Política de Seguridad de la Información de la Universidad de La Laguna

(Aprobada en el Consejo de Gobierno del 27 de marzo de 2015)

La Universidad de La Laguna (ULL) ha ejercido una importante función de liderazgo educativo, científico y cultural en Canarias durante sus más de dos siglos de historia, impulsando el progreso de nuestra comunidad y contribuyendo decisivamente a su modernización. Conforme a esta tradición, la ULL establece como su principal misión social, contribuir al bienestar de los ciudadanos de Canarias, garantizándoles una educación superior de calidad, impulsando el desarrollo económico mediante una investigación científica y técnica de alto nivel y difundiendo la cultura, el conocimiento científico y las artes a lo largo de todo el Archipiélago mediante sus actividades de extensión universitaria.

La ULL depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El Servicio TIC tiene la misión de planificar, coordinar y gestionar los recursos de comunicación e informáticos de carácter general que soportan técnicamente, en el campo de las TIC, las tareas de gestión universitaria, docencia e investigación. Estas actividades convierten al Servicio TIC en un servicio transversal íntimamente ligado con todos los ámbitos universitarios, facilitando y promocionando el acceso a las tecnologías de la información y gestionando los recursos y servicios tecnológicos en el ámbito de las TIC, a fin de contribuir a los objetivos de la ULL.

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, hace referencia en su articulado a la Política de Seguridad. Así, dispone en su artículo 11.1 lo siguiente: *Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.* Asimismo, en su artículo 12 establece que "*La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad, según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa"* Y, finalmente, en el apartado 3 de su Disposición transitoria se contempla que "*Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo"*.

El presente documento establece la Política de Seguridad de la Información de la ULL y determina como va a ser gestionada dentro de la organización.

Esta Política de Seguridad contempla las disposiciones y regulaciones en este ámbito establecidas por las siguientes normativas:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE nº 298. de 14 de diciembre).
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (BOE nº 166, de 12 de julio).
- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (BOE nº 150, de 23 de junio).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre (BOE nº 17, de 19 de enero de 2008).
- 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 (BOE nº 25, de 29 de enero).
- Estatutos de la Universidad de La Laguna (BOC nº 143, de 26 de Julio de 2004).

El Comité de Seguridad TIC de la ULL estará formado por las personas titulares del Vicerrectorado con competencias en TIC, que ejercerá la Presidencia por delegación del Rector o Rectora, la Secretaría General, la Gerencia, la Secretaría Técnica de Secretaría General, que realizará las funciones de Secretaría del Comité, la Jefatura del Servicio TIC, la Jefatura del Área de Infraestructuras TIC, la Jefatura del Área de Servicios TIC y la Jefatura del Área de Soporte a Usuarios y Gestión de la Calidad. La persona que ostente la secretaría del Comité será la responsable de custodiar toda la información relacionada con el proceso de mejora continua de la gestión de la seguridad de la institución. Esté Comité reportará al Consejo de Dirección todos los incidentes y acciones relacionadas con la seguridad TIC y será responsable de revisar anualmente esta política de seguridad proponiendo modificaciones y mejoras a la misma.

Las TIC se han convertido en un elemento transversal que afecta a todos los ámbitos de la organización. Uno de los elementos más críticos en el acceso a las TIC es la gestión de sus usuarios y sus credenciales. Esta política tiene como objetivo cubrir los sistemas implicados con la gestión de usuarios de la ULL. En ella se regulan los sistemas que mantienen los datos de los usuarios de la institución. Esto incluye las infraestructuras que almacenan los usuarios con sus datos principales, las aplicaciones que manejan los datos para añadir, borrar y modificar los usuarios y las aplicaciones que usan las credenciales de los usuarios para la autenticación. También se incluye en ella el Centro de Atención al Usuario (CAU), que tiene capacidad para cambiar los datos relacionados con el usuario.

Para garantizar el cumplimiento de esta política las actuaciones técnicas deberán contemplar los siguientes aspectos:

- Los datos de los usuarios serán mínimos (DNI, Usuario y Contraseña) y se almacenarán sólo en el sistema central de Gestión de Identidades de la ULL.
- Las aplicaciones que puedan modificar estos datos de usuario sólo serán accesibles desde las redes internas del Servicio TIC o desde los sitios previamente autorizados por el Servicio TIC. Todos los accesos realizados por estas aplicaciones quedarán registrados indicando el personal técnico o sistema que realiza la operación, el usuario afectado y los datos modificados. Esto se registrará en el sistema central de registros (logs) de la institución.
- El usuario será informado por correo electrónico y/o SMS de todas las modificaciones que se realicen en sus datos de usuario.
- Las aplicaciones de validación de usuarios deberán usar CAS (Central Authentication Service), siempre que sea posible, para garantizar que el usuario nunca introduce su contraseña en un aplicativo no controlado. El sistema CAS devolverá a la aplicación del usuario el DNI y el usuario con el que se realizado la validación junto con los datos concretos que necesite cada aplicativo para su funcionamiento.

El Servicio TIC será el responsable de garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos de los usuarios. Los sistemas que provean los servicios de acceso y validación estarán monitorizados 24 horas al día los 7 días de cada semana (régimen 24x7) y considerados como críticos en el nivel de redundancia, recuperación, disponibilidad y planes de contingencias. Se garantizará la integridad y la seguridad de las copias diarias de los datos durante un periodo de 1 año.

Los objetivos que se pretenden alcanzar son los siguientes:

- Disponer de un único almacén con todos los usuarios de los servicios TIC de la institución, garantizando la coherencia y fiabilidad de los datos.
- Lograr una disponibilidad del 99,99% para los sistemas de control de acceso.
- Disponer de una trazabilidad exacta de todas las modificaciones relacionadas con las credenciales del usuario.

La Política de Seguridad de la Información de la ULL establecida en este documento, así como todos los Reglamentos e Instrucciones que la desarrollen, en su caso, serán de público y general conocimiento para todos los miembros de la comunidad universitaria.

La Política de Seguridad de la Información de la ULL establecida en el presente documento entrará en vigor al día siguiente de su aprobación por el Consejo de Gobierno.