UNIVERSIDADE DA CORUÑA

REGLAMENTO GENERAL DE USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN DE LA UNIVERSIDAD DE A CORUÑA

Aprobada por el Consejo de Gobierno del 23 de julio de 2020

Preámbulo

La Universidad de A Coruña (UDC) aprobó, mediante resolución rectoral del 22 de julio de 2019, su política de seguridad de la información y protección de datos personales (en adelante, la Política) con el fin de crear las bases para la implantación de un sistema de gestión de la seguridad de la información, según lo requerido en el Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Esta Política considera que, para su desarrollo, se aprobarán en Consejo de Gobierno las normas que sean necesarias en materia de seguridad de la información y de protección de datos.

Habida cuenta de la gran importancia que las tecnologías de la información y la comunicación (TIC) tienen en el tratamiento de la información y el potencial impacto de estas tecnologías sobre los derechos y las libertades de las personas, así como en el cumplimiento de los objetivos de nuestra universidad, se hace necesario regular su uso en la UDC según los principios, objetivos y directrices de dicha Política.

El presente reglamento, que contiene los aspectos generales que deben regir el uso de las TIC en la UDC, como el ámbito de aplicación, los derechos y deberes de las personas usuarias, las condiciones generales de uso de los recursos, los usos no permitidos y las consecuencias de un posible incumplimiento, se complementará con el desarrollo normativo necesario para regular el uso de recursos específicos.

Artículo 1. Objeto

Este reglamento tiene por objeto establecer las condiciones de uso de los recursos TIC de la UDC como instrumento clave en el manejo de la información corporativa, así como los derechos y deberes de las personas usuarias en la utilización de estos.

Artículo 2. Ámbito objetivo de aplicación

Este reglamento es aplicable a todos los recursos TIC que se utilicen en el tratamiento de la información creada, recibida o utilizada en las actividades de la UDC. Estos recursos pueden ser:

1. Equipamiento adquirido con el presupuesto de la UDC o que la UDC facilite a sus trabajadores, alumnado y usuarios en general, tales como los dispositivos informáticos o de comunicaciones.
2. Dispositivos personales del/de la usuario/a que se conecten a las redes de la UDC o que utilicen los recursos TIC de ésta.
3. Servicios TIC prestados por la UDC, bien directamente, bien a través de un proveedor.
4. Software adquirido por la UDC y puesto a disposición de las personas usuarias.
5. Aplicaciones informáticas que la UDC pone a disposición de sus usuarios/as, ya sean desarrolladas interna o externamente, ya sean adquiridas.
6. Sistemas informáticos y de comunicaciones que posibilitan la prestación de los servicios y el funcionamiento de las aplicaciones.

7. Infraestructuras físicas que sirven de soporte a estos cometidos, tales como las redes cableadas y los locales donde se alojan los sistemas TIC.
8. A la documentación en papel que los sistemas de información pudieran generar, en aquellos artículos que afecten a este tipo de soportes.

Artículo 3. Ámbito subjetivo de aplicación

Este reglamento es aplicable a todas las personas que hagan uso de los recursos TIC indicados en el artículo 2.

Artículo 4. Derechos de las personas usuarias

1. Todas las personas usuarias de los recursos TIC de la UDC tienen derecho, sin perjuicio de lo indicado en la legislación y en la normativa de la UDC en materia de protección de datos personales, a:
    a) Disponer de los recursos TIC necesarios para el desarrollo seguro de sus tareas o funciones, en las mejores condiciones técnicas que fuere posible.
    b) Recibir la información o la formación indispensables para el empleo adecuado de los recursos TIC según sus funciones o necesidades.
    c) Recibir información y soporte técnico sobre los incidentes que afecten a los recursos TIC.
    d) Ver respetados sus derechos fundamentales, especialmente la dignidad de las personas, el derecho al honor, a la intimidad y a la propia imagen y al secreto de las comunicaciones.
    e) A la intimidad frente al uso de dispositivos de videovigilancia y geolocalización.
    f) Expresar su opinión acerca de los servicios TIC corporativos que reciba y presentar quejas y sugerencias.
2. Además de lo indicado en el apartado anterior, el personal de la UDC tiene derecho a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

Artículo 5. Deberes de las personas usuarias

1. Todas las personas usuarias de los recursos TIC tienen los siguientes deberes:
    a) Utilizar de manera leal y responsable los recursos TIC que la UDC ponga a su disposición y, en todo caso, según lo indicado en este reglamento y las normas particulares de desarrollo.
    b) Conocer y cumplir la normativa interna que se pudiera derivar de este reglamento, tales como procedimientos, guías o recomendaciones.
    c) Seguir los procedimientos que la UDC establezca para realizar solicitudes de servicios TIC o comunicar incidentes.
    d) Conocer las consecuencias que pudieran derivarse del incumplimiento de este reglamento.
    e) Respetar las medidas de seguridad, informando de cualquier incidente que pudieran conocer.
    f) Aquellas aplicables al tratamiento de la información mediante lo uso de las TIC, de las indicadas en la Normativa general relativa a la protección de datos personales en la UDC.

