UNIVERSIDADE DA CORUÑA

RESOLUCIÓN RECTORAL POR LA QUE SE APRUEBA LA NORMA SOBRE EL CONTROL DE ACCESO LÓGICO A LOS RECURSOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN (TIC) CORPORATIVOS

Esta norma regula el control de acceso lógico a los recursos TIC corporativos en desarrollo de lo indicado en el Reglamento general de uso de las TIC en la Universidad de A Coruña.

Para aquellas cuestiones que no se explicitan en este documento, como el ámbito de aplicación, la supervisión y las medidas previstas en el caso de incumplimiento, se estará a lo indicado en dicho reglamento.

El control de acceso lógico comprende los mecanismos que permiten la autenticación del/la usuario/a y la autorización del acceso a los recursos TIC con el nivel de privilegios idóneo, lo que permite la trazabilidad en el uso de los recursos e impide accesos no autorizados.

1. El control de acceso lógico a los recursos TIC corporativos

1.1 Autenticación

1. Los mecanismos de autenticación para el acceso a las aplicaciones o sistemas de información corporativos serán los que figuran en el Reglamento de uso de medios electrónicos y firma electrónica en la Universidad de A Coruña, aprobado por el Consejo de Gobierno de 26/01/2017, y en el Reglamento de creación y ordenación de la sede electrónica de la Universidad de A Coruña, aprobado por acuerdo del Consejo de Gobierno de 27/06/2012, modificado por el acuerdo del Consejo de Gobierno de 28/11/2014.
2. En el acceso al puesto informático de trabajo se admitirá también el uso de credenciales almacenadas en el dispositivo, salvo en los equipos del personal de administración y servicios (PAS), donde siempre se utilizarán credenciales corporativas.
3. Los mecanismos de control de acceso admitidos para teléfonos inteligentes y tabletas corporativos son la identificación facial, la impresión digital, la contraseña o PIN.
4. Toda transmisión de información secreta de autenticación se realizará aplicando mecanismos de cifrado.
5. Es responsabilidad del usuario la custodia diligente de los medios de autenticación puestos a su disposición.
6. El/la usuario/a debe comunicar al Servicio de Informática y Comunicaciones (SIC) cualquier incidencia relacionada con sus medios de autenticación, caso de la pérdida de la contraseña, su olvido, sospechas de uso por personas no autorizadas etc.

1.2 Autorización de acceso

7. La autorización de acceso a los recursos TIC corporativos, con los privilegios necesarios, estará basada 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. Se documentará dicha asignación.
8. Se documentarán los permisos de los distintos perfiles que se definan en cada sistema de información.
9. La jefatura del servicio o unidad administrativa deberá comunicar al SIC el alta de un nuevo usuario.

10. En caso de que un usuario requiera permisos distintos de los asignados mediante el mecanismo de roles, deberá realizar una solicitud que tendrá que ser aprobada por el/la responsable del servicio o unidad organizativa.
11. La jefatura del servicio o unidad organizativa comunicará al SIC la baja de los usuarios bajo su dependencia para la eliminación de los permisos de acceso que dejen de ser necesarios.
12. El usuario deberá comunicar cualquier exceso de privilegios de los que tenga constancia en el uso de las aplicaciones.

