NORMATIVA DE USO DE LOS SISTEMAS DE INFORMACIÓN DE LA UNIVERSIDAD DE BURGOS

ACUERDO, de 28 de marzo de 2014, del Consejo de Gobierno de la Universidad de Burgos
BOUBU núm. 102, de 31 de marzo de 2014

TEXTO CONSOLIDADO
Última modificación: sin modificaciones

1. INTRODUCCIÓN

El Consejo de gobierno de la Universidad de Burgos, en su sesión de 30 de octubre de 2013, aprobó la Política de Seguridad de la Información, cumpliendo así la exigencia del Real Decreto

3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Dicha Política prevé en su punto 11 el desarrollo normativo de aspectos específicos de la misma. Uno de los aspectos más importantes de la gestión de la información corporativa, es el usuario final del sistema.

El artículo 5 del ENS establece que: «*La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad*».

El usuario final necesita disponer de unas normas de obligado cumplimiento respecto al uso de los sistemas informáticos a su alcance, y, con especial relevancia, en cuanto a preservar la confidencialidad de la información de carácter personal que pueda ser tratada en la realización de sus tareas y funciones.

El presente documento establece así las normas generales de uso de los recursos informáticos y dispositivos de comunicaciones, redes corporativas, sistemas de información, así como el control de acceso a las instalaciones, servicios y sistemas de la Universidad de Burgos.

Las normas más específicas de uso, se concretarán en Procedimientos que serán aprobados por el Comité de Seguridad de la Información. La Normativa y Procedimientos de Seguridad estarán a disposición de todos los miembros de la organización que necesiten conocerla en la intranet de la Universidad de Burgos, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Resulta, por tanto, fundamental que todos los usuarios de la Universidad de Burgos, que hagan algún tipo de uso de los sistemas de información institucionales, conozcan la presente normativa, sin perjuicio de que se lleven a cabo actividades formativas adicionales de carácter periódico o incluidas en los planes de formación al objeto de favorecer la difusión y el conocimiento de las buenas prácticas en materia de seguridad a todos los trabajadores.

2. ÁMBITO DE APLICACIÓN

La presente normativa será de aplicación a cualquier usuario de los sistemas de información de la Universidad de Burgos, entendiendo por tal a cualquier miembro de la comunidad universitaria, estudiantes, personal de administración y servicios, y personal docente e investigador, así como cualquier usuario de organizaciones externas o cualquier otro que utilice o tenga acceso a los sistemas de información de la Universidad.

3. USO DE LOS RECURSOS INFORMÁTICOS

El equipamiento, dispositivos, programas, información y servicios informáticos que la UBU pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones profesionales encomendadas.

Se evitará el uso privado de todos los recursos informáticos proporcionados por la Universidad de Burgos, que en caso de realizarse, debe limitarse a un tiempo razonable que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos disponibles.

Los usuarios deben tener en cuenta que por razones de mantenimiento y seguridad, los Sistemas de Información y la propia información que albergan, se inventarían y se monitorizan por parte del Servicio de Informática y Comunicaciones, guardando los correspondientes registros informáticos durante los plazos necesarios o legalmente establecidos.

3.1. Uso del equipamiento informático

La UBU facilitará a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional.

3.1.1. Uso aceptable del equipamiento informático

3.1.1.1. General

Los equipos deberán utilizarse fundamentalmente para fines institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.

Los usuarios:

a) Facilitarán al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento.

b) Evitarán comportamientos de riesgo para impedir el acceso y difusión de malware en los equipos.

c) Apagarán los equipos al finalizar la jornada laboral, tanto por seguridad como por eficiencia energética. El Servicio de Informática y Comunicaciones facilitará instrucciones y mecanismos que permitan un uso más eficiente de los recursos.

3.1.1.2. Administración e instalación de software en los servidores y equipos informáticos

Dada la naturaleza de los sistemas, la instalación y administración de los equipamientos de TI deben asignarse a personal especialista, con la preparación necesaria para una implementación segura y eficiente, acorde a la normativa.

