I. COMUNIDAD DE CASTILLA Y LEÓN

D. OTRAS DISPOSICIONES

CONSEJERÍA DE FOMENTO Y MEDIO AMBIENTE

ORDEN FYM/337/2022, de 8 de abril, por la que se aprueba la norma de condiciones de uso de los sistemas de información de la Administración de la Comunidad de Castilla y León.

El Decreto 7/2013, de 14 de febrero, de utilización de medios electrónicos en la Administración de la Comunidad de Castilla y León, establece en su artículo 3 que la política de seguridad de los sistemas de información corporativos, entendida como conjunto de directrices que rigen la forma en que esta Administración gestiona y protege la información y los servicios que considera críticos, se desarrollará aplicando los principios básicos y los requisitos mínimos recogidos en el 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.

Una de las medidas de seguridad del marco organizativo del Anexo II del Esquema Nacional de Seguridad obliga a que las administraciones públicas dispongan de una serie de documentos que describan el uso correcto de equipos, servicios e instalaciones, lo que se considera uso indebido y la responsabilidad del personal respecto al cumplimiento de estas normas.

El artículo 19 del Decreto 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León, regula los diferentes instrumentos de desarrollo de esta política, entre los cuales se encuentran las normas de seguridad de la información, que establecen las directrices y principios generales aplicables a diferentes aspectos de la seguridad. Estas normas, aprobadas por la persona titular de la consejería competente en materia de seguridad de la información y de obligado cumplimiento para todas las consejerías y organismos de la Administración de la Comunidad, son el instrumento adecuado para formalizar los contenidos de los documentos a que se refiere el Anexo II del Esquema Nacional de Seguridad.

El apartado 2 del indicado artículo 19 enumera los diferentes aspectos que deben desarrollar las normas de seguridad de la información y, entre ellos, la «seguridad ligada al personal», el «control de accesos y gestión de claves», la «seguridad operacional», la «seguridad de las comunicaciones» o la «gestión de incidentes de seguridad», señalando que cada uno de estos aspectos podrá ser desarrollado en una o varias normas de seguridad.

De acuerdo con lo exigido en el Esquema Nacional de Seguridad y con lo anteriormente expuesto, mediante la presente orden se aprueba la norma de condiciones de uso de los sistemas de información de la Administración de la Comunidad de Castilla y León.

Esta norma sustituye a la anterior política de uso establecida en la Orden FYM/643/2016, de 12 de julio, por la que se determina la política de uso de los servicios de comunicaciones e informática prestados en la Red Corporativa de la Administración de la Comunidad de Castilla y León.

En su virtud, previo informe favorable del Comité de Seguridad de la Información, vistas las disposiciones citadas y el artículo 26.1.f) de la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León,

RESUELVO:

Primero.– Aprobar la Norma de condiciones de uso de los sistemas de información de la Administración de la Comunidad de Castilla y León (NOR-1110), que se incluye como Anexo de esta orden.

Segundo.– Dejar sin efecto la Orden FYM/643/2016, de 12 de julio, por la que se determina la política de uso de los servicios de comunicaciones e informática prestados en la Red Corporativa de la Administración de la Comunidad de Castilla y León.

Tercero.– Esta orden producirá efectos desde el día de su publicación en el Boletín Oficial de Castilla y León.

Contra la presente orden, que pone fin a la vía administrativa, podrá interponerse, potestativamente, recurso de reposición ante el Consejero de Fomento y Medio Ambiente en el plazo de un mes, tal y como se establece en los artículos 123.1. y 124.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, o directamente, recurso contencioso administrativo ante la Sala de igual denominación del Tribunal Superior de Justicia de Castilla y León, en el plazo de dos meses, tal y como lo establecen los artículos 10.1 a) y 14.2 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa; ambos plazos a contar desde el día siguiente al de la publicación de la presente orden en el Boletín Oficial de Castilla y León.

Valladolid, 8 de abril de 2022.

El Consejero de Fomento
y Medio Ambiente,
Fdo.: Juan Carlos Suárez-Quiñones Fernández

ANEXO

NORMA DE CONDICIONES DE USO DE LOS SISTEMAS DE INFORMACIÓN DE LA ADMINISTRACIÓN DE LA COMUNIDAD DE CASTILLA Y LEÓN

(NOR-1110)

1.– Introducción.

