3. Otras disposiciones

CONSEJERÍA DE LA PRESIDENCIA, INTERIOR, DIÁLOGO SOCIAL Y SIMPLIFICACIÓN ADMINISTRATIVA

Resolución de 25 de marzo de 2024, de la Agencia Digital de Andalucía, por la que se determina la gestión del repositorio de identidades de la Junta de Andalucía.

La Ley 3/2020, de 28 de diciembre, del Presupuesto de la Comunidad Autónoma de Andalucía para el año 2021, mediante su disposición adicional vigesimosegunda, creó la Agencia Digital de Andalucía. La Agencia tiene personalidad jurídica pública diferenciada, plena capacidad jurídica y de obrar, patrimonio y tesorería propios, sin perjuicio del principio de unidad de caja, así como autonomía de gestión para el cumplimiento de sus fines.

De acuerdo con el apartado 1 de la citada disposición, la Agencia tiene como fines:

a) La definición y ejecución de los instrumentos de tecnologías de la información, telecomunicaciones, ciberseguridad y gobierno abierto y su estrategia digital, en el ámbito de la Administración de la Junta de Andalucía, sus agencias administrativas y sus agencias de régimen especial.

b) La definición y coordinación de las políticas estratégicas de aplicación y de seguridad de las tecnologías de la información y de las comunicaciones en el ámbito del sector público andaluz no incluido en el párrafo anterior, incluyéndose los consorcios referidos en el artículo 12.3 de la Ley 9/2007, de 22 de octubre, así como la ejecución de los instrumentos comunes que las desarrollen y la definición y contratación de bienes y servicios de carácter general aplicables.

Tras la publicación en el Boletín Oficial de la Junta de Andalucía del Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía, la Agencia ha iniciado su funcionamiento efectivo.

El apartado 3 del artículo 6 del Decreto 128/2021 establece, entre otras, las siguientes funciones y competencias de la Agencia:

a) El diseño, desarrollo, implantación, mantenimiento, gestión y evolución de la infraestructura tecnológica en materia de informática y telecomunicaciones, así como la ejecución de las actuaciones para su consolidación y racionalización, incluyéndose en particular el puesto de trabajo, las infraestructuras de almacenamiento y el archivo electrónico único de los expedientes y documentos electrónicos.

d) La definición, diseño, implantación tecnológica, mantenimiento y evolución del puesto tecnológico de trabajo del personal y su equipamiento lógico y físico, los espacios tecnológicos de trabajo y las modalidades de movilidad y teletrabajo.

j) El soporte y atención directa al personal empleado sobre los elementos tecnológicos puestos a su disposición para el desempeño de sus funciones, en especial el puesto de trabajo.

n) La dirección estratégica, planificación, impulso, desarrollo y ejecución de la política de telecomunicaciones de la Administración de la Junta de Andalucía y del sector público andaluz, así como la gestión y evolución de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía.

ñ) El desarrollo y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía y del sector público andaluz.

o) La gestión de los recursos comunes para la prevención, detección y respuesta a incidentes y amenazas de ciberseguridad en el ámbito de la Administración de la Junta de Andalucía y del sector público andaluz.

00299737

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad indica, en su artículo 17, en relación con la «Autorización y control de los accesos»:

«El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este Real Decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.»

Dentro del marco operacional, constituido por un conjunto de medidas relacionadas con la organización global de la seguridad, destacan las siguientes:

«- [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

- [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las Administraciones Públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.

- [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las Administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- [op.acc.1.5] En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) núm. 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación.

- [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.»

Por su parte, la Exposición de Motivos de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, la Junta de Andalucía expresa su firme voluntad de apostar por la adopción de las nuevas tecnologías en orden a simplificar la gestión administrativa. Para ello, la figura de los empleados públicos de la Junta de Andalucía debe delimitarse, resultando necesario una gestión unificada de su identidad, conforme a las necesidades vigentes.

La mencionada Ley 9/2007 recoge, asimismo, en el apartado 4 del artículo 7, que «La transmisión y recepción de información en red o de documentos electrónicos entre la Administración de la Junta de Andalucía y la ciudadanía, entre los órganos o entidades de la Junta de Andalucía entre sí, o entre estos y otras Administraciones Públicas podrá realizarse a través de los medios y soportes electrónicos o telemáticos siempre que se garantice el cumplimiento de […]» varios requisitos, siendo especialmente relevante el indicado en la letra c): «la existencia de medidas de seguridad que eviten la interceptación y alteración de las comunicaciones, así como los accesos no autorizados».

