

**11 – Acceso Inalámbrico**

**CASIG 4 – Control de Acceso e Identidades**

**Preguntas de Auditoría**

**Acceso Inalámbrico**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. **Conocimiento de Normativas y Estándares**: Familiaridad con marcos de referencia y estándares de la industria como NIST, ISO 27001, CIS, entre otros. 2. **Habilidades Analíticas**: Capacidad para analizar registros, logs y datos para identificar patrones anómalos o actividades sospechosas. 3. **Comprensión de Sistemas de Autenticación**: Entender diferentes mecanismos de autenticación, como autenticación de dos factores, tokens, certificados digitales, entre otros. 4. **Conocimiento de Tecnologías de Red**: Entender cómo funcionan las redes, protocolos y cómo se pueden explotar las vulnerabilidades relacionadas con el acceso. 5. **Habilidades de Comunicación**: Capacidad para comunicar hallazgos, riesgos y recomendaciones de manera clara a diferentes audiencias, desde técnicos hasta ejecutivos. 6. **Conocimiento de Herramientas de Auditoría**: Familiaridad con herramientas y software específicos utilizados para auditar sistemas y redes. 7. **Comprensión de la Gestión de Riesgos**: Capacidad para identificar, evaluar y priorizar riesgos asociados con la administración de cuentas y credenciales. 8. **Habilidades de Investigación**: Capacidad para investigar incidentes de seguridad, identificar la causa raíz y recomendar medidas correctivas. 9. **Conocimiento de Procesos de Negocio**: Entender cómo funcionan los procesos de negocio y cómo la administración de cuentas y credenciales se integra en ellos. 10. **Habilidades Interpersonales**: Capacidad para trabajar en equipo, gestionar conflictos y colaborar con diferentes departamentos y partes interesadas. 11. **Conocimiento de Legislación y Cumplimiento**: Estar al tanto de las leyes y regulaciones pertinentes que afectan la administración de cuentas y credenciales en la jurisdicción relevante. |

# Visión General

En el contexto actual de interconectividad y movilidad, el acceso inalámbrico a los sistemas críticos de información representa tanto una ventaja operativa como un riesgo significativo para la seguridad. La gestión del acceso inalámbrico garantiza que solo los usuarios autorizados accedan a los recursos organizacionales desde ubicaciones y dispositivos adecuados. Los dispositivos móviles y las conexiones inalámbricas incrementan la superficie de ataque, especialmente cuando los sistemas se acceden desde ubicaciones externas a las instalaciones controladas de la organización. Por ello, un control riguroso sobre la autorización, autenticación y uso de dispositivos es fundamental para evitar accesos no autorizados, fugas de información y mantener la integridad y confidencialidad de los datos en todo momento.

La implementación de políticas de acceso seguro involucra tanto la configuración de los dispositivos como la gestión de conexiones y el monitoreo de accesos, promoviendo un entorno seguro donde el acceso inalámbrico esté debidamente controlado. Estas medidas son parte integral de una estrategia más amplia de Gestión de Acceso e Identidades (IAM, por sus siglas en inglés), que busca regular quién, cuándo y desde dónde se puede acceder a los sistemas críticos de la organización.

**1.1 Directrices para el Control de Acceso Inalámbrico**

El acceso inalámbrico al sistema se realiza solo después de la autorización de cada tipo de dispositivo y conexión, con configuraciones específicas para el uso dentro y fuera de áreas controladas. Las principales directrices incluyen:

* **Restricción de Dispositivos Externos:** Limitar el uso de dispositivos de almacenamiento portátiles y componentes que no sean de la organización en sistemas externos.
* **Prohibición de Dispositivos No Autorizados:** Evitar el uso de dispositivos de almacenamiento accesibles en red y restringir los dispositivos no clasificados en áreas de sistemas clasificados.

Además, el acceso inalámbrico incluye mecanismos de autenticación para usuarios y dispositivos, junto con cifrado integral para proteger la información sobre dispositivos móviles, y desactivación de redes inalámbricas en equipos cuando no están en uso.

