

**06 - Acceso Remoto**

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

**Preguntas de Auditoría**

**Acceso Remoto**

|  |
| --- |
| **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

Con la gestión de acceso remoto en SIC se pretende proteger los sistemas y la información organizacional, permitiendo únicamente conexiones remotas autorizadas y seguras. Este proceso implica la autorización de cada tipo de acceso remoto antes de su implementación y la capacidad de deshabilitarlo cuando sea necesario, asegurando un control estricto sobre las conexiones externas. Para reforzar la seguridad, todo el tráfico remoto debe enrutarse a través de puntos de control de red autorizados, y se implementan mecanismos criptográficos para proteger la confidencialidad e integridad de las sesiones. Los comandos privilegiados y el acceso a información sensible mediante acceso remoto requieren evidencia evaluable y se restringen a las necesidades definidas por la organización, usando autenticación avanzada para validar las acciones remotas.

**1.1 Documentación y Restricciones en el Acceso Remoto**

La implementación de acceso remoto se respalda con documentación detallada, que define las restricciones de uso, los requisitos de configuración y la guía de implementación para cada tipo de acceso permitido. Esto incluye la justificación del acceso remoto, documentada en el plan de seguridad del sistema, y la protección de información sensible asociada a los mecanismos de acceso remoto para evitar su divulgación no autorizada. Estos controles y registros aseguran que el acceso remoto sea seguro y cumpla con los estándares de la organización, minimizando riesgos asociados a conexiones externas.

**1.2 Rol de la Auditoría en el Control del Acceso Remoto en SIC**

La auditoría en SIC valida que los accesos remotos se gestionen conforme a las políticas de seguridad y se monitoreen continuamente mediante mecanismos automatizados. Las auditorías verifican que solo se permita el acceso remoto en casos específicos autorizados, y que los controles criptográficos y de autenticación mantengan la integridad de las conexiones. La documentación y los registros de acceso remoto se revisan para confirmar que todas las conexiones y comandos ejecutados se registren adecuadamente, proporcionando una trazabilidad completa que refuerza la seguridad y transparencia del acceso remoto.

# 2. Matriz de Controles

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Autorizar cada tipo de acceso remoto al sistema antes de permitir dichas conexiones.  1.1 Proporcionar la capacidad de desconectar o deshabilitar el acceso remoto al sistema dentro de un período de tiempo definido por la organización.  2. Enrutar los accesos remotos a través de puntos de control de acceso a la red autorizados y administrados.  2.1 Emplear mecanismos automatizados para monitorear y controlar los métodos de acceso remoto.  3. Autorizar la ejecución de comandos privilegiados y el acceso a información relevante para la seguridad a través de acceso remoto solo en un formato que proporcione evidencia evaluable y para las necesidades definidas por la organización.  3.1 Implementar mecanismos criptográficos para proteger la confidencialidad e integridad de las sesiones de acceso remoto.  3.2 Implementar mecanismos para autenticar comandos remotos definidos por la organización.  4. Proteger la información sobre los mecanismos de acceso remoto del uso y la divulgación no autorizada. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer y documentar las restricciones de uso, los requisitos de configuración/conexión y la guía de implementación para cada tipo de acceso remoto permitido.  2. Documentar la justificación del acceso remoto en el plan de seguridad del sistema. |
| 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 Remoto