Es responsabilidad de los miembros del Servicio de Informática y Comunicaciones la instalación, administración y mantenimiento del equipamiento de usuario. De manera excepcional, se podrán delegar dichas capacidades a los usuarios que lo soliciten y acepten de forma explícita las responsabilidades que conlleva, garantizando en todo momento el cumplimiento de esta normativa.

Los servidores adquiridos por departamentos, áreas o grupos de investigación deberán ser administrados por técnicos designados de forma explícita, que serán responsables de las tareas de administración y mantenimiento de acuerdo a esta normativa de uso.

3.1.1.3. Dispositivos portátiles

En el caso de los dispositivos portátiles (ordenadores, tablets, teléfonos móviles, etc.) deben tomarse las siguientes precauciones:

a) Deben vigilarse adecuadamente en los lugares públicos para evitar que sean sustraídos.

b) Evitar almacenar información sensible, confidencial o protegida en los ordenadores u otros dispositivos portátiles y eliminar periódicamente datos innecesarios.

c) Nunca almacenar contraseñas en archivos de texto ni almacenarlas en los navegadores de internet.

d) Tener actualizado y protegido convenientemente el equipo según las recomendaciones del Servicio de Informática y Comunicaciones.

e) Conectarse semestralmente a la red corporativa bien localmente o bien mediante VPN (Red privada virtual), para permitir la actualización de aplicaciones, sistema operativo, programa antivirus y demás medidas de seguridad.

f) Activar el salvapantallas con contraseña tras un periodo de inactividad.

g) Cuando se traten datos de nivel alto de seguridad o confidenciales, deberán tener cifrado el disco duro, y disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).

Esta medida se aplica tanto a portátiles propiedad de la Universidad como a portátiles privados, siempre que contengan información sensible, confidencial o protegida de la Universidad o se utilicen para conectarse a las aplicaciones, redes o sistemas de la Universidad.

3.2. Usos específicamente prohibidos de los equipos informáticos

Salvo autorización previa y expresa, las siguientes actuaciones están explícitamente prohibidas:

a) Alterar cualquier componente físico o lógico o la configuración de los equipos.

b) Instalar o utilizar programas sin licencia de uso o que vulneren la legislación vigente en materia de Propiedad Intelectual.

c) Utilizar cualquier tipo de software dañino.

d) Utilizar programas que, por su naturaleza, hagan un uso abusivo de la red.

e) Utilizar indebidamente el espectro radioeléctrico de la UBU.

f) No respetar los términos establecidos en las correspondientes licencias de uso de programas y aplicaciones informáticas.

4. USO DE LAS COMUNICACIONES

El acceso a la red de comunicaciones de la Universidad de Burgos estará restringido a los usuarios a los que hace referencia el punto 2 de esta normativa.

Esta normativa aplica a la utilización del conjunto de elementos que conforman la red corporativa de la Universidad de Burgos, bien desde localizaciones físicas pertenecientes a la propia Universidad (ubicados en los Centros y Edificios de la misma), bien desde ubicaciones no pertenecientes a la Universidad pero que como consecuencia de convenios o relaciones contractuales utilizan dicha red, o bien desde cualquier otra ubicación que utilice de una manera u otra, la red de la Universidad de Burgos.

Puesto que la red de comunicaciones de la Universidad de Burgos es para el uso de las tareas que autoriza dicha Universidad, se aceptarán las posibles revisiones de información que por la mencionada red circulen, independientemente del servicio de red que provoque la circulación de información, siempre que para ello exista el oportuno requerimiento legal (basado en la sospecha fundada del incumplimiento de la presente normativa), por necesidades del órgano responsable de la información, o por razones de emergencia (cuando exista riesgo de repercusión grave para la red de datos de la Universidad de Burgos, para los dispositivos conectados a ella, o para los servicios o informaciones que en ella se contengan). Este punto será rigurosamente aceptado a menos que de manera previa, expresa y particular se especifique lo contrario.

