

RESOLUCIÓN RECTORAL POR LA QUE SE ACUERDA ADOPTAR LA NORMATIVA DE RED DE LA UNIVERSIDAD DE CANTABRIA

Vista la aprobación, en fecha de 19 de enero de 2026, por el Comité de Seguridad de la Información y de Protección de Datos de la Universidad de Cantabria, de la Normativa de Red de la Universidad de Cantabria y de acuerdo con lo prevenido por el artículo 41 b) de la Política de Seguridad de la Información de la UC, este Rectorado **HA RESUELTO** adoptar la misma en los siguientes términos:

Normativa de Red de la Universidad de Cantabria

Artículo 1: Introducción

La Red UNICAN es la infraestructura de comunicaciones corporativa que la Universidad de Cantabria pone a disposición de la comunidad universitaria para el cumplimiento de sus fines. Proporciona acceso a recursos internos y externos, y facilita la comunicación con las redes académicas de investigación e Internet.

La gestión de la Red UNICAN corresponde al Servicio de Informática, siendo sus responsabilidades:

- El diseño, implementación y planificación de la capacidad de la Red UNICAN.
- El mantenimiento, administración, operación y seguridad de la Red UNICAN.
- La interlocución con Red Iris (Red Académica y de Investigación Española).
- La gestión de proveedores externos vinculados al mantenimiento, ampliación u operación de la red.
- La coordinación con el Servicio de Infraestructuras para las intervenciones que afecten al cableado o la red de telefonía.

La presente norma desarrolla la regulación de la Red UNICAN, adecuándose a lo dispuesto por el Real Decreto 311/2022 (Esquema Nacional de Seguridad), y la *Política de Seguridad de la Información de la Universidad de Cantabria* y por el *Reglamento de Uso de Recursos TIC de la Universidad de Cantabria*.

Artículo 2: Ámbito de aplicación

La Red UNICAN está constituida por dos infraestructuras principales: red cableada y red inalámbrica.

Artículo 2.1: Red cableada

La red cableada constituye la infraestructura troncal y el medio de acceso principal para los puestos de trabajo y servicios corporativos. Engloba todo el cableado estructurado, la electrónica de red (núcleo, distribución y acceso), los enlaces de interconexión entre edificios y campus, así como los nodos de salida a redes externas, independientemente de su ubicación geográfica.

Debido a sus características de rendimiento, estabilidad y seguridad, el uso de la red cableada es preceptivo para el desempeño de la actividad administrativa, la gestión de servicios críticos y la conexión de equipamiento corporativo fijo.

El acceso a determinados servicios internos críticos puede estar restringido exclusivamente a este medio.

Artículo 2.2: Red inalámbrica

La red inalámbrica (WiFi) es una extensión de la Red UNICAN que proporciona conectividad en el interior de edificios y zonas exteriores mediante puntos de acceso distribuidos.

La red WiFi se concibe como un método de acceso complementario para uso ligero y en movilidad, y no sustituye a la red cableada para puestos de trabajo fijos. Por motivos de seguridad y rendimiento, el acceso a servicios desde esta red presenta limitaciones.

La Universidad participa en la iniciativa Eduroam, permitiendo el acceso seguro a usuarios de instituciones adscritas. Los visitantes que utilicen la red WiFi de UNICAN deberán cumplir la normativa interna de la Universidad de igual forma que los usuarios propios.

Artículo 3: Condiciones de uso

Todos los usuarios de la Red UNICAN deben cumplir con el Reglamento de Uso de Recursos TIC.

En el caso de la red cableada, todo dispositivo conectado que tenga asignada una dirección IP deberá tener asociado un responsable del dispositivo. Un mismo usuario puede figurar como responsable de varios dispositivos.