2. El personal de la UDC tiene, además, los siguientes deberes:
    a) Guardar secreto sobre los datos personales a los que pudiera tener acceso por su actividad profesional. Este deber se mantendrá incluso en caso de que se extinga su relación con la UDC.
    b) Proteger la información y los recursos que tengan que utilizarse fuera de las instalaciones de la UDC.
    c) Utilizar los recursos TIC que la UDC les proporcione para fines profesionales. No obstante, la UDC admite que el/la trabajador/a pueda hacer un uso puntual de los recursos para fines particulares, con las limitaciones indicadas a lo largo de este reglamento, con las que la UDC pueda aplicar para garantizar el funcionamiento de sus servicios y salvaguardar su información y con las advertencias necesarias respecto a las expectativas de privacidad derivadas del contenido del artículo 10 de este reglamento.
    d) En el caso de causar baja en la universidad deberá eliminar toda la información de la UDC que pudiera tener almacenada en medios personales y devolver los dispositivos que ésta pudiera haber puesto a su disposición.

Artículo 6. Condiciones generales de uso de los recursos TIC de la UDC

Los recursos TIC de la UDC se utilizarán conforme a las siguientes condiciones generales, que podrán ser desarrolladas por normas detalladas, en caso de requerirse.

1. El acceso a la información no pública de la UDC y a sus recursos TIC requerirá de un control de acceso lógico que constará de un proceso de autenticación, es decir, de la identificación inequívoca del usuario, y otro de autorización, en el que se asigne al usuario/a el nivel de acceso que le corresponda.
2. El nivel de acceso estará basado en roles o perfiles que se asignarán a cada usuario/a en función de los colectivos a los que pertenezca y de las tareas que tenga encomendadas.
3. El acceso a los locales donde estén situados los sistemas informáticos y de comunicaciones corporativos requerirá de un control de acceso físico y de las medidas de seguridad necesarias para garantizar la prestación de los servicios según los objetivos de la organización.
4. La red de comunicaciones de la UDC se gestionará con la finalidad de garantizar la máxima disponibilidad, calidad y seguridad del servicio. Se aplicarán técnicas de segmentado, filtrado de puertos y de inspección automatizada del tráfico, entre otras medidas de seguridad.
5. Se aplicarán configuraciones seguras en los puestos informáticos de trabajo del personal de la UDC, así como en los equipos de las aulas de informática y aulas de libre acceso. Esto incluye la instalación de actualizaciones del software, el bloqueo del puesto informático por inactividad, el control de acceso basado en credenciales corporativas y la aplicación de medidas contra software malicioso.
6. El desarrollo, la puesta en servicio y el mantenimiento de aplicaciones corporativas, así como la gestión de los sistemas informáticos que les den soporte se realizará respetando lo que se indique en el desarrollo normativo de este reglamento, donde se abordará la gestión del cambio, la gestión de la capacidad, la continuidad de los servicios, la seguridad desde el diseño, la seguridad por defecto, las pruebas previas a la puesta en producción y el cumplimiento de los requisitos legales en materia de seguridad, entre otros aspectos.
7. El almacenamiento de información de la UDC se realizará únicamente en:

a) Sistemas informáticos corporativos, como servidores, cabinas de almacenamiento o volúmenes en red.
b) Sistemas de almacenamiento de información en la nube, siempre y cuando el proveedor de este servicio haya firmado un contrato que incluya las cláusulas necesarias para cumplir la legislación vigente en materia de protección de datos personales y de seguridad de la información en el ámbito de las administraciones públicas. La relación de proveedores de servicios en la nube con los que se haya firmado un contrato de este tipo se dará a conocer en el portal de ayuda de los servicios telemáticos de la UDC.
c) En el ámbito del personal docente e investigador (PDI) se podrá almacenar información en dispositivos locales siempre que el usuario se responsabilice de la realización de las copias de seguridad y del cifrado de la información, si procediera.
d) Otros dispositivos autorizados por la normativa de desarrollo de este reglamento.