Todos los usuarios de la red de comunicaciones de la Universidad de Burgos tienen la obligación de cooperar activamente con el Servicio de Informática y Comunicaciones, tanto en las

tareas de mantenimiento del inventario de los recursos, como en su disposición y uso. Igualmente tienen la obligación de cooperar en las tareas de diagnóstico, que faciliten la resolución de las incidencias técnicas que se puedan producir.

Igualmente será de aplicación a los usuarios de la red de la Universidad de Burgos, las políticas de uso de red y resto de normativas de la Comunidad de RedIRIS, por pertenecer la Universidad de Burgos a dicha Comunidad.

Únicamente se permitirá la conexión a la red cableada de comunicaciones de la Universidad de Burgos, bien de manera física o remota, a aquellos equipos terminales (ordenadores, estaciones de trabajo, servidores, periféricos, etc.) que hayan sido autorizados, previo informe favorable del Servicio de Informática y Comunicaciones, y que utilicen la infraestructura de cableado autorizada por dicho Servicio.

4.1. Usos específicamente prohibidos de las comunicaciones

Las siguientes actuaciones están explícitamente prohibidas:

a) Utilizar los recursos de manera ilícita o ilegal; y particularmente difundir contenidos de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorios contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor o a la propia imagen o a la dignidad de la persona.

b) Difundir contenidos atentatorios contra los principios enunciados en los Estatutos de la Universidad de Burgos.

c) Difundir manifestaciones o referencias falsas, incorrectas e inexactas sobre las páginas y los servicios de la Universidad de Burgos. Quedan excluidas de los usos prohibidos las opiniones de todo tipo en relación con la Institución.

d) El uso ilícito por parte de terceras personas de recursos asociados a un usuario (con conocimiento o no del usuario oficial), tanto por quien realiza el acceso indebido como por el responsable de los recursos.

e) Suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa, salvo al personal técnico expresamente autorizado en relación con las funciones de su puesto, garantizando, en todo caso, la privacidad de los datos consultados.

f) Descargar programas informáticos o ficheros con contenido dañino que supongan una fuente de riesgos para la organización.

g) La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.), salvo autorización expresa del Servicio de Informática y Comunicaciones.

h) Realizar actividades que pongan en peligro la integridad o seguridad de la Información disponible en la red.

i) Realizar de forma intencionada acciones cuyo fin sea la obtención de claves, permisos o algoritmos de cifrado distintos a los asignados, así como revelar identificadores o contraseñas, o permitir que sea difundida información que facilite el acceso no autorizado a cualquier sistema de la Universidad.

j) Usar herramientas para averiguar información para la que no se tiene permiso de acceso.

k) La alteración de la integridad de los datos que circulen por la red de comunicaciones de la Universidad de Burgos, o que se encuentren contenidos en alguno de los equipos conectados a la misma, así como alterar o manipular registros o log de manera que se falseen sus resultados.

l) La conexión de equipos a la red de comunicaciones de la Universidad de Burgos sin autorización previa del Servicio de Informática y Comunicaciones, en especial de aquellos que modifiquen la topología (diseño físico) de la misma (repetidores, módems, enrutadores, pasarelas), salvo autorización particular, expresa y escrita del citado Servicio.

m) La conexión a la red de comunicaciones de la Universidad de Burgos de equipos que utilicen direcciones IP no autorizadas, o el uso de protocolos de comunicación sin previo consentimiento expreso por parte del Servicio de Informática y Comunicaciones.

n) La utilización de «agujeros» en la seguridad de la red y/o de los sistemas informáticos de la Universidad de Burgos o de fuera de ella, o el uso de estos sistemas para atacar a cualquier otro sistema informático de dentro o fuera de la red de comunicaciones de la Universidad de Burgos.