Por otra parte, el artículo 20 de la Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para

00299737

profesionales públicos de la Administración de la Junta de Andalucía, viene a incidir en aspectos del ciclo de vida de la identidad digital del empleado público:

[…] «Cuando un profesional deje de desempeñar las funciones que venía realizando o en caso de baja temporal que suponga una interrupción prolongada del desempeño de las mismas, para garantizar la continuidad del servicio, comunicará a la persona responsable de su unidad administrativa u órgano al menos la siguiente información:

a) Relación de aplicaciones y sistemas que viniera utilizando, en especial aquéllas de otras Administraciones Públicas.

b) Relación de espacios de trabajo colaborativo en los que participa y los que administra.

c) Relación de cuentas no personales que atendiera, en especial de correo electrónico y de redes sociales, y, en su caso, la contraseña cuando la hubiera creado él o fuera su único depositario.

d) Relación de certificados electrónicos de representante de órganos de la Administración que tuviera otorgados.

e) Relación de recursos utilizados, en especial ficheros de herramientas ofimáticas, cuyo acceso o modificación esté protegido por contraseña cuando la hubiera creado él o fuera su único depositario, así como en cada caso, dicha contraseña».

Una gestión de identidades adecuada posibilita que las personas usuarias autorizadas tengan acceso únicamente a los recursos tecnológicos que necesitan para realizar su trabajo. Para lograr este objetivo hace falta disponer de un repositorio de identidad fiable.

Los servicios de autenticación del empleado público andaluz se prestan en la actualidad sobre el sistema de directorio de correo corporativo, sistema que ha ido albergando los diferentes usuarios provenientes del sector público, bajo demanda de las diferentes entidades que lo componen. Dado que la identidad digital de los usuarios ha de adaptarse a los requisitos de seguridad expuestos en el ENS, habrá que llevar a cabo actuaciones orientadas a satisfacer el cumplimiento del ENS y por tanto de las necesidades de seguridad de la Junta de Andalucía.

Además, para hacer evolucionar el paradigma de acceso de los empleados públicos a los recursos tecnológicos se hace necesaria asimismo la evolución de la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía (en adelante, RCJA). Será preciso contar con mecanismos de seguridad perimetral en nube, monitorizar el acceso a recursos y, no menos importante, verificar la identidad del empleado público en el acceso a los servicios de la Junta de Andalucía, además de garantizar un inventario de las sedes donde se preste algún tipo de servicio por la RCJA.

Estos aspectos requieren de una adaptación de los sistemas que permita acceder a datos centralizados únicos y exactos que ayuden a garantizar la identidad del usuario y el medio desde el que se accede al servicio.

La presente resolución regula la organización, funcionamiento y régimen operacional del repositorio de identidades de empleado público (también conocido como Directorio de Correo Corporativo) para todas aquellas entidades incluidas en el ámbito de aplicación de esta resolución.

En virtud de lo anterior y de acuerdo con lo previsto en el artículo 6.3.a) de los Estatutos de la Agencia Digital de Andalucía aprobados mediante el Decreto 128/2021, de 30 de marzo, esta Dirección Gerencia

R E S U E L V E

Primero. Objeto.

Establecer las directrices y condiciones de utilización, organización, aprovisionamiento y funcionamiento del repositorio de identidades (también conocido como Directorio de Correo Corporativo) y las réplicas que se hagan del mismo, en los términos que se detallan en el Anexo I de esta resolución.

00299737

Segundo. Responsable del directorio de correo corporativo y facultades.

1. Definir la figura del responsable de directorio de correo corporativo, en adelante RDCC, que recaerá en la persona que ostente la jefatura del Servicio de Transformación y Evolución a Modelo en Nube e Inventario.

2. Las facultades del RDCC son las siguientes:

a) Llevar a cabo cualquier actualización sobre los usuarios existentes: altas, bajas o modificaciones.

b) Establecer las ramas de pertenencia de los usuarios.

c) Autorizar a los organismos la utilización de una réplica propia, total o parcial, del Directorio de Correo.

d) Definir las características de los identificadores de usuarios.

e) Eliminar aquellos usuarios que incumplan la normativa vigente.

f) Permitir espacios de nombres alternativos.

g) Establecer los criterios y procedimientos necesarios para el cumplimiento del ENS.

h) Suspender temporalmente la creación de nuevos usuarios LDAP en un organismo.

i) La creación, mantenimiento y borrado de ramas.

j) Establecer las tareas de control y auditoría que se estimen oportunas.