Con la extensión del uso generalizado de las tecnologías de la información y las comunicaciones, en las Administraciones Públicas se ha puesto a disposición de los empleados públicos y de los proveedores externos una serie de sistemas de información cuyo empleo ha de hacerse de una forma ordenada y enfocada exclusivamente al desempeño de la actividad pública garantizando en todo momento su seguridad y eficiencia.

La presente norma constituye la norma de seguridad que describe las condiciones de uso de los sistemas de información de la Administración de la Comunidad de Castilla y León (ACCyL) de acuerdo con lo exigido en el Esquema Nacional de Seguridad. Esta norma, sustituye a la anterior política de uso establecida en la Orden FYM/643/2016, de 12 de julio, por la que se determina la política de uso de los servicios de comunicaciones e informática prestados en la Red Corporativa de la ACCyL.

2.– Objetivo y ámbito de aplicación.

El objetivo de la presente norma es establecer el uso correcto de los sistemas de información, servicios e instalaciones, lo que se considera uso indebido y la responsabilidad del personal respecto al cumplimiento de esta norma.

A los efectos previstos en esta norma, se entiende por usuarios a todo el personal que, de manera permanente o eventual, preste sus servicios en la ACCyL incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los sistemas de información de la ACCyL. Respecto a estos últimos usuarios, en los pliegos de contratos firmados con la ACCyL deberá contemplarse la obligación de aceptar de forma expresa lo previsto en la presente norma por parte del personal externo que, por sus funciones, requiera el uso de los sistemas de información corporativos.

Se entiende por sistemas de información aquellos cubiertos por el ámbito de aplicación del Decreto 22/2021, de 30 de septiembre, por el que se aprueba la Política de Seguridad de la Información y Protección de Datos.

No se considerarán usuarios ni estarán sujetos por tanto a las previsiones de esta norma quienes hagan uso de las conexiones que se ponen a disposición de los ciudadanos en algunos edificios oficiales y centros públicos.

3.– Gestión de la norma y responsabilidades.

El Servicio de Seguridad de la Información (SSI) será el responsable de todas las actividades de la gestión de la documentación de la presente norma y realizará las tareas de redacción, difusión, verificación de su efectividad y revisión. Asimismo, interpretará las dudas que puedan surgir con relación a su aplicación.

El Comité de Seguridad de la Información (CSI) en su reunión de 21 de marzo de 2022 ha informado favorablemente la norma, siendo aprobada por la presente orden del titular de la Consejería competente en materia de seguridad de la información (CONSEJERÍA SSI).

Los Responsables de Seguridad (RSEG) asegurarán la difusión de la norma/procedimiento en su Consejería.

Los usuarios de los Sistemas de Información de la ACCyL (USUARIOS) aplicarán la presente norma.

El órgano competente para la prestación de los servicios corporativos de informática y de comunicaciones (TIC) será consultado para su redacción y para su revisión.

En la siguiente matriz RACI1 se detalla la asignación de responsabilidades de las actividades que tienen relación con el desarrollo y aplicación de esta norma.

ACTIVIDAD	*CSI*	*SSI*	*CONSEJERÍA SSI*	*RSEG*	*TIC*	*USUARIOS*
Redacción		AR			C	
Validación	R	A				
Aprobación		A	R			
Difusión		AR		R		
Aplicación		A				R
Verificación		AR				
Revisión		AR			C	

4.– Vigencia y revisión.

La norma surtirá efectos inmediatamente después de su aprobación y publicación.

La revisión de esta norma se realizará de forma anual o con menor periodicidad si existen circunstancias que así lo aconsejen.

La revisión de la norma se orientará principalmente a la identificación de oportunidades de mejora en la seguridad del uso de los sistemas de información, sin olvidar la necesidad de adaptar la norma a los cambios habidos en el marco legal, a las mejoras tecnológicas y a los cambios en la organización.

