

**10 – Notificaciones y Bloqueo de Sesión**

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

**Preguntas de Auditoría**

**Notificaciones y Bloqueos de Sesión**

|  |
| --- |
| **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

Para proteger el acceso y el uso autorizado de sistemas, el manejo de notificaciones y bloqueos de sesión en sistemas de información críticos incluye controles rigurosos sobre las sesiones y el acceso de usuarios. Se establecen procedimientos de inicio de sesión seguros, que minimizan el riesgo de acceso no autorizado mediante la ocultación de información sensible y la validación completa de credenciales antes de conceder acceso. Las medidas incluyen advertencias de uso, límites de intentos de inicio de sesión, bloqueo temporal y notificaciones al usuario, como el último inicio de sesión y alertas de intentos fallidos. Estos elementos aseguran la transparencia y seguridad en los accesos, proporcionando retroalimentación al usuario sobre el estado de su sesión y acciones sospechosas.

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

El control de acceso se apoya en procedimientos documentados y notificaciones específicas de seguridad y privacidad, mostrando términos y condiciones que establecen los usos autorizados del sistema. Estos mensajes de bienvenida, advertencias de monitoreo y recordatorios de seguridad mejoran la concientización de los usuarios sobre el uso adecuado del sistema, mientras que las acciones como el cierre de sesión automático en condiciones de inactividad protegen el sistema ante accesos no autorizados.

**1.2 Perspectiva de Auditoría en el Control de Sesiones**

La auditoría del control de sesiones y acceso remoto en SIC verifica la implementación de políticas de seguridad en el inicio y cierre de sesión, así como en el manejo de errores y bloqueos. La auditoría revisa los mecanismos de autenticación, monitoreo de intentos fallidos y notificaciones al usuario, asegurando que todas las medidas establecidas se mantengan en línea con los objetivos de seguridad de la organización y cumplan con las normativas aplicables.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. El procedimiento para iniciar sesión en un sistema o aplicación debe estar diseñado para minimizar el riesgo de acceso no autorizado. Se debe tener en cuenta lo siguiente:  1.1 No mostrar información confidencial del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado con éxito para evitar proporcionar asistencia innecesaria a un usuario no autorizado.  1.2 Mostrar un aviso general advirtiendo que el sistema o la aplicación o el servicio solo deben ser accedidos por usuarios autorizados.  1.3 No proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que ayuden a un usuario no autorizado (por ejemplo, si surge una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta).  1.4 Validar la información de inicio de sesión solo al completar todos los datos de entrada.  1.5 Protección contra intentos de inicio de sesión de fuerza bruta en nombres de usuario y contraseñas, requerir el restablecimiento de la contraseña después de un número predefinido de intentos fallidos o bloquear al usuario después de un número máximo de errores].  1.6 Registrar intentos fallidos y exitosos.  1.7 Generar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de inicio de sesión (p. ej., enviar una alerta al usuario y a los administradores del sistema de la organización cuando se alcanza un determinado número de intentos de contraseña incorrectas).  1.8 No mostrar una contraseña en texto claro cuando se está introduciendo; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión del usuario (por ejemplo, por razones de accesibilidad o para evitar el bloqueo de usuarios debido a errores repetidos).  1.9 No transmitir contraseñas en texto claro a través de una red para evitar ser capturado por un programa "sniffer" de la red.  1.10 Finalizar sesiones inactivas después de un período definido de inactividad, especialmente en lugares de alto riesgo, como áreas públicas o externas fuera de la gestión de seguridad de la organización o en los dispositivos de punto final del usuario. . 1.11 Restringir los tiempos de duración de la conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.   2. Limitar el número de sesiones simultáneas para cada cuenta y/o tipo de cuenta a un número definido por la organización.  3. Hacer cumplir un límite de número de intentos consecutivos de inicio de sesión no válidos por parte de un usuario durante en un período de tiempo definido por la organización.  4. Permitir, tras alcanzar el límite de intentos fallidos de inicio de sesión, el uso de factores de autenticación alternativos:  4.1 Permitir el uso de factores de autenticación definidos por la organización que son diferentes de los factores de autenticación principales después de que se haya superado el número de intentos de inicio de sesión no válidos consecutivos definidos por la organización.  4.2 Hacer cumplir un límite de intentos de inicio de sesión no válidos consecutivos mediante el uso de factores alternativos por parte de un usuario durante un período de tiempo definido por la organización.  5. Tras alcanzar el límite de intentos consecutivos de inicio de sesión fallidos bloquear la cuenta o el nodo automáticamente. Se deben tomar las siguientes medidas:   5.1 Bloquear la cuenta o el nodo hasta que un administrador lo libere.  5.2 Retrasar el próximo inicio de sesión según algoritmo de retraso definido por la organización.  5.3 Notificar al administrador del sistema  5.4 Realizar cualquier otra acción definida por la organización cuando se exceda el número máximo de intentos fallidos.  6.Mantener el bloqueo del dispositivo hasta que el usuario restablezca el acceso utilizando los procedimientos de identificación y autenticación establecidos.  7. Finalizar automáticamente una sesión de usuario después de algún evento desencadenante que requieren la desconexión de la sesión u otro evento definido por la organización.  8. Proporcione una capacidad de cierre de sesión para las sesiones de comunicaciones iniciadas por el usuario siempre que se utilice la autenticación para obtener acceso a recursos de información definidos por la organización. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Documentar y formalizar los requisitos, procedimientos y controles de inicio y cierre de sesión.   2. Mostrar, y retener hasta que el usuario reconozca los términos y condiciones, los mensaje de notificación o banner de uso del sistema definido por la organización a los usuarios antes de otorgarles acceso al sistema que proporcione avisos de privacidad y seguridad consistente con las leyes, órdenes ejecutivas, directivas, reglamentos, políticas, estándares y lineamientos aplicables y establecer que:  2.1. El uso del sistema puede ser monitoreado, registrado y sujeto a auditoría.  2.2. El uso no autorizado del sistema está prohibido y sujeto a sanciones penales y civiles.  2.3. El uso del sistema indica consentimiento para el monitoreo y registro.  3. Mostrar, y retener hasta que el usuario reconozca los términos y condiciones, para sistemas de acceso público:  3.1. Información de uso del sistema, condiciones definidas por la organización, antes de otorgar más acceso al sistema de acceso público.  3.2. Referencias, si las hubiera, al monitoreo, registro o auditoría que sean consistentes con las adaptaciones de privacidad para tales sistemas que generalmente prohíben esas actividades.  3.3. Descripción de los usos autorizados del sistema.   4. Notificar al usuario:  4.1 al iniciar sesión con éxito en el sistema, la fecha y hora del último inicio de sesión.  4.2 luego de un inicio de sesión exitoso, la cantidad de intentos de inicio de sesión fallidos desde el último inicio de sesión exitoso.  4.3 al iniciar sesión correctamente, el número de inicios de sesión exitosos e intentos fallidos de inicio de sesión, ambos durante un período de tiempo definido.  4.4 luego de un inicio de sesión exitoso, de los cambios en características o parámetros relacionados con la seguridad de la cuenta del usuario.   5. Mostrar un mensaje explícito a los usuarios indicando que la sesión finalizará en un tiempo definido de inactividad.  6. Mostrar un mensaje de cierre de sesión explícito a los usuarios que indique la finalización de las sesiones de comunicaciones autenticadas. |
| 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 las Notificaciones y los Bloqueos de Sesión