Tercero. Ámbito de aplicación.

El ámbito de aplicación de la presente resolución es el establecido en el artículo 6, apartado 2, letra a), del Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía, sobre la definición y ejecución de instrumentos de tecnologías de la información, esto es, la Administración de la Junta de Andalucía, sus agencias administrativas y sus agencias de régimen especial.

Asimismo, por constituir un elemento de definición y coordinación de las políticas estratégicas de aplicación y de seguridad de las tecnologías de la información, así como la ejecución de los instrumentos comunes que las desarrollen y la definición y contratación de bienes y servicios de carácter general aplicables, este ámbito se extiende al sector público andaluz no incluido en el párrafo anterior, incluyéndose los consorcios referidos en el artículo 12.3 de la Ley 9/2007, de 22 de octubre, al amparo del artículo 6, apartado 2, letra b), del decreto citado en el párrafo anterior.

Cuarto. Finalidad.

La presente resolución tiene como principal objetivo contar con un servicio de DCC optimizado, con un contenido acorde a la realidad de las entidades participantes en el mismo.

Los administradores de ramas LDAP dispondrán de un plazo de 6 meses, desde la entrada en vigor de la presente norma, para actualizar los usuarios LDAP de sus ramas. En particular:

- Sólo se permitirá la existencia de un usuario LDAP externo o interno asociado a un NIF, debiéndose eliminar los restantes.

- Deberán darse de baja los usuarios LDAP con buzón de correo para los que no haya constancia de acceso al mismo en los 12 meses anteriores a la entrada en vigor de la presente resolución.

- Deberán darse de baja los usuarios de aplicaciones para los que no haya constancia de que hayan cambiado la contraseña en los 15 meses anteriores a la entrada en vigor de la presente resolución.

Pasados los 6 meses, la presente resolución autoriza al RDCC a eliminar los usuarios LDAP que no cumplan con los requisitos establecidos, previo aviso a los administradores de rama de dicho borrado.

Quinto. Efectos.

La presente resolución se publicará en el Boletín Oficial de la Junta de Andalucía y surtirá efectos a partir de la fecha de su publicación.

00299737

Sexto. Recursos.

Contra la presente resolución, que agota la vía administrativa, cabe interponer recurso de reposición, con carácter potestativo, en el plazo de un mes a contar desde el día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía, de acuerdo con el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, o recurso contencioso-administrativo ante el Juzgado de lo Contencioso-Administrativo del municipio en que tenga su sede el órgano competente o ante el Juzgado en cuya circunscripción tuviera el demandante su domicilio, a elección de este último, en el plazo de dos meses desde el día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía, de acuerdo con lo previsto en el artículo 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

Sevilla, 25 de marzo de 2024.- El Director Gerente, Raúl Jiménez Jiménez.

ANEXO I

DIRECTRICES Y CONDICIONES

Uno. Definiciones.

Active Directory (o Directorio Activo): Implementación del protocolo LDAP realizada por la empresa Microsoft para su servicio de directorio.

Administrador de Rama: Cualquier usuario LDAP correspondiente a una persona (empleado público o personal externo) con permisos para realizar tareas de administración y gestión sobre los usuarios y recursos de la rama LDAP. Será en todo caso responsable de ratificar las acciones del mismo el responsable de Rama.

Atributos estandarizados: Aquellos atributos definidos que forman parte de un conjunto inalterable y comunes a los usuarios del Directorio de Correo Corporativo dependiendo de su tipología.

Directorio de Correo Corporativo (en adelante, DCC): Aplicación basada en la actualidad sobre OpenLDAP que, en sus orígenes, se utilizó como plataforma de autenticación para el Correo Corporativo de la Junta de Andalucía, pero que ha evolucionado a plataforma centralizada para servicios de autenticación y/o autorización de otras muchas aplicaciones prestadas por la Junta de Andalucía.