ñ) La creación, instalación, difusión o uso de programas, elementos perturbadores o informaciones que puedan ser utilizados para atacar a sistemas informáticos de la red de comunicaciones de la Universidad de Burgos, o a sistemas informáticos que se encuentren fuera de ella.

5. USO DEL CORREO ELECTRÓNICO

Todos los usuarios que lo precisen para el desempeño de su actividad, dispondrán de una cuenta de correo electrónico proporcionada por la Universidad.

5.1. Recomendaciones de uso del correo electrónico

a) Asegurarse de que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

b) Hacer un uso eficiente en los envíos de correo: agrupar los envíos a múltiples destinatarios en un solo mensaje, evitar la incorporación de firmas escaneadas, imágenes y fondos como formato habitual de los correos (ya que incrementan innecesariamente el tamaño y volumen de los mismos), envíos innecesarios, etc.

c) Vaciar los buzones de correo cuando se esté alcanzando su límite de almacenamiento. El sistema indicará cuándo se encuentra al límite de su capacidad, tras el cual no se permitirá enviar y recibir correos.

d) Evitar intercambiar o descargar ficheros voluminosos. El sistema evitará el intercambio de correos de tamaños superiores a lo establecido por el Servicio de Informática y Comunicaciones de acuerdo a los recursos disponibles.

5.2. Usos específicamente prohibidos del correo electrónico

Las siguientes actuaciones están explícitamente prohibidas:

a) Transmitir, distribuir o almacenar cualquier material ilegal, difamatorio o discriminatorio, programas informáticos (software) sin licencia, material que vulnere derechos de propiedad intelectual, mensajes o cartas en cadena o cualquier otro tipo

de contenidos que puedan perjudicar a los usuarios y a los propios sistemas de información de la Universidad.

b) Distribuir o facilitar la distribución de mensajes no deseados (spam) y la participación en cadenas de mensajes electrónicos.

c) Responder a mensajes en los que se soliciten las claves de acceso al correo electrónico.

d) Acceder a un buzón de correo electrónico distinto del propio, salvo autorización expresa del propietario del mismo o en su presencia.

e) Difundir la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.

f) El uso indiscriminado o personal de listas de distribución (listas de usuarios de correo electrónico, etc.).

6. USO DE LA INFORMACIÓN

6.1. Uso aceptable de la información

Las normas de uso son:

a) La información contenida en los Sistemas de Información o que circule por sus redes de comunicaciones debe ser utilizada fundamentalmente para el cumplimiento de las funciones profesionales del usuario.

b) Los usuarios sólo podrán acceder a la información sensible, confidencial o protegida para la que posean autorización explícita, manteniendo absoluta reserva sobre la misma.

c) Se evitará almacenar información sensible, confidencial o protegida en medios desatendidos (tales como CDs, DVDs, memorias USB, listados, etc.) o dejar visible tal información en la misma pantalla del ordenador. Los documentos en papel que contengan este tipo de información, deben custodiarse bajo llave.

d) Los usuarios deberán almacenar sus ficheros de trabajo en las carpetas de red que le hayan sido asignadas, que son sobre las que se realizan copias de seguridad. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario, que deberá ser realizada por el propio usuario.

e) Sólo deberá salvaguardarse la información que se considere estrictamente necesaria, haciendo un uso razonable de la capacidad de almacenamiento disponible.

f) Se evitará almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartido o local.

g) Cuando se utilicen equipos de manipulación de documentos (faxes, impresoras, escáneres, etc.), se retirarán inmediatamente los documentos en papel, tanto los originales como sus copias de los equipos.

h) Cualquier tratamiento en los Sistemas de Información deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo.

i) En el caso de que deban transmitirse fuera de la universidad datos sensibles, confidenciales o protegidos, se cifrarán o se utilizará cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte.

j) Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras disponibles de forma que no sea recuperable la información que pudieran contener.

k) Los soportes de información que deban ser destruidos o vayan a ser reutilizados se procesarán según lo definido en el procedimiento de Protección de la información.

