Covid-19 - Cuestiones de interés en materia de protección de datos

Información sobre protección de datos en el marco del plan de contingencia Covid-19

Seguridad en teletrabajo: Medidas orientadas a garantizar la privacidad y la confidencialidad de los datos personales y cualquier otra información relativa a la actividad profesional en la U.G.R.

Gestión de documentos

1. Si hemos **sacado documentación de la** UGR por necesitarlo para nuestro trabajo la debemos custodiar lo mejor posible, bajo llave cuando no la utilicemos y hacer un inventario de documentos extraídos.

2. **Imprimir** en la **menor medida posible**, documentos en casa. Si se ha hecho, cuando se termine de trabajar custodiarlos bajo llave o garantizar que pueden ser a visualizados por terceras personas a través de cualquier otro medio.

3. Cuando el documento no sea ya útil **destruirlo** mediante máquina destructora, si se posee. En caso contrario, asegurarse de hacerlo en pedazos lo más pequeños posibles antes de tirarlo a la basura.

4. **Cuando termine el confinamiento**, si fuera necesario trasladar físicamente los documentos a la Universidad, hacerlo en un soporte físico cerrado, siempre con la debida vigilancia.

Puesto de trabajo, ordenador propio/local

1. Protegerlo con **contraseña**, usar **antivirus**, y activar el **firewall.**
2. Intentar que el **equipo** que se utilice sea **distinto al que emplee el resto de la unidad familia**r.
3. Con objeto de proteger nuestro portátil aconsejamos utilizar sistemas de cifrado de disco, en windows bitlocker, por si en algún desplazamiento perdemos el ordenador no puedan acceder a los contenidos del disco duro. Busca en la ayuda información sobre esto.
4. Para evitar la visualización o modificación, intencionada o no, de los miembros de la unidad familiar, **bloquear el dispositivo cuando nos levantemos**, en windows tecla windows + l, si es que no se posee de un protector de pantalla que automáticamente bloquee el acceso.
5. **Evitar hacer copias locales de los ficheros** (documentos, carpetas, etc.). Si nos resulta necesario guardar en nuestro ordenador o dispositivo personal un documento para trabajar, una vez terminada la tarea almacenarlo donde corresponda y eliminarlo a la mayor brevedad posible.
6. Hay que tener cuidado con las **memorias USB (pendrives)** personales y los ficheros que metemos en ellos como copias no autorizadas. Hay que evitarlo.
7. Importante prestar especial atención al **“phising”**: mensajes que te merezcan dudas o desconfianza. No debes de abrir, en ningún caso, ni los enlaces, ni los adjuntos que contengan.
8. Aconsejamos que las **claves** tanto de vpn como de otros servicios **se cambien con mas periodicidad**. Cada mes por ejemplo.
9. De la misma forma hay que intentar hacer un **uso moderado de los almacenamientos en la nube** de documentos de expedientes administrativos.
10. En **caso de pérdida del dispositivo de trabajo**, el trabajador debe avisar de la brecha de seguridad según protocolo establecido en protección de datos .

Animamos a que se consulten las medidas de seguridad para protección de datos en UGR, así como la normativa en materia de ENS (Esquema Nacional de Seguridad) para trabajo fuera de UGR.

RECUERDA que tú eres el responsable de la información, **contenga o no datos personales**, que estás manejando fuera del entorno universitario. Ante cualquier duda, envía un correo a protecciondedatos@ugr.es o seguridadinformatica@ugr.es

Comunicaciones de consejo de transparencia y protección de datos de Andalucía

- En el teletrabajo también se protegen los datos personales

Comunicación de la agenda española de protección de datos

Control de temperatura en el acceso a centros de trabajo

Nota informativa Protección de datos, 5 de mayo de 2020

La reciente nota informativa de la Agencia Española de Protección de Datos analiza el impacto y la adecuación a la normativa de protección de datos, de la medición de temperaturas como medida para frenar la transmisión del virus.

La toma de temperaturas, para garantizar el acceso a los centros de trabajo, **supone llevar a cabo un tratamiento de datos personales relativos a la salud** , que precisa de garantías adicionales y ajuste a la legalidad.

En este sentido, considera la AEPD que una correcta implementación de la medida precisa que la autoridad sanitaria competente, actualmente el Ministerio de Sanidad, determine, con carácter previo y sin perder de vista el objetivo principal, cómo ha de realizarse esta operación.

Ello se debe a que se requiere de un criterio uniforme y homogéneo, delimitado dentro de las posibilidades que ofrece la evidencia científica, para establecer un límite que, de superarse, permita denegar el acceso a los trabajadores a sus centros de trabajo sin que se produzca disparidad de decisiones en función del centro.

De manera más específica, la denegación de acceso ha de realizarse de forma que se minimice el impacto en la persona afectada, evitando, al ocurrir en espacios públicos y con la presencia de terceros, que se produzca una revelación de información personal.

En ningún caso ha de condicionarse el acceso a la prestación de consentimiento por el interesado a someterse a la medición, luego el fundamento jurídico que legitima este tratamiento de datos de carácter personal no podrá basarse ni en el consentimiento de los interesados, ni tampoco en la posible existencia de un interés legítimo de los responsables.

De conformidad con los artículos 6.1 y 9.2 del Reglamento General de Protección de Datos, el fundamento no es otro que el **deber de los empleadores de garantizar la seguridad y salud de los trabajadores a su servicio**, ponderando la incidencia en la esfera de derechos de clientes y usuarios y el nivel de protección de los trabajadores. Igualmente, podría fundamentarse en intereses generales en el terreno de la salud público, artículo 9.2.i), siempre y cuando exista respaldo normativo legal.

Concluye la AEPD, recalcando que **ha de limitarse el tratamiento a la finalidad de detectar posibles contagiados** y evitar su acceso a ciertos lugares y que han de utilizarse instrumentos que garanticen un alto nivel de precisión en la toma de temperaturas, **evitando emplear instrumentos como cámaras térmicas,** siempre que sea posible utilizar medios menos intrusivos.

En cualquier caso, **se debe cumplir con el deber de informar a los interesados,** y en particular del ejercicio de derechos, si se registran y conservan los datos, evento que sólo será posible en caso de que se pretenda utilizar como prueba frente a acciones legales fruto de una denegación de acceso al interesado.

- Acceso a documento completo
- Preguntas frecuentes dirigidas tanto a ciudadanos como a empresas
- Informe sobre tratamiento de datos relacionados con Covid-19
- Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo

Comunicaciones de la CRUE Universidades Españolas

- FAQS Covid-19_Grupo de Trabajo Delegados de Protección de Datos
- Informe sobre Procedimientos de Evaluación no Presencial. Estudio del Impacto de su Implantación en las Universidades Españolas y Recomendaciones
- Informe sobre el impacto normativo de los procedimientos de evaluación online: protección de datos y garantía de los derechos de las y los estudiantes

Covid-19: Ciberconsejos

Centro Criptológico Nacional (CCN)

- Ciberconsejo "Phishing"
- Ciberconsejo "Teletrabajo"
- Ciberconsejo "Videollamadas y reuniones virtuales"

Información amplia y detallada: "Principios y recomendaciones básicas en Ciberseguridad"

Secretaría de Estado de Digitalización e Inteligencia Artificial

- Recomendaciones ante ataques de ‘Phishing’ para personal en teletrabajo.
- Recomendaciones generales de ciberseguridad para usuarios.

Oficina de Seguridad del Internauta (OSI)

- Cómo poner freno a los fraudes y bulos con buenas prácticas.