1 Significado de los roles que se incluyen en la matriz de asignación de responsabilidades (matriz RACI):
Accountable (A): Autoriza el trabajo a realizar y lo aprueba una vez finalizado. Toma la decisión.
Responsible (R): Realiza el trabajo y es responsable por su realización. Ejecuta la tarea.
Consulted (C): Se le consulta antes de hacer el trabajo. Tiene información para realizar el trabajo. Comunicación bidireccional.
Informed (I): Se le informa de las decisiones tomadas. Comunicación unidireccional.

5.– Condiciones de uso.

5.1. *Principios generales.*

La ACCyL proporcionará a los usuarios los recursos informáticos y servicios de comunicaciones adecuados para la realización de las tareas que les son asignadas.

El uso de estos recursos tendrá una finalidad profesional, exclusivamente para el ejercicio de actividades y tareas que correspondan a las funciones encomendadas y durante el tiempo necesario. Se prohíben usos privados o personales ajenos a las actividades y tareas referidas.

Se prohíben actividades que pretenden comprometer, evitar o dificultar las actuaciones de protección de los sistemas de información de la ACCyL.

Se fomentará un uso eficiente y seguro de los sistemas de información del ámbito de aplicación, prohibiéndose todo tipo de actividades que comprometan su rendimiento y su seguridad. Sin perjuicio del cumplimiento de los deberes y aplicación de los principios éticos contenidos en los artículos 52 a 54 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, la actividad de los usuarios se ajustará a los principios de legalidad, eficacia, profesionalidad, eficiencia y diligencia en la utilización de los recursos informáticos y de comunicaciones.

El usuario devolverá todos los recursos informáticos y de comunicaciones, y se eliminarán todas las cuentas y accesos que tuvieran asignados cuando se modifiquen las circunstancias profesionales que originaron la asignación al mismo.

5.2. *Confidencialidad de la información.*

Los usuarios solo podrán acceder a aquella información para la que posean las autorizaciones correspondientes, en función de las labores que desempeñen.

La información a la que se tenga acceso en virtud de la actividad profesional deberá utilizarse únicamente para el cumplimiento de las funciones encomendadas, garantizando su privacidad y confidencialidad. Ésta deberá mantenerse aún después de finalizada su relación con la ACCyL.

Se evitará almacenar información sensible, confidencial o protegida en medios desatendidos o dejar accesible y visible tal información sin atención.

Se respetará la normativa vigente en materia de protección de datos personales. Todo usuario que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, estará obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso una vez finalizada su relación con la ACCyL.

5.3. *Incidentes de seguridad.*

Cuando un usuario detecte cualquier anomalía o incidente de seguridad que pueda comprometer el buen uso y funcionamiento de los sistemas de información de la ACCyL deberá informar inmediatamente por los cauces establecidos a su Centro de Atención a Usuarios o a los centros de servicios especializados que se habiliten.

Los incidentes de seguridad que afecten a datos de carácter personal serán comunicados, por el Responsable del Tratamiento, a la Agencia Española de Protección de Datos, siempre que dichos incidentes puedan causar daños o perjuicios a las personas. Si además estos daños son graves, la brecha o incidente de seguridad deberá ser comunicada asimismo al interesado.

5.4. *Utilización de los recursos informáticos y de comunicaciones.*

Es responsabilidad del usuario la custodia y cuidado de los recursos informáticos y de comunicaciones puestos a su disposición, debiendo facilitar su instalación, soporte, reparación y mantenimiento. Dichos recursos deberán utilizarse de forma eficiente y segura y a tal fin los usuarios deberán:

- Mantener el puesto de trabajo despejado, guardando la documentación de forma segura.
- Activar el salvapantallas si está disponible.
- Bloquear la sesión de usuario en el dispositivo o, en su caso, apagar el dispositivo ante ausencias prolongadas.
- Verificar la ausencia de virus en los ficheros en soportes extraíbles autorizados y en adjuntos a los correos electrónicos, utilizando el antivirus del equipo.
- Evitar almacenar en el disco local del puesto de trabajo información relevante. Preferentemente deberán utilizarse las unidades de red de trabajo compartido que permitan disponer de una copia de seguridad de la información almacenada.
- Para el intercambio de ficheros de trabajo, siempre que sea posible, se deberán utilizar las unidades de red adecuadas en cada caso, teniendo en cuenta quien puede tener acceso a la información. Con carácter general se utilizarán las impresoras en red y fotocopiadoras compartidas, asegurando la documentación enviada al dispositivo. La documentación deberá permanecer el menor tiempo posible en las bandejas de salida de impresoras, escáneres y fax, para evitar que terceras personas puedan acceder a la misma.