**1.2 Directrices Específicas para el Control de Acceso de Dispositivos Móviles**

Cada acceso de dispositivos móviles debe cumplir con una configuración establecida que asegure el control de conexiones y la protección de la información. Las medidas incluyen:

* **Requisitos de Configuración y Conexión:** Documentar los requisitos de configuración y los sistemas externos prohibidos por la organización.
* **Términos y Condiciones de Uso Externo:** Para dispositivos móviles en sistemas externos, se aplican acuerdos con otras organizaciones que operen estos sistemas, determinando los niveles de acceso y restricciones.

Se requiere que los dispositivos no clasificados en instalaciones sensibles tengan restricciones adicionales, como la prohibición de conexiones a sistemas clasificados, y están sujetos a inspecciones para detectar información clasificada inadvertida.

**1.3 Perspectiva de Auditoría en el Control de Acceso Inalámbrico**

La auditoría del control de acceso inalámbrico verifica la implementación de políticas de autorización, autenticación y cifrado, asegurando que los accesos y el uso de dispositivos móviles se alineen con las directrices organizacionales. Los auditores revisan la documentación de requisitos de configuración y conexión, la autorización de dispositivos, y el cumplimiento de las condiciones en sistemas externos, promoviendo un uso seguro y controlado de la infraestructura inalámbrica.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1 Autorizar cada tipo de acceso inalámbrico y dispositivos móviles al sistema antes de permitir dichas conexiones incluyendo la configuración para cuando dichos dispositivos estén fuera de las áreas controladas. Al momento de autorizar, se debe tener en cuenta:  1.1 Restringir el uso de dispositivos de almacenamiento portátiles controlados por la organización por parte de personas autorizadas en sistemas externos.  1.1 Restringir el uso de sistemas o componentes de sistemas que no pertenezcan a la organización para procesar, almacenar o transmitir información de la organización.  1.1 Prohibir el uso de dispositivos de almacenamiento accesibles en red.  1.1 Prohibir el uso de dispositivos de almacenamiento portátiles controlados por la organización por parte de personas autorizadas en sistemas externos.   2 Proteger el acceso inalámbrico al sistema mediante la autenticación de usuarios, dispositivos y cifrado. Se debe tener en consideración para personas autorizadas que usen un sistema externo para acceder al sistema o para procesar, almacenar o transmitir información controlada por la organización solo después de:  2.1 Verificación de la implementación de controles en el sistema externo como se especifica en las políticas de seguridad y privacidad y los planes de seguridad y privacidad de la organización.  2.2 Retención de la conexión del sistema aprobado o acuerdos de procesamiento con la entidad organizativa que aloja el sistema externo.  3. Emplear cifrado del dispositivo completo y/o cifrado basado en contenedores para proteger la confidencialidad e integridad de la información sobre los dispositivos móviles.  4 Deshabilitar, cuando no esté previstas para su uso, las capacidades de redes inalámbricas integradas en los componentes del sistema antes de su emisión y despliegue.  5 Seleccionar antenas de radio y calibre los niveles de potencia de transmisión para reducir la probabilidad de que las señales de los puntos de acceso inalámbrico puedan recibirse fuera de los límites controlados por la organización.  . |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer y documentar para cada tipo de acceso inalámbrico y los dispositivos móviles controlados por la organización:  1.1 Los requisitos de configuración  1.2 Los requisitos de conexión   1.3 Tipos de sistemas externos prohibidos por la organización  1.4 La guía de implementación   2. Incluír dentro de los requisitos de control de acceso para dispositivos móviles:  2.1 Prohibir el uso de dispositivos móviles no clasificados en instalaciones que contengan sistemas que procesen, almacenen o transmitan información clasificada, a menos que lo permita específicamente el funcionario autorizador. Las personas a las que se les autorice el uso de dispositivos móviles no clasificados en estas instalaciones deben seguir las siguientes restricciones:  2.1.1 Está prohibida la conexión de dispositivos móviles no clasificados a sistemas clasificados.  2.1.2 La conexión de dispositivos móviles no clasificados a sistemas no clasificados requiere la aprobación del funcionario autorizador.  2.1.3 Está prohibido el uso de módems internos o externos o interfaces inalámbricas dentro de los dispositivos móviles no clasificados.  2.1.4 Los dispositivos móviles no clasificados y la información almacenada en esos dispositivos están sujetos a revisiones e inspecciones aleatorias por parte de funcionarios de seguridad definidos por la organización, y si se encuentra información clasificada, se sigue la política de manejo de incidentes.  2.2 Restringir la conexión de dispositivos móviles clasificados a sistemas clasificados de acuerdo con las políticas de seguridad definidas por la organización.  3. Establecer términos y condiciones e identificar controles necesarios en sistemas externos, en conformidad con las relaciones de confianza establecidas con otras organizaciones que poseen, operan y/o realizan mantenimiento de sistemas externos, permitiendo a las personas autorizadas:  3.1. Acceder al sistema desde sistemas externos.  3.2. Procesar, almacenar o transmitir información controlada por la organización utilizando sistemas externos.  3.3 Determinar si las autorizaciones de acceso asignadas a un socio que comparte información coinciden con las restricciones de acceso y uso de la información para circunstancias de intercambio de información en las que se requiere la discreción del usuario. Para esto, se deben:  3.3.1 Emplear mecanismos automatizados o procesos manuales para ayudar a los usuarios a tomar decisiones sobre colaboración e intercambio de información.  3.3.2 Emplear mecanismos automatizados para hacer cumplir las decisiones de intercambio de información por parte de los usuarios autorizados en función de las autorizaciones de acceso de los socios de intercambio y las restricciones de acceso a la información que se compartirá.   3.3.3 Implementar servicios de búsqueda y recuperación de información que apliquen restricciones de intercambio de información.  4. Identificar y autorizar explícitamente a los usuarios que pueden configurar de forma independiente las capacidades de redes inalámbricas. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. |  |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles |  |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. |  |

