Universidad de Jaén
Secretaría General

RECOMENDACIONES DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD DE JAÉN

Consejos

CONTRASEÑAS

•Utiliza contraseñas robustas (al menos 8-10 caracteres, combinando números, caracteres específicos y letras mayúsculas y minúsculas).
•No utilices el mismo patrón.
•No reutilices la misma contraseña en otros servicios.
•Nunca publiques o compartas tú contraseña.
•Renueva la contraseña cada 6 meses.
•Siempre que sea posible, configura protecciones adicionales, como la autenticación de dos factores (2FA). Los sistemas corporativos de UJA (Google Workspace, Univ. Virtual, etc) a los que se accede mediante SIDUJA ya están configurados para pedir obligatoriamente 2FA cuando se accede desde el exterior a la UJA

SISTEMAS A UTILIZAR

•Para el tratamiento de datos personales, utiliza exclusivamente equipos y sistemas de la Universidad de Jaén.
•Ten siempre instalado la última versión de antivirus y el software de seguridad microCLAUDIA.
•Intentar utilizar software aconsejado o aprobado por Servicio de Informática. En caso de duda contactar. Evita utilizar sistemas personales.
•Realiza frecuentemente copias de seguridad.

TRANSFERENCIA DE INFORMACIÓN

•Cifrar las comunicaciones o utilizar sistemas que encripten. Si se desconoce, al menos comprime el archivo y establece contraseña.
•No compartir contraseñas por el mismo medio al que se comparte el archivo.
•No compartir información por Whatsapp.
•Evitar la utilización de USB o discos duros portátiles. Si se usan, deben estar cifrados. Especialmente, se deben cifrar, si van a salir de las instalaciones.
•Evita usar aplicaciones de control remoto tipo Anydesk, TeamViewer... Para el acceso remoto desde el exterior, utiliza la VPN segura de la UJA

Universidad de Jaén
Secretaría General

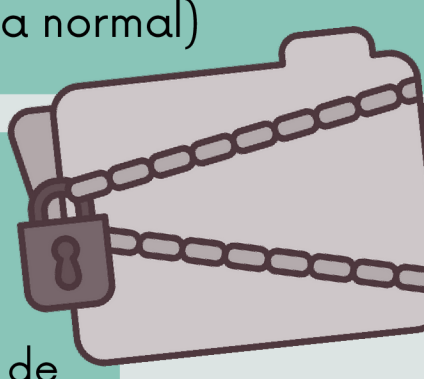
Universidad de Jaén

Secretaría General

Consejos

ALERTA EN EL USO DEL EMAIL

•No respondas mensajes que soliciten claves de usuarios, datos personales o bancarios.
•No abras ficheros adjuntos ni enlaces contenidos en correos sospechosos o procedentes de remitentes desconocidos.
•Cuando envíes mensajes a múltiples destinatarios, utiliza los campos CCO (Con copia oculta), en lugar de CC (copia normal)



CONSERVACIÓN DE LA DOCUMENTACIÓN

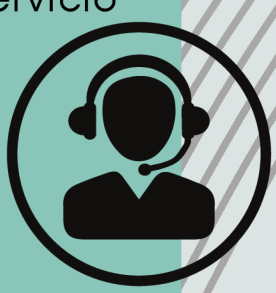
•Encripta en archivos información que contenga datos personales.
•Una vez concluida la finalidad de la investigación, borra de manera segura la información
•Limpia los metadatos
•Mantén tu puesto de trabajo despejado, sin más material encima de la mesa que el necesario en cada momento. Si has de atender a un alumno, procura que no visualice información de terceros.

CONFIGURACIÓN DE LOS SISTEMAS

•Procura no modificar la configuración de seguridad de los equipos de la Universidad.
•Mantén los equipos debidamente actualizados.
•Apaga el equipo tras finalizar tu jornada laboral o si no requiere ser utilizado durante un espacio de tiempo considerable.
•Bloquea el sistema si te ausentas temporalmente de tu puesto de trabajo (En sistemas Windows el comando es "Tecla Windows + "L")

USO ATENCIÓN AL USUARIO

•La UJA tiene una Oficina de Atención al Usuario del Servicio de Informática.
- Vía telemática: Intranet->Portal de Autoservicio TIC (Murphy)
- Vía telefónica: 953212000 (tf. interno 82000)
- Vía presencial: Edif. D1, planta baja, ventanilla 8010



•Si detectas alguna incidencia de seguridad o expones datos a terceros contacta con la Oficina de Atención al Usuario.
•Si has sido víctima de algún tipo de fraude o delito informático, puedes interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado

Universidad de Jaén

Secretaría General