El uso de dispositivos particulares para el ejercicio de funciones públicas estará condicionado a la autorización previa por parte de la ACCyL.

El cese de actividad de cualquier usuario o cuando un cambio en sus funciones implique la restricción de algún privilegio asignado, deberá ser comunicado de forma inmediata por parte del jefe de la unidad correspondiente por los cauces establecidos a su Centro de Atención a Usuarios o a los centros de servicios especializados que se habiliten, al objeto de que le sean retirados los recursos informáticos y de comunicaciones que se le hubieren asignado. Correlativamente, cuando los recursos informáticos y de comunicaciones proporcionados estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente cuando finalice su vinculación con dicho puesto o función.

5.5. *Instalación y configuración de los recursos informáticos y de comunicaciones.*

Las unidades competentes definirán la configuración de los diferentes recursos informáticos y de comunicaciones, podrán autorizar la utilización de periféricos y la

instalación de software en los equipos informáticos que se conecten a las distintas redes internas y concederán permisos de administración de los recursos informáticos y de comunicaciones. Ningún usuario no autorizado por esas unidades podrá conectar equipos, sensores o dispositivos a los recursos informáticos y de comunicaciones, o alterar cualquiera de los componentes de dichos recursos.

Los usuarios no dispondrán de privilegios para la administración de equipos, salvo autorización de las referidas unidades.

Únicamente el personal autorizado podrá instalar o desinstalar software y hardware. Asimismo, está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los recursos informáticos y de comunicación.

Se prohíbe el uso de aplicaciones o herramientas para la descarga o el intercambio de archivos salvo los autorizados por la ACCyL.

5.6. *Dispositivos móviles.*

El usuario deberá adoptar las medidas de seguridad que sean necesarias para evitar la pérdida, el robo y el uso inadecuado de los dispositivos móviles (ordenadores portátiles, teléfonos móviles o similares) que le han sido proporcionados para el desarrollo de sus tareas profesionales, así como la información contenida en ellos.

En caso de extravío o robo del dispositivo móvil y en caso de detectar cualquier funcionamiento anómalo del dispositivo o incidente que pueda afectar a la seguridad de la información, deberá informar inmediatamente por los cauces establecidos a su Centro de Atención a Usuarios o a los centros de servicios especializados que se habiliten.

El usuario deberá devolver el dispositivo móvil cuando se modifiquen las circunstancias profesionales que originaron la asignación al mismo.

Únicamente el personal debidamente autorizado será el encargado del mantenimiento de los dispositivos móviles.

Se prohíbe la manipulación, sin la debida autorización, de las configuraciones de seguridad y del software instalado en los dispositivos móviles, así como la desactivación de los componentes de seguridad instalados en dichos equipos.

5.7. *Autenticación y acceso.*

Con carácter general, toda persona autorizada para acceder a un sistema de información dispondrá de una única cuenta, personal e intransferible, compuesta al menos por el identificador y la contraseña. Únicamente los usuarios con privilegios especiales podrán disponer de más de una cuenta, con perfiles distintos en función de las tareas a desarrollar.

Por razones de seguridad o cuando la naturaleza del sistema así lo requiera, podrán establecerse modos de acceso o autenticación distintos al señalado en el párrafo anterior que permitan la identificación del usuario.

Los usuarios deben custodiar convenientemente sus credenciales.

Se prohíbe el uso de credenciales ajenas, la cesión de las propias y la utilización de mecanismos o sistemas cuyo objeto sea ocultar o suplantar la identidad de los usuarios.

No podrán utilizarse las credenciales profesionales para registrarse en servicios y sitios de internet no relacionados con las funciones del puesto de trabajo.

5.8. *Acceso de terceras personas.*

El personal ajeno a la ACCyL que deba acceder a sus sistemas de información, deberá hacerlo previa autorización de la persona responsable del sistema de información que corresponda.

Tales personas, en lo que les sea de aplicación, deberán cumplir la presente norma de Condiciones de Uso, así como el resto de normativa y procedimientos de seguridad de la información de la ACCyL, así como la normativa vigente en materia de protección de datos.