6.2. Usos específicamente prohibidos de la información

Sin perjuicio de lo establecido en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE núm. 295 de 10 de diciembre de 2013) y en su correspondiente normativa de desarrollo, salvo autorización previa y expresa, las siguientes actuaciones están explícitamente prohibidas:

a) Acceder a información sensible, confidencial o protegida sin la debida autorización.

b) Comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) información sensible, confidencial o protegida propiedad de la UBU.

c) Publicar o transmitir información sensible, confidencial o protegida, a personas, empresas o sistemas de información externos a la misma o no autorizados.

d) Si se autorizara lo anterior, se comprobará la inexistencia de trabas legales para ello y se establecerá un contrato que incluya provisiones para la protección de la información proporcionales a los riesgos asociados a tal externalización.

e) Extraer información sensible, confidencial o protegida fuera de la organización por cualquier medio, correo electrónico, dispositivos móviles (portátiles, teléfonos) o soportes tales como memorias USB, CDs, DVDs, etc., salvo en la medida que las funciones del usuario lo requieran.

f) Realizar cualquier actividad de promoción de intereses personales.

7. CONTROL DE ACCESO

Todo usuario dispondrá de unas credenciales, usuario y contraseña, que serán personales e intransferibles, con los que se realizará el inicio de sesión y el acceso a los sistemas de información a los que esté autorizado. Es responsabilidad del usuario custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad que elabore la UBU, para garantizar que aquellas no puedan ser utilizadas por terceros. En caso de detectar que sus credenciales pueden estar siendo usadas por otra persona, deberá poner este hecho inmediatamente en conocimiento del Responsable de Seguridad.

7.1. Acceso físico a las instalaciones

7.1.1. Áreas públicas

El acceso a las áreas públicas no está restringido. En estas áreas no se ubicarán equipos o información sensible, confidencial o protegida que puedan ser accedidos por terceros sin autorización.

En áreas en las que se lleven a cabo tareas de atención a usuarios, no se mantendrán documentos sobre las mesas y en las pantallas, que no deban ser visibles por terceros sin autorización. Debe mantenerse especial precaución en zonas en las que se trate información sensible o confidencial y, en los casos en los que se manejen datos de carácter personal, observar las medidas de seguridad aplicables.

7.1.2. Áreas restringidas

Para el acceso a las áreas restringidas (centros de datos, salas de servidores, etc.) se necesitará autorización previa.

En el caso de que visitantes o personal no autorizado deba acceder a las instalaciones o a la información, deberá estar siempre acompañado por un miembro responsable y autorizado de la organización que controlará en todo momento que la seguridad de los recursos esté garantizada.

7.2. Acceso a los sistemas de información

Cada sistema cuenta con un mecanismo de control de acceso. Para entrar, siempre será necesario autenticarse ante el sistema con las claves de acceso que se le proporcionen al usuario para ello.

Los usuarios tienen las siguientes obligaciones respecto a la gestión y utilización de sus claves de acceso:

a) Custodiarlas diligentemente velando por preservar la confidencialidad de las mismas, por lo que no se anotarán en soportes accesibles a otros usuarios.

b) Deberán cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo dejen desatendido.

c) Las claves de acceso se crearán y utilizarán de acuerdo con las instrucciones establecidas por el Servicio de Informática y Comunicaciones.

- Deben ser suficientemente complejas y difícilmente deducibles por terceros, evitando emplear como contraseña el propio identificador.
- Se evitará utilizar como contraseña palabras sencillas o relacionadas con el usuario tales como el nombre propio, el DNI, la matrícula del coche, la fecha de nacimiento, etc.
- Deben ser renovadas, obligatoriamente, cada doce meses.
- Deben ser distintas, por lo menos, a las tres contraseñas anteriores.
- Debe evitarse utilizar la misma contraseña para los servicios de la UBU y servicios ajenos a la misma.
- En el caso de que participen otras personas en su creación o distribución, deben ser cambiadas obligatoriamente, la primera vez que el usuario la utilice.
- El usuario deberá proceder a cambiar la contraseña de forma inmediata en el caso de que se haya visto comprometida o se sospeche que lo puede haber sido, se olvide de ella o se le bloquee el acceso tras varios intentos fallidos.

8. DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO

La información de la UBU que comprenda datos de carácter personal está protegida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su normativa derivada o de desarrollo.

Para garantizar dicha protección, se han adoptado las medidas de seguridad que se correspondan con las exigencias previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

El Documento de Seguridad, al que se podrá acceder a través de la intranet de la Universidad de Burgos, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas

de información de la Universidad de Burgos se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

En aplicación del artículo 10 de la LOPD, todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la UBU.

9. INCIDENCIAS DE SEGURIDAD

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de las instalaciones o los sistemas de Información de la UBU, o cualquier posible infracción de la presente Normativa, deberá informar inmediatamente al Responsable de Seguridad.

El Responsable de Seguridad se encargará de que se registren debidamente los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan, informando al Comité de Seguridad de la Información para tomar las acciones organizativas y legales que apliquen en cada caso.

Estos registros se emplearán para la mejora continua de la seguridad del sistema.

10. RESPONSABILIDADES Y COMPROMISOS DE LOS USUARIOS

Cada usuario es responsable del equipamiento que la Universidad le ha confiado para el desarrollo de sus funciones profesionales.

Las labores de instalación, mantenimiento, reparación, configuración del sistema operativo, manipulación de los mecanismos de seguridad o traslado, se realizarán por el personal técnico del Servicio de Informática y Comunicaciones o personal autorizado a tal fin, debiendo los usuarios respetar la integridad de los equipos, sin ocasionar daños físicos o lógicos por un uso negligente de los mismos.

El usuario es responsable de realizar las copias de seguridad o de tomar otras medidas de respaldo de la información contenida en los discos duros locales del equipo. El Servicio de Informática y Comunicaciones se encargará de las copias de seguridad y recuperación de los datos contenidos en el sistema de almacenamiento centralizado. Los usuarios deberán almacenar sus ficheros de trabajo en las carpetas de red que le hayan sido asignadas, que son sobre las que se realizan copias de seguridad.

Todo usuario deberá proteger la información sensible, confidencial o protegida, evitando su envío no autorizado al exterior, incluyendo la visualización de la misma por personal no autorizado.

La descarga o instalación de software con propiedad intelectual de un tercero estará sometida a las condiciones expresadas en el Contrato de licencia para el usuario final de cada producto. El incumplimiento de estas condiciones es responsabilidad del usuario.

Los usuarios se comprometen a no acceder a los sistemas y recursos de la UBU para desarrollar actividades que persigan o tengan como consecuencia:

- El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.
- La degradación de los servicios.

- La destrucción o modificación no autorizada de la información, de manera premeditada.
- La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
- El deterioro intencionado del trabajo de otras personas.
- Dañar intencionadamente los recursos informáticos propios o ajenos.
- Incurrir en cualquier otra actividad ilícita, del tipo que sea.
- Efectuar cualquier tratamiento con los datos suministrados por la Universidad o recibidos de terceros, para finalidades distintas del cumplimiento de la función encomendada a su puesto de trabajo.
- El tratamiento de los activos de información de manera contraria a las pautas definidas por la Universidad.
- Alterar, evitar o saltarse las medidas de seguridad informática configuradas en el equipo entregado.

11. INCUMPLIMIENTO DE LA NORMATIVA

Ante un posible incumplimiento de la presente normativa que pueda suponer un perjuicio para los sistemas y recursos de la Universidad, el Responsable de Seguridad, en el ejercicio de sus funciones, podrá proceder a la suspensión cautelar del servicio prestado y/o bloqueo temporal de sistemas, cuentas o accesos a la red de forma preventiva, con el fin de garantizar el buen funcionamiento de los servicios de la Universidad.