|  |
| --- |
| 3.1 Temática: Políticas, procedimientos y restricciones del Acceso Remoto |
| La practicas se enfocan en revisar y analizar detalladamente las políticas o controles que regulan y limitan el acceso remoto a los recursos de la organización. El objetivo principal es asegurarse de que existan directrices claras y efectivas que rijan quiénes pueden acceder remotamente, las restricciones y las capacidades de los usuarios. En la auditoria debe revisar en detalle cómo se gestionan las conexiones remotas a los sistemas y recursos de la organización, asegurando que se sigan las mejores prácticas de seguridad. El acceso remoto es esencial para permitir que el personal trabaje de manera eficiente fuera de las instalaciones, pero también puede ser un vector de riesgo significativo si no se maneja adecuadamente. Para disponer de un entorno de teletrabajo, trabajo a distancia o conexiones remotas seguras, el primer paso será establecer una política organizativa en la que se definan las normas a cumplir en los distintos escenarios o respecto al uso de los distintos sistemas y métodos de acceso.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen políticas o procedimientos establecidos para autorizar y gestionar el acceso remoto a los sistemas? * ¿Se requiere una solicitud formal para acceder remotamente a los sistemas? * Verifique que acceso a los sistemas y aplicaciones de forma remota debe estar controlado por el inicio de sesión seguro, en que el usuario de identifica y autentifica. * Examine los registros de autorización y verificación para confirmar que el acceso remoto sea otorgado únicamente después de la aprobación de las partes autorizadas. * ¿La organización mantiene y ejecuta estándares o modelos de seguridad a aplicar en el acceso remoto? Para la evaluación, el auditor debe tener en consideración: * Protocolos para la solicitud y autorización del trabajo remoto. * Verifique los documentos, si tienen las firmas correspondientes en los acuerdos de Confidencialidad y requerimientos entre las partes, para los contratos que requieran acceso remoto. * Protocolos de seguridad para término del servicio que requiere accesos remotos. * Identifique el usuario que dispondrá de esta modalidad y los permisos de acceso remoto de que dispondrá. * Protocolo de conexión remota de emergencia para atender requerimientos de soporte e incidencias puntuales. * Normativas referentes al almacenamiento y recuperación de información fuera de las instalaciones, ya sea en equipos corporativos, personales de funcionarios o dispositivos extraíbles. * Examine la documentación de políticas y procedimientos relacionados con el acceso remoto para asegurarse de que se establezcan requisitos de seguridad específicos, como el uso de VPN, el cifrado de datos, entre otros. * ¿Cuáles son las condiciones que la organización mantiene para un acceso remoto seguro? * Para evaluar el control el acceso remoto, el auditor debe tener en consideración: * Toda conexión remota debe ser solicitada, autorizada y registrada para posterior control de vigencia. Se debe evaluar los modelos de conexión, con el objetivo de discriminar el nivel de seguridad necesario a implementar en la conexión. * Verifique si se utilizan softwares definidos en el estándar para una conexión remota segura, salvo que el Encargado o personal de TI indique otro tipo de conexión. * Los accesos remotos deben estar sujetos a las fechas de inicio y finalización de inicio de sesión, y registrarse. * Verifique si se utilizan métodos de conexión segura, como métodos de identificación y autenticación robusta. * Las actividades efectuadas por los usuarios remotos deben ser registradas en los respectivos Logs. * ¿La organización ha documentado claramente las restricciones de uso para cada tipo de acceso remoto permitido? * Verifique si hay una descripción explícita, como qué recursos se pueden acceder, en qué circunstancias, y si se incluyen escenarios de uso aceptables. * ¿Se han establecido y documentado los requisitos de configuración y conexión para cada tipo de acceso remoto permitido? * Verifique si se proporcionan planes de seguridad e instrucciones claras y detalladas para establecer conexiones seguras y si se abordan los aspectos técnicos necesarios. * ¿Las políticas y los procedimientos relacionados con las capacidades de acceso de los usuarios remotos están formalizados? Considere: * Usuarios remotos (p.ej., empleados, contratistas, terceros) con acceso a los sistemas críticos están aprobados y documentados * Conexiones remotas son solo abiertas según sea requerido. * Conexiones remotas están encriptadas. * La capacidad para borrar datos de forma remota en dispositivos móviles cuando faltan datos o son robados está habilitada. * Los controles de seguridad de la institución (p.ej., antivirus, patch management) son requeridos en dispositivos remotos que se conectan a la red. * ¿Existe un procedimiento que establece el período de tiempo dentro del cual se debe desconectar o deshabilitar el acceso remoto a los sistemas de la organización? * Verifique si se establece un plazo específico para desconectar o deshabilitar dicho acceso. Compare este plazo con las necesidades de seguridad de la organización y las mejores prácticas de la industria. * Revise los registros o evidencia de que los procedimientos de acceso remoto se siguen cuando excede el período de tiempo definido. * ¿Se utilizan puntos de control de acceso a la red autorizados para enrutar las conexiones remotas a la red de la organización? * Revise los registros de configuración de enrutadores/firewalls para confirmar que las conexiones sean dirigidas a través de puntos de control autorizados.} * Revise los inventarios de puntos de control de acceso utilizado para el enrutamiento de conexiones remotas, comparándolo con la infraestructura real para asegurarse de que esté al día y completo. * ¿La organización ha establecidos procedimientos para autorizar el acceso remoto a comandos o programas privilegiados y a información relevante para la seguridad? * Verifique todos los softwares capaces de sobrepasar o anular los controles normales de seguridad, por lo que se debe restringir y controlar su utilización. * Analice la lista de usuarios que tienen acceso remoto a comandos privilegiados y verificar si estos accesos se basan en los roles y responsabilidades de cada individuo dentro de la organización. * Revise si existe un proceso documentado y si se obtiene aprobación de las partes autorizadas antes de otorgar dichos accesos. * ¿Se utiliza procedimientos robustos de Control de Acceso para la identificación, autenticación y autorización de los programas o comandos de utilidad privilegiado? * Segregación del acceso de usuarios autorizados a los programas o comandos de utilidad privilegiada del software de aplicaciones. * Limitación del uso de programas de utilidad privilegiada al número mínimo práctico de usuarios. * ¿La organización realiza auditorías regulares de los procesos de acceso remoto para evaluar su conformidad con las mejores prácticas de seguridad? * ¿Qué tipo de actividades y aspectos son cubiertos por estas auditorías? * ¿Qué áreas específicas se abordan en estas auditorías? * Realice auditorías trimestrales para evaluar la conformidad de las mejores prácticas * ¿Cuáles son las metas cuantitativas específicas establecidas para la utilización efectiva de los recursos de conexión remota y red? * Medir la eficiencia a través de la tasa de utilización de ancho de banda y la latencia en las conexiones remotas. * ¿Qué acciones se toman si las metas cuantitativas no se cumplen? * ¿Se realiza un seguimiento regular de estas métricas y se comparan con las metas establecidas? |