ENS: Esquema Nacional de Seguridad. El Esquema Nacional de Seguridad establece la política de seguridad, en el ámbito público, en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Entidad instrumental: Tienen la consideración de entidades instrumentales de la Administración de la Junta de Andalucía las entidades dotadas de personalidad jurídica propia, creadas, participadas mayoritariamente o controladas efectivamente por la Administración de la Junta de Andalucía o por sus entes públicos, con independencia de su naturaleza y régimen jurídico, que tengan por objeto la realización de actividades cuyas características por razones de eficacia justifiquen su organización y desarrollo en régimen de autonomía de gestión y de mayor proximidad a la ciudadanía, en los términos previstos en la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

Identidad: En lo relativo a esta resolución, nos referimos a la identidad digital, como conjunto de información que nos identifica en un determinado entorno de internet.

Identificador LDAP: Conjunto de caracteres que identifica de forma unívoca a un usuario LDAP.

LDAP: Acrónimo de Lightweight Directory Access Protocol, protocolo ligero de acceso a directorio. Hace referencia a un protocolo a nivel de aplicación que permite el acceso a

00299737

un servicio de directorio (conjunto de objetos con atributos organizados en una manera lógica y jerárquica) ordenado y distribuido para buscar diversa información.

OpenLDAP: Tecnología en la que se basa el servicio de directorio de correo corporativo, una implementación libre y de código abierto del protocolo LDAP.

Organismo LDAP: Entidad de la Junta de Andalucía (Consejería, Delegación Provincial, organismo autónomo, agencia pública, …) que dispone de una rama LDAP para gestionar a los usuarios que trabajan en ella.

Punto de servicio: Lugar desde donde se presta un servicio de RCJA. Puede estar ubicado en una sede, en cuyo caso la dirección postal será la de ésta, o en una dirección postal alternativa.

Rama LDAP: Estructura en LDAP que contiene los usuarios de una entidad de la Junta de Andalucía (Consejería, Delegación Provincial, organismo autónomo, agencia pública, etc.) con un nombre único, que generalmente es un acrónimo del nombre de la entidad.

RCJA: Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía. La Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía, integra el conjunto de servicios avanzados de telecomunicaciones para todos los organismos de la Administración

Responsable del Directorio de Correo Corporativo: Empleado público responsable del servicio de Directorio de Correo Corporativo.

Responsable de Rama: Persona física encargada de la gestión de una rama LDAP, responsable de mantener la vigencia y la autenticidad de la información recogida en cada rama.

Sede: Edificio con dirección postal normalizada donde trabaja un conjunto de empleados públicos de la Junta de Andalucía.

Sirhus: Sistema de información de gestión integrada de recursos humanos de la Junta de Andalucía.

Sistema RR.HH.: Sistema de información para la gestión de Recursos Humanos en un organismo adscrito a la Junta de Andalucía que no hace uso de Sirhus, en el que se encuentran dados de alta los empleados públicos que trabajan para dichos organismos.

Usuario LDAP: Conjunto de atributos que definen a un usuario en el ámbito del DCC.

Dos. Clasificación de los usuarios en el Directorio.

Los diferentes tipos de usuario que existen en el Directorio de Correo Corporativo se pueden clasificar según el tipo de usuario y según el tipo de entrada LDAP.

Según el tipo de usuario:

- Usuario LDAP Sirhus: Usuario LDAP asignado a un empleado público dado de alta en Sirhus.

- Usuario LDAP interno: Usuario LDAP asignado a un empleado público dado de alta en cualquier otro Sistema de RR.HH. distinto de Sirhus.

- Usuario LDAP externo: Usuario LDAP perteneciente a una persona que no es empleado público, prestando sus servicios en un organismo que está dado de alta en el Directorio de Correo Corporativo.

- Usuario LDAP genérico: Usuario LDAP no perteneciente a una persona física, sino de uso de propósito general, como nombre de proyecto, servicios generales de los organismos, entre otros.

- Usuario LDAP Lista de distribución: Usuario LDAP perteneciente a una lista de correo electrónico (dirección de correo electrónico que al recibir un correo lo hace llegar de forma simultánea a todos los miembros incluidos en dicha lista).

Según el tipo de entrada LDAP:

- Usuario LDAP con buzón de correo electrónico: Entrada en el Directorio de Correo Corporativo que lleva asociado un buzón de correo electrónico de cualquiera de los dominios de correo gestionados por la Junta de Andalucía, principalmente @juntadeandalucia.es.

