UNIVERSIDAD DE BURGOS

MEDIDAS DE SEGURIDAD Y PRIVACIDAD

1. SEGURIDAD EN EL USO DE MEDIOS INFORMÁTICOS

1. No se almacenarán recursos que contengan datos personales en medios privados propios.

2. Se utilizarán las unidades para el almacenamiento de información o medios análogos autorizados por la Universidad.

2. CONTROLES DE ACCESO FÍSICO Y LÓGICO

3. La información se almacenará en medios, recursos o áreas sólo accesibles a personas autorizadas.

4. Cada usuario podrá acceder exclusivamente a los recursos y sistemas de información autorizados.

5. Los ordenadores y equipos vinculados al desarrollo del proyecto deberán disponer de un sistema de validación de usuario y contraseña.

6. En caso de ausencia del puesto de trabajo en espacios que no excluyan a terceros debe procederse al bloqueo del puesto que en todo caso deberá producirse automáticamente tras 15 minutos de inactividad. En particular, cuando se trate de ámbitos como una biblioteca el propio usuario deberá bloquear el acceso al abandonar el puesto.

7. En el diseño del puesto de trabajo se asegurará que la pantalla no resulte accesible o legible para terceros no autorizados.

8. Debe procederse a apagar el ordenador al finalizar el periodo de trabajo, así como evitar el uso del mismo por terceras personas.

9. Las contraseñas no deben ser almacenadas en ficheros legibles, macros, PCs sin control de acceso o ningún otro lugar donde puedan ser accedidas por personas sin autorización.

10. Es recomendable proceder al cambio de contraseñas periódicamente cuando lo solicite el sistema, o en todo caso a iniciativa propia. Siempre deberá utilizar contraseñas seguras que incorporen ocho o más caracteres, mayúsculas, números o signos y que no deben ser palabras, nombres o conceptos. Se considera que el periodo razonable de cambio de una contraseña abracará como mínimo ciclos de seis meses.

11. Nunca se facilitarán los datos de usuario y contraseña a ningún tercero.

12. El acceso remoto a los sistemas de información de la Universidad de Burgos deberá realizarse a través de la red privada virtual o bien a través de los medios seguros que proporciona la Universidad. El usuario aplicará al equipo que utilice las normas de seguridad contenidas en este apartado para los equipos ubicados en puestos de la Universidad de Burgos.

3. USO, MANTENIMIENTO Y DESTRUCCIÓN DE DISPOSITIVOS O SOPORTES QUE CONTENGAN INFORMACIÓN PROTEGIDA

13. Cuando ello fuera posible la información objeto de tratamiento en soporte no automatizado (papel) se almacenará en dispositivos cerrados con llave o en salas o despachos habilitados por la Universidad de Burgos y de acceso exclusivo para las personas autorizadas. Durante su utilización se encontrará siempre bajo la custodia de un usuario autorizado.

14. Como regla general, se recomienda no sacar la documentación de trabajo fuera de los despachos y espacios físicos destinados al mismo.

15. No se debe dejar abandonada información en la impresora, fax o dispositivos similares, o desatendida en el puesto de trabajo.

16. Cuando la información sea calificada como restringida o confidencial deberá guardarse en los lugares designados al efecto por el usuario al final de la jornada y, en todo caso, al abandonar el puesto cuando su conformación no permita que esté bajo el control de algún usuario.

17. Antes de abandonar salas comunes o permitir que alguien ajeno entre, se limpiarán adecuadamente las pizarras de las salas de reuniones o despachos que contuvieran información relacionada con el proyecto, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.

18. La impresión o fotocopia de documentos debe limitarse únicamente a aquellos que sean estrictamente necesarios y preferiblemente a doble cara. Los documentos desechados, incluidas las fotocopias erróneas no podrán ser reutilizados cuando contengan datos personales o información confidencial o restringida debiéndose proceder a su inmediata destrucción.

19. En el caso de reutilización de documentos impresos el usuario comprobará previamente que éstos no contienen datos de carácter personal, comunicando la incidencia en caso contrario.

20. La destrucción de cualquier tipo de soporte automatizado (CD, DVD, Disco duro, Pendrive, etc.) o manual (papel, cintas de vídeo, etc.) se realizará de forma que los datos que contenían no sean recuperables y en su caso a través de los procedimientos establecidos.

21. No podrán donarse soportes informáticos que contengan información protegida a ningún tercero sin que previamente se haya realizado un borrado completo del mismo.

22. Queda prohibido alojar información confidencial o restringida propia de la Universidad de Burgos en servidores externos en la "nube" no ofrecidos por la propia institución, en particular cuando se trate de datos personales contenidos en los sistemas de información. Para ello se hará uso de los espacios de disco corporativos.

23. El usuario es responsable de un uso adecuado de los dispositivos portátiles. Debe mantenerlos bajo su custodia y no permitir su uso a ningún tercero. Si se conecta externamente a la Universidad debe hacerlo siempre mediante la red privada virtual VPN. Si el dispositivo fuese robado o extraviado debe notificarse inmediatamente a la Universidad de Burgos, siguiendo el Procedimiento de Gestión de Incidencias.

4. CORREO ELECTRÓNICO Y RED CORPORATIVA

24. El envío de datos o información a terceros (cesión de datos), por medio del correo electrónico, transferencia FTP o equivalente deberá estar autorizada, por el responsable para la finalidad exclusiva para la cual sea necesario. Cuando la información sea calificada como confidencial sólo será admisible mediante un procedimiento que impida accesos no autorizados.

25. No deben abrirse correos electrónicos no solicitados, de remitentes desconocidos o de remitentes conocidos que puedan levantar sospechas. Asimismo, no deben ejecutarse archivos no confiables.

26. El usuario se hace responsable de los accesos a Internet que puedan comprometer la seguridad del equipo.

27. El acceso a información corporativa se realizará a través de la red de datos corporativa. También se realizará mediante la Intranet, cuyo acceso estará limitado a los usuarios que deban usarla mediante autenticación por nombre de usuario y contraseña.

5. RECURSOS INFORMÁTICOS

28. Todo usuario debe mantener actualizados los sistemas operativos, antivirus y cortafuegos (firewalls) de su equipo de trabajo mediante actualizaciones automáticas y en todo caso de acuerdo con los procedimientos consultables a través del Centro de Atención al Usuario.

6. INCIDENCIAS DE SEGURIDAD

29. El usuario debe comunicar cualquier Incidencia de Seguridad que a su juicio ponga en peligro información protegida mediante notificación al responsable de seguridad de la Universidad de Burgos.

7. PUBLICACIÓN

30. La publicación de contenidos relacionados con el proyecto se limitará a los documentos o informaciones de carácter público o en todo caso a aquellos para los que se haya obtenido la debida autorización.

31. La información publicada debe garantizar los principios de proporcionalidad, autenticidad e integridad. En todo caso, no se publicará información que pueda lesionar la dignidad de las personas y en particular de los menores de edad que en ningún caso podrán ser identificados o identificables.

8. AUTORIZACIONES

32. La recogida de información personal o corporativa, así como la captación de imágenes y sonidos sólo será posible cuando se haya obtenido previamente la debida autorización.

33. En caso de los menores o incapaces esta autorización corresponderá al padre, madre o representante o tutor legal, en su caso previa información a los responsables del centro educativo o equivalente.