|  |
| --- |
| **3.2 Temática: Mecanismos, herramientas y supervisión para Acceso Remoto** |
| Las Prácticas se centran en evaluar la seguridad, eficacia de los cumplimientos de los procesos y tecnologías que permiten a usuarios acceder a sistemas y recursos desde ubicaciones externas. Implica la utilización de herramientas y sistemas de supervisión que rastrean y registran las actividades de acceso desde ubicaciones externas. Estos mecanismos permiten identificar patrones inusuales o potencialmente maliciosos, lo que ayuda a prevenir intrusiones y ataques. La auditoría evalúa la correcta implementación de protocolos de cifrado y autenticación, que aseguren que los datos se transmitan de manera segura y protegida de interceptaciones no autorizadas, también permite la ejecución de controles de acceso estrictos que autoricen únicamente a usuarios autorizados a acceder a los sistemas de manera remota.  Este levantamiento puede incluir análisis específicos tales como:  ¿Existen herramientas o sistemas de monitoreo implementados para supervisar el acceso remoto a sistemas y redes?   * Verifique la configuración y el funcionamiento de estas herramientas. * Evalúe si se han configurado alertas o notificaciones automatizadas para actividades anómalas, como múltiples intentos de inicio de sesión fallidos. * ¿Se generan registros de actividad de acceso remoto de manera automática? * Verifique la información registrada, como direcciones IP, usuarios, horarios (fecha-hora) y acciones realizadas. * ¿Se definen umbrales de actividad y comportamiento para el acceso remoto en las herramientas de monitoreo? * ¿Existen procedimientos establecidos para revisar regularmente los registros de acceso remoto en busca de actividades inusuales o no autorizadas? * ¿Se ha configurado el cifrado de punto a punto para las sesiones de acceso remoto? * ¿Se utilizan protocolos criptográficos como SSL/TLS o SSH para cifrar las sesiones de acceso remoto? * ¿Se ha configurado el acceso remoto para permitir únicamente conexiones cifradas? * Evalúe la configuración del servidor de acceso remoto para identificar los algoritmos de cifrado utilizados y verificar si cumplen con los estándares de seguridad recomendados. * ¿Se implementan restricciones basadas en direcciones IP para limitar los accesos remotos únicamente a direcciones IP autorizadas? * ¿Se realiza el seguimiento y la revocación adecuada de los privilegios de acceso remoto de los empleados que abandonan la organización? * ¿Se han establecido mecanismos de autenticación para validar la identidad de los usuarios que emiten comandos remotos? * Verificar si se utiliza autenticación de dos factores (2FA), certificados digitales u otros métodos seguros. * ¿Existen restricciones sobre los usuarios o roles que tienen permitido emitir comandos remotos? * ¿Los comandos remotos requieren la aprobación o autorización previa antes de su ejecución? * Examine la configuración de autenticación de los sistemas y las herramientas de acceso remoto para identificar el uso de claves SSH, certificados digitales u otros métodos seguros. * ¿La organización tiene un proceso establecido para revisar, mejorar los procesos y mecanismos de acceso remoto? * Verifique si las recomendaciones identificadas en auditorías anteriores se han implementado y documentado de manera adecuada. * ¿Se establecen indicadores clave de rendimiento (KPIs) para medir la efectividad de las mejoras implementadas en los procesos de acceso remoto? * Porcentaje de Cumplimiento de Recomendaciones. * Tasa de Incidentes de Acceso No Autorizado. * Tiempo de Respuesta a Incidentes Relacionados con Acceso Remoto. * Nivel de Satisfacción del Usuario. * Rendimiento de la Red en Conexiones Remotas. * ¿Existe un ciclo de retroalimentación en el que los resultados de las mejoras implementadas se evalúan y se utilizan para informar futuras decisiones de mejora? |