# Preguntas de Auditoría para el Acceso Inalámbrico

|  |
| --- |
| 3.1 Temática: Control de Acceso Inalámbrico |
| Durante esta evaluación, el auditor debe revisar los controles y medidas de seguridad establecidas para proteger las redes inalámbricas y evaluar si se utilizan protocolos de autenticación fuertes y cifrado robusto para prevenir accesos no autorizados. Se verificará si las redes inalámbricas están configuradas correctamente y si se implementan políticas de gestión para supervisar y administrar dispositivos conectados. Además, se analizarán los registros de acceso y se revisarán las medidas de prevención de intrusiones para garantizar la integridad de las redes inalámbricas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen requisitos de configuración documentados para cada tipo de acceso inalámbrico utilizado en la organización? * Verifique si se pueden encontrar documentos o guías que detallen los requisitos de configuración específicos para cada tipo de acceso inalámbrico, como WiFi, Bluetooth, etc. * ¿Existe una guía de implementación detallada para cada tipo de acceso inalámbrico? * ¿Se actualizan regularmente los requisitos de configuración y la guía de implementación para mantenerse al día con las mejores prácticas de seguridad? * ¿La organización configura los dispositivos para que no resulten visibles a terceros? ¿Se asigna nombres a los dispositivos que no reflejen marcas ni modelos? * ¿Se modifica el nombre de la wifi o SSID (Service Set Identifier)? * ¿Existe un proceso documentado para autorizar y gestionar el acceso inalámbrico al sistema? ¿Se establecen criterios claros? * ¿Los usuarios tienen una cuenta personal e intransferible para acceder a la red? * Verifique si los usuarios tienen un acceso Wifi a la red establecida y regida por reglas la organización para acceder a la red, el usuario será responsable de cualquier actividad que se realice bajo sus dispositivos usados. * Evalúe una muestra de solicitudes de acceso inalámbrico aprobadas para determinar si los criterios establecidos se aplicaron consistentemente. * ¿Se documentan las solicitudes y aprobaciones de acceso inalámbrico? * ¿Se implementa autenticación para controlar el acceso a las redes inalámbricas? * Realice pruebas de conexión a una muestra de redes inalámbricas para verificar si se solicita un proceso de autenticación adecuado. * ¿Se autentican los dispositivos antes de permitir el acceso a la red inalámbrica? * ¿Se utiliza cifrado para proteger la comunicación inalámbrica? * Revise las configuraciones de seguridad de las redes inalámbricas para identificar si se implementa el cifrado (por ejemplo, WPA2, WPA3) en lugar de dejar las redes en modo abierto. * Escanee las redes inalámbricas disponibles para verificar si están configuradas con cifrado activado. * Verifique si los puntos de accesos utilizan autenticación de usuarios y además de restringir la aceptación de la conexión mediante la verificación de la dirección MAC de los equipos. * ¿Existen políticas que establecen requisitos de complejidad para contraseñas de acceso a la red inalámbrica? * ¿Se lleva un registro de acceso a la red inalámbrica y se monitorea para detectar actividades sospechosas? * ¿La organización establece los sistemas de acceso al dispositivo que sean válidos como utilización de PIN o clave de acceso, además de medidas adicionales como el cifrado de la tarjeta? * ¿Se realiza una verificación de rutina para asegurarse de que las capacidades inalámbricas estén deshabilitadas antes de la emisión y el despliegue de componentes? * Evalúe una muestra de componentes recientemente emitidos y desplegados para verificar si las capacidades inalámbricas están desactivadas. * Examine los registros relacionados con los componentes emitidos y desplegados para verificar si se documenta la desactivación de las capacidades inalámbricas. * ¿Existe un proceso documentado para identificar y autorizar a los usuarios que tienen permiso para configurar las capacidades de redes inalámbricas? * Entreviste a los responsables de TI y seguridad para confirmar la existencia y los detalles del proceso de identificación y autorización. * ¿Se mantienen registros de los usuarios que están autorizados para configurar las capacidades de redes inalámbricas? * ¿La autorización para configurar redes inalámbricas se basa en la necesidad de conocer y las responsabilidades laborales? * ¿La organización ha seleccionado antenas de radio adecuadas para sus puntos de acceso inalámbricos? * ¿Se compara las características de las antenas utilizadas con las recomendaciones del fabricante y las necesidades específicas de la organización? * ¿Se han calibrado los niveles de potencia de transmisión de los puntos de acceso inalámbrico para reducir la propagación de señales más allá de los límites controlados? * Utilice herramientas de medición de señal inalámbrica para verificar el alcance de las señales emitidas por los puntos de acceso y comparar los resultados con los límites controlados. * ¿La organización establece una política de uso del BYOD corporativa? * Verifique si se establecen los usos permitidos y las restricciones con respecto al uso de los dispositivos personales.  |  | | --- | | * **BYOD:** Hace referencia a las políticas corporativas de TI que permiten a los empleados utilizar sus propios smartphones, ordenadores portátiles y otros dispositivos para tareas relacionadas con el trabajo. | |