2. Registro de usuarios en el directorio corporativo

13. El SIC mantendrá un directorio corporativo cuyo objeto será la identificación, autenticación y autorización de los usuarios para acceder a los recursos TIC.
14. El registro de los datos del usuario en el directorio corporativo se realizará mediante los datos facilitados en el proceso de matrícula, en el caso del alumnado, o de la incorporación a la UDC, en el caso de su personal.
    a) El usuario completará este registro telemáticamente, eligiendo su identificador y su contraseña inicial mediante un código de un solo uso que se le entregará en el momento de la vinculación con la UDC. Este código deberá ser generado de manera totalmente aleatoria.
    b) En el caso de usuarios que no puedan completar esta información telemáticamente, la UDC empleará mecanismos que garanticen la entrega confidencial de las credenciales y requerirá, además, el cambio de la contraseña en el primero uso.
15. El registro de personas no pertenecientes a la comunidad universitaria en el directorio corporativo requerirá que el/la responsable del acuerdo, convenio o contrato, que los/las vincule con la institución, apruebe la solicitud. En este tipo de cuentas deberá consignarse la fecha tras la cual pasará al estado de suspensión o bloqueo, que no deberá ser nunca superior a la vigencia del acuerdo, convenio o contrato. En el momento en que una cuenta de este tipo deje de ser necesaria, la persona que aprobó la solicitud deberá comunicar su baja.
16. En los procesos de alta en el directorio, los usuarios deberán consignar una dirección de correo alternativo, distinta de la del dominio *udc.es/udc.gal*, así como un número de teléfono de contacto, a los efectos de recuperación de la contraseña de la cuenta de la UDC u otras situaciones que requieran de la comunicación por vías distintas del correo electrónico corporativo.
17. Cada cuenta del directorio corporativo deberá estar asignada a una única persona.
18. El almacenamiento de las contraseñas corporativas se realizará exclusivamente en los sistemas del directorio corporativo mediante mecanismos no reversibles.
19. Las cuentas en el directorio corporativo se bloquearán cuando no presenten actividad en un período de 12 meses, tras la notificación por correo electrónico a la persona interesada, quien podrá solicitar el desbloqueo de su cuenta en el momento en que lo necesite.
20. El bloqueo de una cuenta en el directorio no implica su eliminación. Estos datos se mantendrán el tiempo necesario para atender las necesidades de trazabilidad requeridas en la ley.

3. Contraseñas

21. Todas las contraseñas, incluidas aquellas que se asignen en los procedimientos de recuperación, deberán cumplir con los siguientes requisitos:
    a) Su longitud mínima será de 10 caracteres.
    b) Deberá contener caracteres de, al menos, tres de los siguientes tipos: números, mayúscula, minúsculas y caracteres no alfabéticos.
    c) No podrá incluir el identificador de usuario, su DNI, número de teléfono o cualquier otro dato que sea fácilmente relacionable con la persona usuaria.
    d) No deberá coincidir con las últimas 5 contraseñas.
22. Se establecerán los siguientes mecanismos de protección de las cuentas de usuario:
    e) La contraseña deberá renovarse, al menos, cada año.
    f) El tiempo mínimo entre cambios de contraseña será de 24 horas.
    g) Se bloquearán las cuentas de usuario que presenten 10 intentos de autenticación erróneos durante un período de 15 minutos. El tiempo de bloqueo será de 5 minutos.
    h) Se aplicará un bloqueo preventivo de aquellas cuentas de usuario que presenten indicios de haber sido sustraídas o que incurran en un uso indebido. Este bloqueo se levantará una vez resuelto el problema que lo provocó.
23. Los requisitos de este apartado no se aplican en el caso de cuentas de acceso a la red WiFi para personas invitadas a congresos o eventos.

4. Usos no permitidos

24. Los siguientes son usos no permitidos de los medios de autenticación:
    a) Acceder a los recursos TIC de la UDC suplantando la identidad de otro usuario o usuaria.
    b) Realizar intentos de autenticación con identificadores ajenos.
    c) Ceder las credenciales o cualquier otro medio de autenticación a otro/a usuario/a.
    d) Utilizar identificadores no personales para el acceso a recursos TIC de la UDC.
    e) Almacenar cualquier información secreta de autenticación en dispositivos que no cumplan el Reglamento de uso de las TIC en la UDC o su normativa de desarrollo.
    f) Usar la contraseña corporativa para servicios ajenos a la UDC.

5. Entrada en vigor

Esta norma entrará en vigor al día siguiente de su publicación en el Tablón Electrónico Oficial de la Universidad de A Coruña.