00299737

- Usuario LDAP de aplicaciones: Entrada en el Directorio de Correo Corporativo que no lleva asociado un buzón de correo electrónico corporativo. Sólo se utiliza para autenticar contra algún servicio prestado por el DCC.

Tres. Nomenclatura de usuarios.

Los organismos que tienen una rama en el DCC podrán generar los identificadores de los usuarios utilizando el espacio de nombres general o uno propio según las reglas que se indican a continuación:

- Para los organismos que formen parte del espacio de nombres general, los usuarios LDAP seguirán los siguientes formatos:
  - Usuarios Sirhus e internos: El identificador se basará en una combinación del nombre completo y los apellidos de la persona, que no coincida con ningún otro usuario LDAP existente en el sistema.
  - Usuarios externos: El identificador se basará en una combinación del nombre y apellidos de la persona, a los que se les unirá el sufijo «.ext».
  - Usuarios genéricos y listas de distribución: Tendrán un identificador libre, pero con el sufijo del acrónimo del organismo al final del mismo.
- Se autoriza al RDCC a permitir espacios de nombres alternativos, mediante el empleo de sufijos diferenciados, a organismos que por volumen de usuarios puedan presentar colisiones (casos en los que a dos usuarios con nombre parecido el sistema les asigna el mismo nombre de código de usuario) coincidencias con los organismos que se encuentran en el espacio de nombres general.
- Los usuarios internos y externos dependientes de un organismo poseedor de un espacio de nombre propio tendrán un identificador basado en el nombre y los apellidos del usuario, al que se le añadirá el sufijo que se determine para el tipo de usuario en el organismo.

Se aplicarán, además, las siguientes normas adicionales:

- Quedan excluidas partículas como «del», «de las», «de los», … de los identificadores de correo de personas físicas.
- Todas las cuentas de personas físicas (usuarios Sirhus, internos y externos) deberán contener un NIF o NIE asociado al usuario LDAP. El campo designado en el DCC para albergar dicha información será JAdni.
- Las cuentas genéricas deberán tener asignada una persona física responsable, con un usuario de DCC.
- No se permitirá más de un usuario LDAP de un tipo, interno o externo, con un mismo NIF dentro de una rama LDAP, ni más de cinco usuarios LDAP en todo el Directorio de Correo Corporativo con un mismo NIF asociado.
- Se autoriza al RDCC a permitir a los organismos la utilización de identificadores de usuarios que no cumplan con las reglas establecidas para cada tipo de usuario, previa justificación de las razones técnicas o de organización que justifiquen la excepcionalidad.
- Se autoriza al RDCC al borrado de aquellos usuarios que incumplan las reglas y no cuenten con la correspondiente autorización del RDCC, previo aviso a los administradores de ramas LDAP en la que se encuentren dichos usuarios, así como a los propios usuarios.

Cuatro. Provisión de identidades a empleados públicos con Sirhus.

Sirhus proporcionará diariamente la información sobre los usuarios dados de alta y de baja en su sistema y una aplicación se encargará de sincronizar estos cambios de forma automática en el Directorio de Correo Corporativo.

Los usuarios LDAP de Sirhus se mantendrán el periodo máximo permitido por el ENS después de la fecha en la que causen baja en dicho sistema. Pasado ese tiempo, se procederá al borrado automático del usuario LDAP, previo aviso a los administradores y los responsables de rama, de dicho borrado.

00299737

De forma excepcional, se autoriza al RDCC a que prorrogue este plazo a aquellos usuarios cuyas circunstancias particulares queden debidamente justificadas por parte del administrador de la rama LDAP en la que se ubica.

Cinco. Provisión de identidades a empleados públicos de organismos con otros sistemas de RR.HH.

El alta, modificación y baja de empleados públicos que no están en Sirhus quedará delegada en los administradores de la rama LDAP donde se ubiquen o deban ubicarse estos usuarios.

Será responsabilidad de los administradores de las ramas de LDAP la vigilancia y revisión del correcto uso de los usuarios LDAP de empleados públicos que se ubican en dichas ramas.

Cada organismo deberá enviar periódicamente, en el formato que se determine, un listado con todos los empleados que se encuentren de alta en los sistemas de RR.HH. de su organización. El DCC se encargará de reflejar de forma automática, en base a ese listado, las altas y bajas que no hubieran quedado reflejadas por el administrador de la rama LDAP del organismo de forma manual.