|  |
| --- |
| **3.2 Control de Acceso para Dispositivos Móviles** |
| Evaluar si se utilizan soluciones de gestión de dispositivos móviles (MDM) para aplicar controles de seguridad, como autenticación y cifrado de datos. Se debe revisar los registros de acceso para identificar dispositivos móviles autorizados o cualquier intento de acceso no autorizado, y si se implementan medidas de respuesta a incidentes en caso de pérdida o robo de dispositivos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha establecido requisitos específicos de configuración para los dispositivos móviles que están bajo su control? * ¿Se han definido requisitos de conexión segura para los dispositivos móviles al acceder a redes y sistemas de la organización? * Analice registros de conexión de dispositivos móviles y verificar si se cumplen los requisitos de seguridad al acceder a redes y sistemas. * ¿Los requisitos y la guía de implementación incluyen medidas de seguridad específicas para dispositivos móviles cuando están fuera de las áreas controladas? * ¿Existe una política o procedimiento establecido para la autorización de la conexión de dispositivos móviles a sistemas organizacionales? * Evalúe la documentación para determinar si se establecen los pasos y requisitos necesarios para solicitar y obtener la autorización para conectar dispositivos móviles. * ¿Los usuarios son informados sobre los procedimientos y requisitos para autorizar la conexión de sus dispositivos móviles a los sistemas organizacionales? * Solicite evidencia de evaluaciones de seguridad realizadas en dispositivos móviles previamente autorizados para verificar si se siguió un proceso de revisión. * ¿Se mantiene un registro de los dispositivos móviles autorizados y las fechas de autorización? * ¿Se prohíbe el uso de dispositivos móviles no clasificados en instalaciones que manejen información clasificada, a menos que lo autorice un funcionario responsable de la autorización? * ¿Se aplican controles para prohibir la conexión de dispositivos móviles no clasificados a sistemas clasificados? * ¿Se realizan revisiones e inspecciones aleatorias a los dispositivos móviles no clasificados y la información almacenada en ellos en áreas con sistemas clasificados? * Verifique si existen registros de revisiones e inspecciones aleatorias realizadas por funcionarios de seguridad designados. * ¿La organización emplea cifrado de dispositivo completo en sus dispositivos móviles? * ¿Se utiliza cifrado basado en contenedores para proteger la confidencialidad e integridad de la información en dispositivos móviles definidos por la organización? * Evalúe un dispositivo móvil seleccionado al azar que sea propiedad de la organización y verificar si se ha implementado cifrado basado en contenedores para las aplicaciones y los datos confidenciales. * ¿Se realizan pruebas de eficacia del cifrado en dispositivos móviles? * ¿Existe un proceso para la gestión de dispositivos móviles, incluyendo el monitoreo y control de dispositivos cifrados?  |  | | --- | | **Cifrado basado en contenedores:** Es una técnica de seguridad que implica la creación de un espacio aislado y seguro en el dispositivo donde se almacenan y procesan los datos sensibles y las aplicaciones, separándolos del resto del sistema y de otras aplicaciones. Los datos y las aplicaciones que se almacenan y se ejecutan en este contenedor están protegidos por capas de seguridad. | |