8. Todos los dispositivos de computación (teléfonos inteligentes, tabletas, ordenadores portátiles, etc.) que contengan información de la UDC y que salgan de sus instalaciones deberán contar con un mecanismo de control de acceso dirigido a minimizar el riesgo de acceso no autorizado a la información que contengan o a la que puedan dar acceso. En el caso de uso de contraseñas, estos deberán cumplir los requisitos que se establecerán en una norma sobre el control de acceso lógico.
9. Cuando se utilicen soportes o dispositivos informáticos fuera de las instalaciones de la universidad, y contengan información de la UDC, deberán contar con las medidas de seguridad destinadas a protegerla en caso de robo o acceso no autorizado. Estas medidas serán proporcionales al nivel de seguridad que requiera la información y se detallarán en una norma al respeto.
10. En ningún caso se almacenarán datos personales sensibles en dispositivos que vayan a abandonar las instalaciones de la UDC sin utilizar técnicas de cifrado. Tendrán la consideración de datos personales sensibles, o datos de categoría especial, los que recoge el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, del 27/04/2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).
11. El uso por parte del personal de la UDC de dispositivos de computación particulares, como tabletas, teléfonos inteligentes u ordenadores portátiles, para el tratamiento de la información de la UDC, estará condicionado a la aceptación y adopción de las medidas de seguridad dirigidas a proteger la información de la organización.
12. El envío de datos personales fuera del ámbito de la UDC deberá realizarse con la autorización de la persona responsable del tratamiento.
13. En el caso de datos personales sensibles, las comunicaciones o envíos deberán realizarse utilizando técnicas de cifrado.
14. Todas las solicitudes de servicios TIC y comunicaciones de incidentes deberán realizarse a través del portal de ayuda de los servicios telemáticos de la UDC.
15. Los convenios, acuerdos o contratos que impliquen el acceso de personal no perteneciente a la comunidad universitaria a recursos TIC de la UDC deberán incluir los deberes concretos en el uso de estos recursos. Estos deberes se derivarán del contenido de este reglamento y sus normas de desarrollo.

Artículo 7. Actividades prohibidas

Están prohibidas las siguientes actividades:

1. Utilizar los recursos TIC para la realización de actividades comerciales o con ánimo de lucro ajenas a la UDC.
2. Dañar o producir cualquier deterioro en los recursos TIC de la UDC.
3. Cualquier transmisión, distribución o almacenamiento de contenidos difamatorios, amenazadores o que constituyan un atentado contra la dignidad de las personas.
4. Utilizar aplicaciones o contenidos que vulneren la legislación vigente en materia de propiedad intelectual.
5. Acceder a recursos sin la autorización correspondiente, en el caso de requerirse.
6. Acceder a los recursos con una identificación distinta de la propia.
7. Ceder las credenciales propias a otro usuario.
8. La utilización de mecanismos diseñados para eludir las medidas de seguridad implantadas o la explotación de posibles vulnerabilidades de los sistemas.
9. El uso de los recursos TIC de la UDC para cualquier actividad contraria al ordenamiento jurídico.

Artículo 8. Tratamiento de datos personales

1. Cuando las TIC se utilicen en el tratamiento de datos personales, además de lo indicado en este reglamento, deberá tenerse en cuenta lo especificado en la Normativa general relativa a la protección de datos en la UDC.

Artículo 9. La gestión de los servicios TIC en la UDC

1. Los centros, departamentos, institutos y otros órganos de la UDC gestionarán sus recursos TIC particulares según lo indicado en este reglamento.
2. La gestión de los recursos TIC corporativos le corresponde al Servicio de Informática y Comunicaciones (SIC). Entre otras, las siguientes serán funciones específicas del SIC:
    a) El diseño, desarrollo, operación y mantenimiento de las aplicaciones informáticas demandadas por los diferentes servicios de la universidad, conforme a los requerimientos funcionales especificados por estos.
    b) El diseño, desarrollo, operación y mantenimiento de los sistemas informáticos necesarios para el correcto funcionamiento de las aplicaciones.
    c) La gestión de los servicios de correo electrónico, mensajería, colaboración, etc., bien sean proporcionados por infraestructura propia, bien sean contratados a un proveedor de servicios.
    d) La administración de los puestos informáticos de trabajo del personal de la UDC y de los equipos informáticos puestos a disposición del alumnado o, eventualmente, de personal no perteneciente a la comunidad universitaria.
    e) La gestión de los servicios de impresión y escaneado de documentos.
    f) La gestión del sistema de nombres de dominio (DNS), de los dominios corporativos *udc.es* y *udc.gal* y la asignación de nombres en estos dominios.
    g) El mantenimiento de los sistemas que dan soporte al sitio web institucional.
    h) El diseño, desarrollo, operación y mantenimiento de los sistemas de control de acceso seguro a los servicios TIC.
    i) El diseño, desarrollo, operación y mantenimiento de la red de comunicaciones de la universidad, lo que incluye la gestión del cableado de los edificios, la

