Buenas prácticas en el uso del correo electrónico respecto a la protección de datos

- **Usa siempre tu cuenta institucional**
  - No utilices correos personales para asuntos académicos o administrativos.
  - Esto ayuda a mantener la seguridad y la trazabilidad.
- **Evita enviar datos personales sensibles**
  - No compartas información como **DNI, direcciones, números de teléfono, cuentas bancarias** o cualquier otro dato de carácter personal por correo electrónico.
  - Si es imprescindible, consulta antes al delegado de protección de datos sobre el canal seguro a utilizar.
- **Nunca envíes datos especialmente protegidos**
  - Salud, orientación sexual, ideología política, religión, etc. no deben circular por correo.
  - Estos datos requieren un nivel de protección superior.
- **Protege la identidad de los destinatarios**
  - Si envías correos a varios estudiantes o compañeros que no se conocen entre sí, utiliza siempre el campo **CCO** (copia oculta).
- **Revisa antes de enviar**
  - Comprueba que los destinatarios y adjuntos son correctos.
  - Evita errores de envío que puedan exponer información a terceros.
- **Sé prudente con los archivos adjuntos**
  - No adjuntes documentos con datos personales salvo que sea imprescindible.
  - Si es necesario, protégelos con contraseña y comunícala por un canal distinto (teléfono o mensajería).
- **No reenvíes correos con información sensible**
  - El reenvío puede difundir datos personales a personas no autorizadas.
- **Mantén tu cuenta segura**
  - Usa una contraseña robusta y cámbiala periódicamente.
  - Activa, si está disponible, la autenticación en dos pasos.
  - No compartas tu contraseña con nadie.
- **Cuidado con el phishing y correos sospechosos**
  - No abras enlaces ni descargues archivos de correos que no esperabas o que resulten extraños.
  - La universidad nunca pedirá tu contraseña por correo.
- **Elimina lo que ya no necesites**
  - No acumules correos con datos personales.
  - Borra aquellos que ya no sean útiles para tu actividad académica o laboral.
- **Recordatorio de normativas vigentes sobre correo electrónico**
  - Mostrar enlaces a las mismas
- **En caso de que se haya difundido un mensaje con datos personales**
  - Valora enviar un mensaje a todos los destinatarios para que procedan a eliminar el mensaje con datos personales recibido.

- Informa al **CAU (Centro de Atención a Usuarios) c**on la máxima brevedad para que, en su caso, informen de la brecha de seguridad.

Cosas a evitar

- Incluir el **DNI** o copias de documentos oficiales en correos.
- Usar el correo institucional para fines personales o ajenos a la universidad.
- Compartir listas de estudiantes con datos de contacto en abierto.
- Aprobar mensajes con listados de estudiantes y sus datos de contacto.
- Difundir actas, calificaciones u otra información académica con nombres y apellidos.
- Publicar información médica o personal de miembros de la comunidad universitaria.
- Usar el correo para intercambiar datos académicos sensibles (ej. actas, calificaciones nominales).

Recomendaciones

- El correo institucional es una herramienta de **trabajo y comunicación académica**, no de almacenamiento ni de envío de datos sensibles.
- Si necesitas enviar información personal o confidencial, consulta a tu facultad o al servicio de informática sobre canales **seguros y autorizados**.
- Ante dudas, **piensa antes de enviar**: ¿es necesario que esta información circule por correo electrónico?
- Puedes plantear tus dudas al Delegado de protección de datos en dpd@ehu.eus
- Si envías por error un mensaje que contiene datos personales de terceros y crees que puede suponer un peligro avisa al CAU para que informen de la brecha de seguridad y valora enviar un mensaje a todos los receptores para que eliminen en sus buzones el mensaje ya distribuido.