En los demás supuestos de incumplimiento, se advertirá del hecho al infractor. En caso de que el usuario no responda o ignore la advertencia, el Comité de Seguridad de la Información de la Universidad podrá solicitar al Rector, o Vicerrector en quien delegue, la adopción de las medidas de suspensión cautelar de los servicios prestados y/o bloqueo de sistemas.

Todo ello sin perjuicio de iniciar las acciones disciplinarias, administrativas, civiles y/o penales que en su caso correspondan, en relación con las personas presuntamente implicadas en dicho incumplimiento.

La Universidad de Burgos pondrá en conocimiento de la autoridad judicial y las Fuerzas y Cuerpos de Seguridad del Estado aquellas infracciones que pueden ser constitutivas de delito.

La Universidad de Burgos se reserva el derecho a iniciar las acciones legales oportunas en aquellos supuestos contemplados en los artículos 263 a 267 (delito de daños) y 270 y siguientes del Código Penal (delitos contra la propiedad intelectual); en los artículos 43 a 48 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en los artículos 37 a 45 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

12. PROCEDIMIENTO Y GARANTÍAS DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

Según lo establecido en el artículo 23 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, la Universidad de Burgos, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la información necesaria para monitorizar,

analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Dicha información será retenida solamente durante los plazos necesarios o legalmente establecidos.

Se respetará en los términos establecidos en las normas vigentes la privacidad en el uso de la red de comunicaciones y del contenido de los mensajes de correo electrónico, sin menoscabo de la capacidad de la universidad de Burgos para la aplicación de programas de detección y eliminación de virus y programas de filtró anti-spam a los mensajes que llegan a la estafeta de la Universidad.

No obstante lo anterior, la Universidad de Burgos podrá intervenir y examinar el uso de los sistemas de información y el contenido de los mensajes y buzones de los usuarios en alguna de las siguientes circunstancias:

a) Cuando el responsable o usuario lo solicite, para detectar y corregir posibles problemas que afecten al normal funcionamiento de los sistemas y servicios.

b) Cuando sucedan eventos que afecten al funcionamiento general del servicio, para detectar el origen y las causas del problema.

c) Cuando el Comité de Seguridad de la Información de la Universidad detecte indicios claros, sospechas fundadas o reciba denuncia de incumplimiento en materia de seguridad.

d) Por requerimiento judicial o de las Fuerzas y Cuerpos de Seguridad del Estado.

Asimismo, la Universidad de Burgos, en cumplimiento de los dispuesto en el artículo 103 del real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, registrará los accesos que sus usuarios realicen o intenten realizar a los ficheros con datos de carácter personal. Los accesos podrán ser revisados y controlados, previa solicitud del Secretario General de la Universidad, como responsable de la información, en el supuesto de que se produzcan accesos no autorizados o mal uso de la información, con el fin de poder determinar las responsabilidades en las que, en su caso, hayan podido incurrir los miembros de la comunidad universitaria.

13. EXENCIÓN DE RESPONSABILIDAD

La Universidad de Burgos no tendrá responsabilidad u obligación legal por la pérdida de datos, errores en las comunicaciones o cualquier otro daño o perjuicio cuando estos se deriven de acciones efectuadas durante las tareas de mantenimiento normal de los servicios o durante situaciones especiales o de emergencia.

La Universidad de Burgos queda eximida de cualquier responsabilidad derivada del mal funcionamiento de los servicios que tenga su origen en una circunstancia accidental, de fuerza mayor o de cualquier otra causa no imputable a la misma.

14. ENTRADA EN VIGOR

La presente normativa entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Universidad de Burgos.

HISTORIA DE LA NORMA

Texto original: CG de 28/03/2014 (BOUBU de 31/03/2014)

Modificaciones: sin modificaciones