El incumplimiento del apartado anterior podrá conllevar la suspensión temporal de creación de nuevos usuarios LDAP al organismo, si así lo determina el RDCC.

Seis. Provisión de identidades a usuarios externos, genéricos y listas de distribución.

El alta, modificación y baja de usuarios externos, genéricos y listas de distribución quedarán delegados en los administradores de la rama del DCC en la que se ubiquen estos usuarios.

Para los usuarios externos se exigirá un NIF único en la rama, que corresponderá siempre a una persona física, quedando prohibida la existencia de personas jurídicas.

Las cuentas genéricas deberán tener asignada una persona física responsable que ya figure en el Directorio de Correo Corporativo.

Siete. Mantenimiento y baja de usuarios en el Directorio de Correo Corporativo.

La presente resolución faculta al RDCC a la baja de usuarios para los que no haya constancia de que han accedido a los sistemas de información en un plazo determinado por el tipo de usuario:

- Los usuarios con buzón de correo electrónico corporativo se darán de baja cuando no haya constancia de acceso o envío de correo electrónico durante los últimos doce meses.

- Los usuarios de aplicaciones sin buzón de correo corporativo se darán de baja cuando transcurran 15 meses sin evidencia de actividad».

Para llevar a cabo la baja, se establece un proceso de eliminación automática de usuarios que constará de tres fases:

- Fase 1: Desactivación temporal de los usuarios LDAP.

- Fase 2: Aviso a los usuarios y administradores de rama LDAP de que van a ser borrados si continúan sin acceder a los sistemas de información de la Junta de Andalucía.

- Fase 3: Eliminación definitiva de los usuarios LDAP que hayan superado el tiempo establecido según los plazos indicados en el primer apartado.

Este procedimiento será de aplicación para:

- Usuarios LDAP de empleados públicos de organismos que no están en Sirhus mientras no exista una notificación periódica por parte de los organismos de las altas y bajas de los mismos.

-Usuarios LDAP de personal externo, cuentas genéricas y listas de distribución.

Se faculta al RDCC a establecer procedimientos para permitir que determinados usuarios LDAP, previa correcta justificación por parte del administrador de la rama, puedan continuar en sus ramas a pesar de superar el plazo determinado de inactividad.

00299737

Ocho. Gestión de sedes de la Junta de Andalucía.

Para facilitar el cumplimiento del ENS y la gestión de los recursos vinculados al DCC, se proveerá un listado de las sedes relacionadas con el DCC, incluyendo las sedes en las que actualmente se presta algún servicio público con relación al DCC. Este repositorio estará normalizado por direcciones postales y actuará de repositorio central para el consumo de servicios relacionados con el DCC. Estos servicios deberán hacer uso de este atributo normalizado.

Se requiere a los organismos incluidos dentro del ámbito de la presente resolución llevar a cabo las actuaciones necesarias para mantener actualizadas las sedes vinculadas a su entidad en dicho listado. Serán atribuidas estas actuaciones al responsable de rama en cada entidad incluida en el DCC.

Nueve. Creación de nuevas ramas en el Directorio de Correo Corporativo.

La creación, mantenimiento y borrado de ramas será responsabilidad del RDCC. Para la creación de una nueva rama será necesario que el organismo aporte los siguientes datos:

- Identificador (por lo general, un acrónimo) de la rama, que identificará al organismo de manera unívoca en el DCC.
- Descripción completa de la rama.
- Correo electrónico para notificaciones oficiales y correo electrónico para notificaciones técnicas de la persona o personas responsables de la rama.
- Teléfono de contacto de la persona responsable de la administración de los usuarios de la rama.
- Usuario/s LDAP de Sirhus, interno o externo, responsable de la administración de la rama.

Cuando la creación de una nueva rama se deba a cambios que afecten a una o más ramas preexistentes en el Directorio de Correo Corporativo, los administradores de la/s rama/s antiguas tendrán la obligación de dar de baja o trasladar las cuentas existentes en dichas ramas a la nueva en un plazo máximo de seis meses.

Este plazo podrá ser prorrogado por el RDCC, previa justificación de las razones técnicas, de organización o de cualquier otra índole que impidan llevar a cabo el proceso de actualización de datos en dicho plazo.

Diez. Mantenimiento y baja de ramas en el Directorio de Corporativo Corporativo.