electrónica de red, la gestión y asignación de las direcciones de red, la interconexión con otras redes, la coordinación y la administración del espectro radioeléctrico dentro de los espacios físicos de la UDC.

j) La gestión técnica de los servicios de telefonía fija y móvil corporativos.
k) La autorización de la dotación de nuevas infraestructuras de cableado estructurado.
l) La implantación de las medidas de seguridad asociadas a las infraestructuras, servicios y aplicaciones anteriormente citadas.
m) La gestión de los locales destinados a alojar los sistemas informáticos y de comunicaciones, incluyendo las medidas de seguridad física que les afecten, en coordinación con el Servicio de Arquitectura, Urbanismo y Equipamientos.

Artículo 10. Supervisión del cumplimiento de este reglamento

1. La UDC, por motivos legales, de seguridad y calidad del servicio, cumpliendo en todo momento los requisitos que establece la legislación vigente, realizará una supervisión del uso correcto de sus recursos TIC.
2. Con dichos fines realizará un registro de las actividades de los usuarios en el uso de los recursos TIC de la UDC, que consistirá en la retención (almacenamiento y custodia) de información para la monitorización, análisis, investigación y documentación en relación con actividades indebidas o no autorizadas.
3. La UDC podrá realizar también, con carácter común, un seguimiento del uso de la red por parte de las personas usuarias cuya actividad quedará registrada. Igualmente, con carácter extraordinario, durante los procesos de investigación de un incidente y con el fin de asegurar los indicios recogidos de otras fuentes, se podrá realizar el análisis del tráfico de red, hasta el nivel de paquete.
4. La UDC realizará estas actividades de supervisión de manera proporcional al riesgo, con las cautelas legales pertinentes, las señaladas en la jurisprudencia y con observancia de los derechos de las personas usuarias.
5. En este campo realizará, entre otros, la supervisión del uso de los servicios de acceso a internet, correo electrónico y otros servicios de colaboración o comunicación.
6. Con el objeto de minimizar los incidentes de seguridad la UDC analizará, si fuera necesario, el tráfico de las aplicaciones o servicios externos potencialmente peligrosos, incluso si éste estuviera cifrado, y limitará estas actuaciones al mínimo necesario para tal fin.

Artículo 11. Medidas previstas en el caso de incumplimiento de este reglamento

1. El incumplimiento de este reglamento podrá comportar, de forma preventiva, la suspensión del servicio prestado o el bloqueo temporal del equipo del usuario o de su cuenta de acceso a la red, servicios o aplicaciones, sin perjuicio de las acciones legales, disciplinarias o de cualquiera otra índole que la UDC pudiera adoptar.
2. La suspensión o bloqueo se levantarán cuando remita la actividad que provocó el incumplimiento y cesen los efectos que hubiera provocado.
3. En el caso de un incumplimiento reiterado o que provoque daños de especial gravedad se actuará según el régimen disciplinario contenido en los Estatutos de la universidad.

Artículo 12. Revisión de este reglamento

1. Le corresponde al Comité de Seguridad de la Información:
   a) Interpretar las dudas que pudieran surgir en la aplicación de este reglamento.
   b) Verificar su efectividad.
   c) Promover su revisión para actualizar su contenido, especialmente en aquellos casos donde se identifiquen oportunidades de mejora o se produzcan cambios relevantes en el marco legal, tecnológico u organizativo.
   d) Proponer al Consejo de Gobierno las revisiones de este reglamento.

Disposición final primera

Las normas de desarrollo y aplicación de este reglamento serán adoptadas por el rector de la UDC.

Disposición final segunda

El presente reglamento entrará en vigor al día siguiente de su publicación en el Tablero Electrónico Oficial de la Universidad de A Coruña.

Todos los sistemas de información que se implanten a partir de esta fecha deberán respetar lo indicado en este reglamento.

Los sistemas existentes deberán adaptarse en el plazo máximo de un año.