El responsable del dispositivo tiene las siguientes obligaciones:

- Supervisar que dicho dispositivo dispone del adecuado control de acceso, tal y como establece la Política de Seguridad de la Información.
- Supervisar que los usuarios del dispositivo cumplen la normativa interna.
- Adoptar y respetar todas las medidas de seguridad, herramientas y configuraciones que el Servicio de Informática determine.
- Notificar cualquier incidente de seguridad relacionado con el dispositivo.
- Comunicar al Servicio de Informática cualquier cambio de ubicación física, lógica o de titularidad del dispositivo.

En el caso de la red inalámbrica, el responsable a efectos de cumplimiento de la normativa de uso de la red será el usuario que se haya autenticado para conectar el dispositivo, independientemente de si es miembro de la Universidad de Cantabria o visitante de otras instituciones.

En el caso de redes especiales creadas para eventos o congresos, el responsable del uso que los dispositivos conectados hagan de dicha red será, a efectos de cumplimiento normativo, el solicitante de la creación de dicha red especial.

Artículo 4: Seguridad de la red

Artículo 4.1: Prohibición del acceso remoto a sistemas internos

Queda expresamente prohibido el uso de aplicaciones o técnicas que permitan conexiones remotas directas a equipos internos desde redes externas. El acceso remoto deberá realizarse exclusivamente a través de la VPN institucional u otros canales autorizados por el Servicio de Informática.

Esta restricción incluye soluciones de escritorio remoto, redes overlay, túneles inversos, dispositivos que conecten a redes de otras tecnologías y similares, que eludan los controles de seguridad perimetrales.

Cualquier excepción requiere autorización expresa del Responsable de Seguridad y el Servicio de Informática, previo análisis de riesgos.

Artículo 4.2: Apertura de servicios a internet

La exposición de servicios a Internet introduce riesgos críticos para la Red UNICAN, por lo que toda apertura debe responder a necesidades operativas imprescindibles y estar sujeta a autorización previa.

El responsable del dispositivo deberá formalizar la solicitud detallando la justificación técnica, el alcance, la duración estimada, los medios técnicos disponibles y medidas de seguridad aplicadas y el proyecto asociado.

El Responsable de Seguridad y el Servicio de Informática evaluarán la solicitud considerando la criticidad, el nivel de riesgo, el estado de actualización del sistema y la viabilidad de alternativas seguras (como el uso de VPN). Podrán requerirse medidas compensatorias adicionales o denegarse la solicitud si no se alcanzan los criterios de seguridad exigidos.

En caso de aprobación, el solicitante asume el compromiso de instalar el agente de monitorización institucional y mantener el sistema permanentemente actualizado y libre de vulnerabilidades. Todas las aperturas se registrarán en un inventario y estarán sujetas a revisión periódica.

Finalizado el plazo autorizado, el servicio se cerrará automáticamente salvo solicitud expresa de renovación, que conllevará la reevaluación de la solicitud.

Artículo 4.3: Segmentación de redes

Para garantizar la seguridad y disponibilidad, la Red UNICAN implementa segmentación de redes. Estas medidas limitan la exposición de recursos críticos y mitigan movimientos laterales ante incidentes.

La red se segmenta en zonas según criticidad y naturaleza de los servicios, con políticas de acceso que restringen la comunicación entre segmentos. Los dispositivos se asignarán al segmento correspondiente según su función.

Cualquier excepción a las políticas de segmentación requiere solicitud formal, justificación técnica y análisis de riesgos por parte del Responsable de Seguridad.

Artículo 5: Documentación y notificación de incidencias

La documentación, instrucciones de acceso, limitaciones en vigor, recomendaciones y resto de procedimientos e información que deba hallarse públicamente disponible en relación con la Red UNICAN se mantendrá actualizada por el Servicio de Informática en su sitio web <https://sdei.unican.es>.

Los usuarios deberán contactar con el Servicio de Informática para cualquier cuestión relacionada con la infraestructura de red de la forma habitual a través de su servicio de Atención a Usuarios (sopORTE@unican.es).

LA RECTORA,

Fdo.: María Concepción López Fernández