|  |
| --- |
| **3.3 Acceso al Sistema desde Sistemas Externos** |
| Evaluar si se utilizan soluciones como redes virtuales privadas (VPN), para asegurar conexiones seguras y si se implementa autenticación multifactorial para garantizar la identidad del usuario. Se revisarán los registros de acceso remoto para detectar patrones inusuales o intentos de acceso no autorizados, verificar si se establecen y comunican procedimientos de seguridad para los usuarios remotos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha establecido términos y condiciones claros para el acceso y uso de sistemas externos que contienen información controlada? * Compare la documentación de controles definidos por la organización con la implementación real en sistemas externos para confirmar si los controles se están aplicando correctamente. * ¿Se han identificado los controles definidos por la organización que se implementarán en sistemas externos en conformidad con relaciones de confianza establecidas? * ¿Se ha definido un proceso para permitir a las personas autorizadas acceder al sistema desde sistemas externos? * ¿Existe un proceso definido para procesar, almacenar o transmitir información controlada por la organización utilizando sistemas externos? * ¿En los sistemas para la conexión remota a los equipos de la organización se utiliza una red privada virtual, también llamada VPN? * ¿Permite al usuario conectarse a la entidad de una manera segura, incluso desde redes abiertas o poco seguras? * ¿Funciona sobre conexiones 3G, 4G y wifi? * ¿Limita el medio de acceso remoto a la organización a un único punto con autenticación? * ¿Reduce los servicios expuestos a Internet, disminuyendo riesgos, vulnerabilidades y la posibilidad de ser atacados? * ¿Se han identificado los tipos de sistemas externos específicos que están prohibidos por la organización? * Verifique si hay comunicaciones internas, manuales o capacitaciones que describan los tipos de sistemas externos que no están permitidos. * ¿Se implementan medidas técnicas para bloquear o evitar el acceso a los tipos prohibidos de sistemas externos? * ¿Se realizan inspecciones regulares para detectar la presencia de sistemas externos no autorizados? * ¿Se establecen sanciones o consecuencias claras para aquellos que violen los controles de prohibición de sistemas externos? * Entreviste a los empleados para determinar si están al tanto de las consecuencias de utilizar sistemas externos prohibidos. * ¿Se verifica la implementación de controles en los sistemas externos antes de permitir el acceso o el procesamiento de información controlada? * Evalúe una muestra de sistemas externos que han sido autorizados para acceder o procesar información y verificar si hay evidencia de verificación de controles. * ¿Se retiene una conexión aprobada o se establecen acuerdos de procesamiento con la entidad organizativa que aloja el sistema externo? * ¿Se documentan adecuadamente los resultados de la verificación de controles en sistemas externos y las conexiones aprobadas? * ¿La organización establece procedimientos para revisar periódicamente las conexiones aprobadas y los acuerdos de procesamiento con sistemas externos? * ¿Se han implementado medidas técnicas para restringir el uso de dispositivos de almacenamiento portátiles en sistemas externos? * Verifique si existe una solución técnica (por ejemplo, software de gestión de dispositivos) que permita controlar y restringir el acceso de dispositivos de almacenamiento portátiles en sistemas fuera de la red interna. * ¿Se lleva un registro de los usuarios autorizados que tienen permitido usar dispositivos de almacenamiento portátiles en sistemas externos? * ¿Las restricciones definidas por la organización se aplican de manera consistente a todos los sistemas externos y usuarios autorizados? * ¿La organización implementa restricciones para el uso de sistemas o componentes de sistemas que no pertenezcan a la organización para procesar, almacenar o transmitir información de la organización? * ¿Se prohíbe el uso de dispositivos de almacenamiento accesibles en red definidos por la organización en sistemas externos? * ¿Se prohíbe el uso de dispositivos de almacenamiento portátiles controlados por la organización por parte de personas autorizadas en sistemas externos? * Evalúe registros de actividades para identificar posibles incidentes de uso de dispositivos controlados por la organización en sistemas externos. |