La/s persona/s responsable de la rama tendrán la obligación de mantener actualizados los datos de contacto de ésta.

La presente resolución autoriza al RDCC a actualizar o dar de baja aquellas ramas cuyos responsables incumplan el deber de mantener los datos actualizados, así como a mover las cuentas de ramas antiguas a ramas actuales, agotado el tiempo en el que el organismo deba darlo de baja, previa información a los responsables y administradores de dichas ramas.

Once. Creación y control de réplicas del Directorio de Correo Corporativo.

Con anterioridad a la existencia de la ADA y su asignación de competencias, por razones técnicas y organizativas, los diferentes organismos relacionados con el DCC, estaban facultados para disponer en sus sedes de réplicas del mismo. Estas réplicas podían tener un carácter parcial o total.

Con carácter general, es objetivo de esta resolución tanto minimizar el número de las réplicas existentes en los organismos de la Junta de Andalucía como el número de atributos no estandarizados, siendo necesaria la justificación sobre la existencia de los mismos.

Para ello:

- El RDCC pondrá a disposición de los organismos un conjunto de instancias LDAP sobre la que estos puedan configurar el sistema de autenticación de sus aplicaciones.

00299737

- Se faculta al RDCC a autorizar a los organismos la utilización de una réplica propia del Directorio de Correo Corporativo o de una parte de él, previa justificación de las razones técnicas o de cualquier otra índole.

- Los organismos que en la actualidad dispongan de una réplica de la totalidad o parte del servicio de DCC deberán justificar su necesidad ante el requerimiento del RDCC o la persona que este determine.

- Para la autorización deberán facilitar al menos los siguientes datos:
  • Servidor donde desean realizar la réplica.
  • La/s rama/s que desean replicar.
  • Persona responsable de la administración de la réplica.
  • Justificación de la necesidad de disponer de una réplica.

Doce. Cumplimiento: control y auditoría.

La Agencia Digital de Andalucía pondrá los medios necesarios para el control efectivo de las autorizaciones emitidas.

La Agencia Digital de Andalucía podrá auditar y monitorizar las actividades realizadas sobre el DCC, con el objetivo de prevenir y detectar incidentes de seguridad, verificando el cumplimiento de las medidas de seguridad establecidas.

El proceso de auditoría y monitorización será llevado a cabo por el personal técnico de la ADA o bien por parte de la persona física o jurídica con la especialización suficiente que la Agencia haya estimado para la realización de esta tarea.

Bajo los procesos de auditoría y monitorización podrá solicitarse a las entidades integradas en el DCC toda aquella información necesaria y pertinente para asegurar el correcto cumplimiento de las normas en seguridad, identidad y protección del dato vigentes. La participación en estos procesos no tendrá carácter optativo, siendo obligatoria la colaboración de las entidades. La falta de colaboración en los procesos aquí descritos derivará en las acciones que se consideren oportunas.

Entre las principales tareas susceptibles de ser sometidas a control y auditoría por parte de la ADA se encontrarán, al menos, las siguientes:

- Revisión de cuentas activas.
- Autorizaciones especiales.
- Vigencia de los usuarios de alta en el sistema.
- Cumplimiento de las normas detalladas en esta resolución.
- Cumplimiento de las normas de nomenclatura en cuentas.
- Seguimiento y control de las ramas asociadas a los organismos.
- Identificación fehaciente de los titulares de las cuentas en el directorio.
- Seguimiento de asignación y uso de las cuentas genéricas.

El RDCC o la persona designada por la ADA podrá establecer las tareas de control y auditoría que estime oportunas.

Trece. Comunicación y notificación de incidentes de seguridad.

En los incidentes de seguridad que afecten al DCC, las entidades participantes del DCC deberán seguir las medidas de comunicación y notificación de incidentes de seguridad según la Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC.

Catorce. Autenticación en sistemas basada en el Directorio de Correo Corporativo.

Los sistemas de información cuyo nivel de seguridad permita el acceso mediante nombre de usuario y contraseña usarán, con carácter general, la autenticación basada en el Directorio de Correo Corporativo al objeto de facilitar el cumplimiento del artículo 17, «Autorización y control de los accesos», del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. En este sentido, la Agencia Digital de Andalucía facilitará la plataforma de integración con el Directorio de Correo Corporativo para la gestión de identidades y accesos necesaria para el proceso de autenticación.

00299737