5.9. *Acceso remoto.*

El acceso remoto a los sistemas de información de la ACCyL deberá ser previamente autorizado en función de sus necesidades. En el acceso remoto se deberán tener en cuenta las siguientes consideraciones:

- Se utilizarán solo conexiones a redes de confianza evitando especialmente las redes abiertas.
- Se vigilarán los equipos para evitar accesos no deseados o robos.
- Se limitará el uso del acceso remoto al mínimo tiempo imprescindible. En caso de ausentarse de su puesto deberá bloquear el equipo o finalizar el acceso remoto.
- Se mantendrá el equipo actualizado.

5.10. *Salidas de información.*

Está prohibido el envío al exterior de información que no esté categorizada como pública por cualquier soporte y medio de comunicación que no hubiere sido previamente autorizada por el Responsable de la Información.

Cuando el nivel de seguridad de la información lo requiera, la salida de información deberá ser cifrada o protegida con cualquier medida de seguridad que garantice que la información no sea inteligible durante su remisión o transporte para asegurar la confidencialidad de la información, incluyendo tanto los soportes físicos como cualquier otro medio de transmisión a través de redes no confiables (correo electrónico).

Con carácter general, el uso de soportes extraíbles de información como memorias USB, CD/DVD o cualquier otro dispositivo externo de almacenamiento no está autorizado. En el caso de que el usuario disponga de autorización, éste será responsable de salvaguardar la información extraída a través de tales dispositivos. La pérdida o sustracción de una memoria USB, CD/DVD o cualquier otro dispositivo externo con información no pública deberá notificarse como incidente de seguridad. Los soportes de información que vayan a ser reutilizados o causen baja deberán ser previamente tratados para eliminar permanentemente la información que pudieran contener, de manera que resulte imposible su recuperación.

No se considera salida de información el uso de servicios de almacenamiento en la nube que estén autorizados por la ACCyL y cuya configuración de seguridad esté gestionada por las unidades competentes para la prestación de los servicios corporativos de informática y de comunicaciones. El uso de otros servicios de almacenamiento en la nube distintos al anterior se considerará salida de información y deberá cumplir lo establecido en el presente apartado.

5.11. *Acceso a Internet y herramientas de colaboración.*

Con carácter general, el acceso a Internet por los usuarios se realizará, previa autorización, únicamente empleando los medios y a través de las comunicaciones puestas a su disposición por la ACCyL. A tal efecto se podrá asignar un perfil de acceso en función de sus necesidades que determinará a qué tipo de contenidos podrá acceder. La ACCyL podrá restringir el acceso a determinadas páginas web que por su contenido se consideren innecesarias para la organización o inseguras.

La utilización de cualquier dispositivo de comunicaciones (teléfonos móviles, USB de comunicaciones y similares) para acceso alternativo a Internet, solo podrá realizarse previa asignación y autorización de esos medios.

Solo se podrá acceder a Internet mediante los navegadores autorizados y configurados por la ACCyL en los puestos de usuario. No podrá alterarse su configuración ni utilizar navegadores alternativos sin la debida autorización.

No deberá accederse en ningún caso a direcciones de Internet que tengan un contenido ilegal, ofensivo o atentatorio de la dignidad humana o que comprometan el rendimiento y seguridad de los recursos informáticos y de comunicaciones. El hecho de que la ACCyL no haya bloqueado el acceso a una determinada página web no implica que el acceso a la misma esté permitido.

Se prohíbe la descarga o compartición de contenidos que vulneren la legislación, entre otras, la relativa a la Propiedad Intelectual y a las materias clasificadas.

5.12. *Uso del correo corporativo.*

Las unidades competentes para la prestación de los servicios corporativos de informática y de comunicaciones suministrarán a cada usuario una dirección individual de correo electrónico asociada a su cuenta de usuario. Cada usuario será responsable de las actividades realizadas a través de las cuentas de correo electrónico de las que es titular.

Únicamente podrán utilizarse clientes de correo electrónico autorizados por la ACCyL.

A los efectos de evitar que los servidores queden colapsados por su uso inadecuado o que puedan resultar dañados, los usuarios deberán abstenerse de enviar mensajes masivos o con ficheros adjuntos de gran tamaño.