|  |
| --- |
| **3.4 Restricciones del intercambio de información** |
| El objetivo es la evaluación de los mecanismos implementadas para controlar y restringir el intercambio de información entre diferentes sistemas y usuarios dentro de una organización. Esto implica asegurarse de que solo se comparta información autorizada y relevante, y que se evite el acceso no autorizado a datos sensibles. Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha definido y documentado mecanismos automatizados o procesos manuales para apoyar a los usuarios en la toma de decisiones relacionadas con la colaboración y el intercambio de información? * Evalúe la existencia de formularios, guías o herramientas que los usuarios puedan utilizar para entender cómo tomar decisiones adecuadas sobre colaboración e intercambio de información. * ¿Los mecanismos automatizados o los procesos manuales incluyen criterios claros para determinar qué tipo de información puede compartirse y con quiénes? * ¿Los mecanismos o procesos consideran aspectos de seguridad, privacidad y nivel de acceso al tomar decisiones? * ¿Se lleva un registro o seguimiento de las decisiones de colaboración e intercambio de información tomadas utilizando los mecanismos o procesos establecidos? * ¿La organización cuenta con mecanismos automatizados para gestionar y hacer cumplir las decisiones de intercambio de información por parte de usuarios autorizados? * ¿Los mecanismos automatizados se basan en las autorizaciones de acceso de los socios de intercambio y las restricciones de acceso a la información compartida? * ¿Los mecanismos automatizados aseguran que solo los usuarios autorizados tengan acceso a la información correspondiente según las decisiones de intercambio? * Realice pruebas de acceso simulado utilizando cuentas de usuario con diferentes niveles de autorización para verificar si los mecanismos automatizados impiden el acceso no autorizado. * ¿Se mantienen registros de las decisiones de intercambio de información y los accesos realizados a la información compartida? * ¿Los mecanismos automatizados son auditables y permiten rastrear las actividades relacionadas con el intercambio de información? * ¿Se han implementado servicios de búsqueda y recuperación de información dentro de la organización? * Verifique si existen sistemas, aplicaciones o herramientas específicas implementadas para facilitar la búsqueda y recuperación de información. * ¿Las restricciones de intercambio de información definidas por la organización se aplican adecuadamente en los servicios de búsqueda y recuperación? * ¿Las restricciones de acceso y compartición de información se ajustan a las políticas y regulaciones de seguridad de la organización? ¿Los usuarios son conscientes de las restricciones? * ¿La organización proporciona a los usuarios autorizados la capacidad de revisar y evaluar las autorizaciones de acceso asignadas a los socios? * Evalúe la existencia de una función o característica en el sistema que permite a los usuarios visualizar las autorizaciones de acceso de los socios. * ¿Se definen restricciones de acceso y uso de la información para situaciones específicas de intercambio de información con socios? * ¿La declaración que establece que el usuario no debe utilizar el servicio si no está de acuerdo con los términos es claramente visible y accesible? * ¿Están claramente establecidas las reglas y responsabilidades de los usuarios para el acceso a la red Wifi? * ¿Se requiere el consentimiento explícito del usuario con respecto a estos términos antes de acceder al servicio? * ¿Se prohíbe de manera explícita la transmisión y distribución de material que viole leyes o derechos de propiedad intelectual? * ¿Se establece la prohibición de transmitir contenido discriminatorio, hostil o intimidatorio? * ¿Se prohíbe la transmisión de información ilegal, abusiva o cuestionable? * ¿Se prohíbe la realización de spam a cualquier destinatario? * ¿Se establece la prohibición de uso comercial y promocional de la red inalámbrica sin autorización? |