Universitat d'Alacant
Universidad de Alicante

INFORMACIÓN SOBRE EL TRATAMIENTO DE DATOS PERSONALES CON MOTIVO DEL TRABAJO NO PRESENCIAL EN LA UNIVERSIDAD DE ALICANTE

Durante la situación de actividad no presencial y atendiendo a las medidas adoptadas por la Universidad de Alicante para evitar contagios se considera necesario poner a disposición de la comunidad universitaria determinadas recomendaciones ante la generalización de la actividad laboral en su modalidad no presencial en relación con el cumplimiento de las garantías del derecho a la protección de datos de carácter personal de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Ante este escenario y desde la necesidad de adaptar los hábitos de trabajo a esta situación en la que las relaciones con los sistemas de soporte y atención a usuarios tienen que realizarse por cauces no habituales, cabe realizar de modo sintético las siguientes recomendaciones:

1. Recomendaciones generales

- De forma general, siga las instrucciones que la Universidad facilite para realizar las conexiones y accesos remotos a sus servicios. En caso de dudas o incidentes, consulte siempre con fuentes oficiales de la Universidad.
- Para incidentes o consultas en materia de seguridad de la información, incluyendo aquellas que puedan afectar a la protección de datos de carácter personal, puede remitir su consulta o notificar el incidente a Servei.informatica@ua.es

2. Recomendaciones en relación con el uso de las herramientas y medios propios de la Universidad:

- Se debe tener cuidado con el soporte técnico, de manera que, si recibe llamadas, correos, mensajes, etc., aparentemente provenientes de personal de la organización, centros de atención a usuarios, etc., se debe recordar que nunca debe facilitar información de medios de acceso (usuario y contraseña, tokens, códigos recibidos por SMS, etc.). El personal de atención a usuarios del organismo cuenta con medios de acceso a las infraestructuras que les deben permitir solventar los problemas sin requerir datos del acceso de los usuarios finales.
- Si está detectando problemas en su acceso remoto, contacte directamente con los medios de atención a usuarios que la Universidad haya puesto a su disposición. No confíe en llamadas o correos "proactivos" de un supuesto centro de atención a usuarios si no puede confirmar que se trata realmente del centro de atención a usuarios de la Universidad.
- Si se dispone de un equipo en el que pueden realizarse actividades ajenas a la actividad de trabajo, se recomienda configurar un usuario exclusivo para el uso profesional y otro para usos ajenos a la actividad de trabajo. Desde el usuario profesional se accederá a la cuenta institucional, se ejecutarán las aplicaciones corporativas y se evitará abrir documentos no corporativos o recibidos desde fuentes no confiables, o permitir la ejecución de macros de documentos ofimáticos.

- Se debe realizar la actividad desde las herramientas recomendadas en el Plan de Continuidad de la Docencia de la Universidad de Alicante, que permiten la conexión directa mediante mensajería, la creación de espacios de trabajo, etc.
- Se debe recordar que los medios de protección en un equipo fuera de las instalaciones de la Universidad de Alicante pueden ser en algunos aspectos menores que cuando se está situado dentro del perímetro de seguridad de la Universidad. Se recomienda seguir las directrices básicas de seguridad en el puesto de trabajo informático, disponible en https://si.ua.es/es/documentos/servicios/seguridad/seguridad-trabajo-informatico.pdf.
- Se pueden seguir una serie de medidas para concienciar a los usuarios acerca de la seguridad, de las redes que utilizan y los datos personales que tratan, y que están recogidas en la Guía CCN-CERT – Medidas de seguridad para Acceso Remoto (disponible en https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/abstract/191-abstract-politica-de-acceso-remoto-seguro/file),https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/4688-ccn-cert-bp-18-recomendaciones-de-seguridad-para-situaciones-de-teletrabajo-y-refuerzo-en-vigilancia/file.html, y también vid. la guía INCIBE "Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario", disponible en https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el
  Además, cualquier información oficial se hará a través de los canales definidos por la Universidad de Alicante a través del Plan de Continuidad de la Docencia.

3. Recomendaciones en relación con el phishing y Covid-19:

- Se debe ser cuidadoso con los correos recibidos con información sobre el COVID-19.
- No debe pulsar enlaces ni abrir archivos adjuntos en correos electrónicos, mensajes de texto, WhatsApp, etc.
- Se debe desconfiar de correos que soliciten donaciones a supuestas víctimas.
- Se debe ignorar enlaces a páginas web donde ofrezcan vacunas o tratamientos para superar la enfermedad.
- Se debe sospechar de posibles oportunidades de inversión en compañías que afirman poder detectar, prevenir o incluso curar los efectos del virus.
- Nunca se debe contestar al remitente. Uno de sus objetivos es simplemente confirmar direcciones de e-mail.
- Y por supuesto si se solicitan claves en pagina ajenas a dominio ua.es no les haga caso.
- Se puede encontrar más información en: https://social.inap.es/sites/default/files/ciberCOVID19%20frente%20a%20phising_0.pdf, y https://www.aepd.es/es/prensa-y-comunicacion/blog/campanas-de-phishing-sobre-el-covid-19

Si se tiene alguna duda o consulta puede contactar con la delegación de protección de datos en: dpd@ua.es

Alicante a 23 de marzo de 2020

DELEGACIÓN DE PROTECCIÓN DE DATOS