Universidad de Valladolid
Secretaría General

Valladolid, 14/01/2019

En la madrugada del 10 al 11 de enero de 2019 la Universidad de Valladolid ha sido víctima de una violación de seguridad mediante acceso a datos a través del sitio web del Servicio de Relaciones Internacionales.

La Universidad de Valladolid comunica que ha sido víctima de un ataque y robo de datos personales alojados en la página web del Servicio de Relaciones Internacionales, hecho del que se ha tenido constancia en la madrugada del 10 al 11 de enero de 2019. La Universidad de Valladolid ha puesto estos hechos en conocimiento de la Agencia Española de Protección de Datos y ha formalizado una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado, que la han remitido a la Brigada de Delitos Tecnológicos. La Universidad mantiene un compromiso firme con los derechos de la comunidad universitaria y con la garantía del derecho fundamental a la protección de datos y de su seguridad. Desde la entrada en vigor del Reglamento Europeo de Protección de Datos el pasado 25 de mayo de 2018, la Universidad ha actualizado su esquema de seguridad para adaptarnos a la nueva normativa, y dispone de un Responsable de Privacidad y de un Delegado de Protección de Datos, además de un Comité de Seguridad de la Información. La Secretaria General, en su calidad de Responsable de la Información, del Servicio de Tecnologías de la Información y de las Telecomunicaciones, y del Desarrollo de la Política de Protección de Datos, ha asumido la gestión de este incidente. Estamos trabajando al servicio de la comunidad universitaria para mejorar la seguridad de los sistemas de información afectados y lamentamos las molestias que este incidente pueda ocasionar.

Desde el mismo momento en que hemos tenido conocimiento de estos hechos hemos activado los mecanismos establecidos para afrontarlos:

- Se ha procedido a iniciar la evaluación del incidente de acuerdo a los protocolos establecidos por el Esquema Nacional de Seguridad del Real Decreto 3/2010, de 8 de enero, en su art. 24.
- Se han seguido los protocolos de actuación y notificación a la Agencia Española de Protección de Datos según recoge el Reglamento General de Protección de Datos 2016/679, en su art. 33. A su vez, se ha tenido en cuenta lo dictado en la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales en sus disposiciones adicionales primera y novena.

In the early hours of January 10 to 11, 2019, the University of Valladolid was the victim of a security breach by which data was accessed through the website of the International Relations Service.

The University of Valladolid reports that it has been the victim of an attack and theft of personal data hosted on the website of the International Relations Service, a fact that has been recorded at dawn from January 10th to 11th, 2019. The University of Valladolid has brought these facts to the attention of the Spanish Agency for Data Protection and has formalized a complaint with the State Security Forces, which has sent it to the Technological Crimes Brigade. The University maintains a firm commitment to the rights of the university community and to the guarantee of the fundamental right to data protection and its security. Since the entry into force of the European Data Protection Regulation on May 25th, 2018, the University has updated its security scheme to adapt to the new regulations, and has a Privacy Officer and a Delegate for Data Protection, in addition to an Information Security Committee. The General Secretary, in her capacity as Responsible of the Information, of the Information Technology and Telecommunications Service, and of the Development of the Data Protection Policy, has assumed the management of this incident. We are working at the service of the university community to improve the security of the affected information systems and we regret the inconvenience that this incident may cause.

From the moment we have had knowledge of these facts, we have activated the established mechanisms to face them:

- Proceedings have been initiated to evaluate the incident according to the protocols established by the National Security Scheme of Royal Decree 3/2010, of January 8th, in its art. 24.
- We have followed the protocols of action and notification to the Spanish Agency for Data Protection as set out in the General Data Protection Regulations 2016/679, in its art. 33. In turn, the provisions of the Organic Law on Data Protection as well as the Digital Rights Guarantee have been taken into account in its first and ninth additional provisions.

Valladolid, 14/01/2019

Las operaciones llevadas a cabo o planificadas hasta la fecha son las siguientes:

1. Bloqueo de la máquina afectada. Volcado de la última copia de seguridad almacenada en una máquina diferente
2. Elaboración de un informe y remisión a la Agencia Española de Protección de Datos dentro del plazo establecido de 72 horas.
3. Identificación de las personas afectadas, y clasificación según el riesgo al que han sido expuestas. Redacción de un mensaje para cada una de dichas categorías.
4. Presentación de una denuncia ante las Fuerzas y Cuerpos de seguridad del Estado.
5. Envío de un mensaje en dos idiomas a las personas afectadas, con activación de un sistema de acuse de recibo para las cuentas que no son de la Universidad de Valladolid.
6. Notificación a la Agencia Española de Protección de Datos del envío de los citados mensajes.

Hemos de enfatizar que lo que se ha detectado ha sido una vulnerabilidad, pero no existen evidencias de que se haya causado ningún daño. El equipo de trabajo está evaluando esta posibilidad y la Universidad pondrá los medios necesarios en todos los niveles. En la sociedad actual los delincuentes tecnológicos son con frecuencia protagonistas de perpetrar ataques, incluso en los sistemas más seguros del mundo. Haber sido víctima de un ataque de esta naturaleza nos impulsa a apoyar a los posibles damnificados, porque la mayor preocupación de la Universidad de Valladolid son las personas.

Los detalles concretos y el alcance de este ataque que ha comprometido nuestra seguridad no pueden hacerse públicos, ya que ello podría afectar a las investigaciones que se están llevando a cabo e incidir negativamente sobre la propia seguridad.

La Universidad de Valladolid está trabajando intensamente con las autoridades y los expertos en seguridad informática para conocer el origen y alcance del ataque y minimizarlo al máximo.

The operations carried out or planned to date are the following:

1. Blocking of the affected machine. Dump of the last backup stored on a different machine.
2. Preparation of a report and referral to the Spanish Agency for Data Protection within the established period of 72 hours.
3. Identification of the people affected, and classification according to the risk to which they have been exposed. For each of these categories a message has been written.
4. Submission of a complaint to the State Security Forces and Bodies.
5. Sending a message in two languages to the affected people, with activation of an acknowledgment system for accounts that are not from the University of Valladolid.
6. Notification to the Spanish Agency for Data Protection of the sending of the aforementioned messages.

We must emphasize that what has been detected has been a vulnerability, but there is no evidence that any damage has been caused. The working team is evaluating this possibility and the University will put the necessary means at all levels. In today's society, technology criminals are often the protagonists of perpetrating attacks, even in the safest systems in the world. Having been the victim of an attack of this nature encourages us to support the possible victims, because the greatest concern of the University of Valladolid is the people.

The specific details and the scope of this attack that has compromised our security cannot be made public, since this could affect the investigations that are taking place and impact negatively on our own security.

The University of Valladolid is working intensively with the authorities and experts in computer security to know the origin and scope of the attack and minimize it to the maximum.