**LINEAMIENTOS PARA LA GESTIÓN Y USO DEL ACCESO REMOTO**

**OBJETIVO**

Establecer un marco orientador para la gestión del acceso remoto a los servicios informáticos y recursos institucionales de la Universidad Católica de Manizales, mediante un protocolo claro, seguro y estandarizado. Este lineamiento tiene como propósito principal garantizar que dicho acceso se lleve a cabo en estricto cumplimiento de los lineamientos de seguridad de la información, velando por la **disponibilidad, integridad y confidencialidad** de los activos institucionales. De igual forma, busca asegurar la trazabilidad de las solicitudes, la validación de la necesidad del acceso por parte de los responsables designados y la implementación de controles técnicos adecuados que salvaguarden la infraestructura tecnológica de la Universidad

**ALCANCE**

El presente lineamiento aplica a todas las actividades asociadas con el acceso remoto a los recursos y servicios tecnológicos de la Universidad Católica de Manizales (UCM), brindado a miembros de la comunidad universitaria, colaboradores o proveedores que, por razones justificadas, requieran conexión remota a equipos físicos ubicados en las instalaciones o a servidores institucionales.

Este acceso se proporciona a través de mecanismos como la Red Privada Virtual (VPN), herramienta que permite asegurar la continuidad operativa de la Universidad, pero que, al mismo tiempo, representa riesgos que deben ser gestionados adecuadamente. Por ello, este lineamiento ha sido estructurado conforme a buenas prácticas de seguridad de la información, en concordancia con los lineamientos de la norma ISO/IEC 27001.

El lineamiento comprende desde la presentación formal de la solicitud de acceso remoto, su validación por parte de la Unidad de Sistemas de Información, la configuración técnica por la Unidad de Redes, la asignación de credenciales (temporales o permanentes), el uso supervisado, el monitoreo, el registro de actividades, hasta la finalización de la sesión y el cierre del acceso. Asimismo, incluye la revocación o desactivación de accesos otorgados cuando se cumpla el propósito de la conexión o se detecte algún incumplimiento de las disposiciones institucionales de seguridad.

En consecuencia, el presente lineamiento establece los pasos que deben seguirse para solicitar, aprobar, habilitar y supervisar el acceso remoto a los recursos institucionales. Cada etapa del proceso ha sido diseñada para garantizar la protección de la información, el cumplimiento de los controles establecidos por la Universidad y la trazabilidad de las acciones realizadas por los usuarios autorizados.

### **Proceso para la Gestión del Acceso Remoto**

El proceso para autorizar y habilitar el acceso remoto a los recursos tecnológicos de la Universidad Católica de Manizales está compuesto por las siguientes etapas:

### **1. Solicitud de acceso**

El usuario interesado deberá enviar una solicitud formal a su jefe inmediato, indicando la razón del requerimiento, el recurso al que desea acceder, la fecha y hora de inicio, y la fecha y hora estimada de finalización del acceso. Esta solicitud podrá realizarse mediante correo electrónico institucional o SAIA.

### **2. Análisis y validación por parte del jefe inmediato**

El jefe inmediato evaluará la necesidad del acceso remoto, la sensibilidad de la información a la que se accederá, y si corresponde con las funciones del solicitante. En caso de aprobación, la solicitud será enviada a la Unidad de Sistemas a través de la herramienta de mesa de ayuda, SAIA o correo electrónico institucional.

### **3. Evaluación técnica de la solicitud**

La Unidad de Sistemas analizará la solicitud recibida, revisará su viabilidad técnica, y escalará el caso a la Unidad de Redes para su configuración, siempre que cumpla con los criterios de seguridad y justificación operativa.

### **4. Aprobación o rechazo del acceso remoto**

Una vez realizada la evaluación técnica, la solicitud podrá ser aprobada o rechazada. En caso de aprobación, se coordinará la configuración del acceso remoto con los permisos mínimos requeridos para cumplir con la solicitud. La asignación de credenciales y configuraciones de VPN será gestionada por el ingeniero de redes, quien además notificará al usuario las instrucciones de acceso.

### **5. Configuración y habilitación del acceso**

El acceso se habilitará únicamente al equipo, carpeta de red o sistema específico solicitado, bajo un perfil de usuario estándar, con las restricciones necesarias y con medidas de seguridad tales como antivirus actualizado, autenticación segura y cifrado. El acceso remoto estará registrado, monitoreado y limitado al tiempo previamente autorizado.

### **6. Seguimiento y finalización del acceso**

Una vez cumplido el tiempo autorizado para la conexión remota, se procederá a su cierre formal. En caso de requerirse una extensión, el usuario deberá realizar una nueva solicitud justificando la necesidad. Los accesos temporales serán revocados automáticamente, y cualquier configuración residual deberá ser deshabilitada por el usuario conforme a las directrices institucionales.

### **Referencias**

El presente lineamiento se fundamenta en las buenas prácticas internacionales de seguridad de la información establecidas en la norma **ISO/IEC 27001**, así como en las directrices operativas sugeridas por la norma complementaria **ISO/IEC 27002**, con el objetivo de fortalecer los mecanismos de control, acceso y trazabilidad en entornos de conexión remota. Estas referencias permiten alinear las acciones institucionales con estándares reconocidos a nivel global en materia de gestión de la seguridad de la información.

**Acceso remoto:**

Conexión a los sistemas o recursos tecnológicos de la universidad desde una ubicación externa, a través de herramientas y protocolos seguros.

**Autenticación:**
Proceso mediante el cual se verifica la identidad de un usuario antes de permitir el acceso a sistemas o servicios.

**Confidencialidad:**
Propiedad de la información que garantiza que solo las personas autorizadas puedan acceder a ella.

**Disponibilidad:**
Cualidad que asegura que los sistemas, servicios y datos estén accesibles y funcionando cuando se necesiten.

**Firewall (Cortafuegos):**

Dispositivo o software que controla y filtra el tráfico de red entre diferentes zonas para proteger los sistemas de accesos no autorizados.

**Integridad:**
Garantía de que la información no ha sido modificada de manera no autorizada, ya sea de forma accidental o maliciosa.

**Red privada virtual (VPN):**

Tecnología que permite establecer una conexión segura y cifrada entre el usuario y los recursos tecnológicos institucionales, a través de redes públicas o no confiables.

**Usuario autorizado:**

Miembro de la comunidad universitaria (colaborador, proveedor, estudiante u otro) al que se le ha concedido permiso formal para acceder remotamente a los sistemas o recursos de la universidad.

|  |  |  |  |
| --- | --- | --- | --- |
| **Elaboró** | **Revisó** | **Aprobó** | **Fecha de vigencia** |
| Coordinación Unidad de Sistemas de Información | Aseguramiento de la Calidad | Rectoría |  |

**CONTROL DE CAMBIOS**

|  |  |
| --- | --- |
| **ITEM** | **MODIFICACIÓN** |
|  |  |