accidental o de suplantación de identidad institucional (enviar correos en nombre de la presidenta sin su consentimiento) supone un riesgo para la unidad de acción del Comité.

4. GARANTÍA DEL DERECHO A LA INFORMACIÓN

El acceso restringido a la cuenta no limita el derecho a la información de los vocales. Para garantizarlo, se establecen los siguientes mecanismos:



Reenvío de información: Todo correo de interés general será reenviado a las cuentas personales de los miembros del Comité de forma inmediata.

5. CONCLUSIÓN

El acceso universal de todos los miembros a la clave de la cuenta institucional es una práctica de riesgo que vulnera principios de seguridad informática y protección de datos. Por tanto, se mantendrá la gestión bajo la responsabilidad de la Presidencia y Secretaría, asegurando siempre el flujo de información veraz y puntual al resto del órgano.

Fdo.: Presidenta del Comité de Empresa Fdo.: Secretario del Comité de Empresa

En Burgos 8 de enero de 2026