No está autorizado el envío de correos que contengan información con datos sensibles o confidenciales sin proteger. En el caso de que sea necesario el envío de esta información y el usuario no tenga los conocimientos necesarios, el usuario deberá ponerse en contacto con su Centro de Atención a Usuarios o a los centros de servicios

especializados que se habiliten, que le proporcionará el apoyo y los mecanismos necesarios para el envío de este tipo de información.

Se prohíbe a los usuarios el reenvío automático del correo corporativo a cuentas externas, así como interceptar, leer, borrar, enviar, copiar o modificar el contenido de los mensajes de correo electrónico de otros usuarios.

Se prohíbe el uso abusivo del correo electrónico, propagación de cadenas de correos, envío de correos ofensivos y el intercambio no autorizado de contenidos protegidos por la legislación de propiedad intelectual. Asimismo, se prohíbe el envío de cualquier clase de código malicioso o dañino que puedan causar perjuicios en los sistemas de información.

5.13. *Monitorización.*

Por razones de seguridad y operatividad de las actividades realizadas con los sistemas de información de la ACCyL y con el objetivo de velar por la correcta utilización de los mismos conforme a lo contenido en esta norma, las unidades competentes para la prestación de los servicios corporativos de informática y de comunicaciones podrán utilizar herramientas de monitorización, registro y análisis de uso que permitan detectar indicios o incidencias que puedan suponer problemas en el buen funcionamiento de los servicios o poner en riesgo la seguridad y la protección de la información, y para la determinación de medidas preventivas, correctivas o paliativas; o herramientas de visualización y análisis del detalle del uso de los servicios corporativos de comunicaciones.

Tal y como se detalla en el Artículo 23 sobre los registros de actividad 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, estas actividades de monitorización, registro y análisis de las actividades de los usuarios, deberán ser proporcionales al riesgo al que se exponen los sistemas de información, manteniendo 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, permitiendo identificar en cada momento a la persona que actúa.

5.14. *Formación y concienciación.*

Los usuarios deberán asistir a los cursos de formación en materia de seguridad que la ACCyL considere necesarios, en función de los recursos informáticos y de comunicaciones puestos a su disposición, así como de los sistemas de información de la ACCyL a los que se le autorice el acceso.

5.15. *Responsabilidades.*

La responsabilidad por el incumplimiento de lo previsto en esta norma, así como por cualquier actuación irregular, ilícita o ilegal que fuese detectada por la ACCyL en el uso de sus de sistemas de información será exigida de acuerdo con lo previsto en el régimen disciplinario de los empleados públicos, así como, en su caso, de conformidad con lo previsto en esta materia en el ordenamiento civil y penal.

5.16. *Medidas cautelares extraordinarias.*

En aquellos casos en los que el incumplimiento de esta norma entrañe un riesgo manifiesto y grave para la seguridad y eficiencia de sistemas de información de la ACCyL,

así como para la confidencialidad, integridad y disponibilidad de la información, se podrán adoptar las medidas que fueren adecuadas a fin de garantizar su buen funcionamiento, incluida, si ello fuere necesario, la suspensión inmediata del servicio prestado, el bloqueo temporal de las cuentas de usuario y el acceso a los sistemas o redes a los que tenga acceso, con comunicación al propio usuario, así como a su superior inmediato en el espacio de tiempo más breve que sea posible.

5.17. *Procedimientos operativos de seguridad.*

El órgano competente para la prestación de los servicios corporativos de informática y de comunicaciones podrá desarrollar esta norma de Condiciones de Uso mediante la elaboración de Procedimientos Operativos de Seguridad específicos en función de la materia.

6.– Anexos.

6.1. *Legislación.*

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (modificado por el Real Decreto 951/2015, de 23 de octubre).
- Decreto 22/2021, de 30 de septiembre, por el que se aprueba la política de seguridad de la información y protección de datos de la Administración de la Comunidad de Castilla y León.

6.2. *Medidas del Esquema Nacional de Seguridad.*

La presente norma cumple con la medida de seguridad [org.2] del Esquema Nacional de Seguridad.

CV: BOCYL-D-20042022-21