|  |
| --- |
| 3.1 Temática: Avisos y notificaciones a los usuarios. |
| El objetivo de estas pruebas de auditoría implica revisar y evaluar cómo una organización comunica información relevante a sus usuarios en relación con la seguridad de la información y el uso de sistemas y recursos tecnológicos, centrándose en verificar si la organización está proporcionando información clara, oportuna y adecuada a los usuarios para mantenerlos informados sobre cuestiones de seguridad y cambios en los sistemas. Además, se examina si la organización ha establecido procedimientos para enviar avisos y notificaciones importantes a los usuarios, como actualizaciones de seguridad, cambios en las políticas, incidentes de seguridad o cambios en el acceso a los recursos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Los usuarios son notificados claramente cuando intentan iniciar una sesión que excedería el límite de sesiones simultáneas? * ¿Los usuarios son notificados cuando su dispositivo ha sido bloqueado debido a intentos fallidos de acceso? * ¿Se proporcionan instrucciones claras sobre cómo restablecer el acceso a través de los procedimientos de identificación y autenticación? * ¿Existen mensajes de notificación o banners que se muestren a los usuarios antes de otorgarles acceso al sistema? * ¿Los mensajes de notificación contienen información relacionada con la privacidad y seguridad? * ¿Los mensajes de notificación abordan temas como políticas de privacidad, términos de uso y advertencias de seguridad? * ¿Se proporciona información suficiente y clara en los mensajes sobre las políticas y regulaciones aplicables? * ¿Los mensajes de notificación o banners permanecen visibles en la pantalla el tiempo suficiente para que los usuarios puedan leer y entender su contenido? * ¿Se ha establecido un período específico durante el cual los mensajes deben permanecer en la pantalla? * ¿Los usuarios deben llevar a cabo una acción explícita, como hacer clic en un botón de "Aceptar” o “Entiendo”, ¿para que el mensaje desaparezca y puedan acceder al sistema? * ¿Se ha implementado una acción que demuestre que los usuarios han reconocido las condiciones y políticas antes de continuar? * ¿Después de iniciar sesión exitosamente, se proporciona información adicional a los usuarios según lo definido por la organización? * ¿Las notificaciones son claras, comprensibles y relevantes para los usuarios? * ¿Se siguen las pautas de diseño y comunicación para garantizar que las notificaciones sean efectivas? * ¿Se muestra a los usuarios un mensaje explícito cuando cierran sesión, indicando claramente que su sesión de comunicaciones autenticadas ha finalizado? * ¿El mensaje de cierre de sesión es fácilmente visible y comprendido por los usuarios? * ¿Se muestra a los usuarios un mensaje explícito antes de que su sesión finalice en un tiempo definido por la organización? * ¿El mensaje indica claramente cuánto tiempo queda hasta el cierre de sesión y qué ocurrirá cuando finalice? * ¿El sistema notifica automáticamente a un administrador cuando se bloquea una cuenta o nodo debido a intentos fallidos? * ¿Las notificaciones incluyen información relevante y suficiente para tomar medidas apropiadas? |

|  |
| --- |
| **3.2 Finalización de sesiones y el bloqueo de dispositivos** |
| La ejecución de estas pruebas de auditoría tiene por objetivo revisar y evaluar cómo una organización administra y garantiza la terminación de las sesiones de usuarios en sistemas y dispositivos según ciertos parámetros, así como la implementación de medidas de seguridad para bloquear dispositivos cuando no están en uso. En este sentido, se verifica si la organización tiene políticas y procedimientos establecidos para asegurarse de que las sesiones de usuarios en sistemas y aplicaciones se cierren cuando los usuarios finalizan su trabajo o abandonan sus dispositivos. Asimismo, se evalúa si la organización implementa medidas para bloquear automáticamente dispositivos, como computadoras y dispositivos móviles, cuando no se utilizan durante un período de tiempo específico, con el fin de prevenir el acceso no autorizado por parte de otros usuarios.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha establecido un límite definido por la organización para el número máximo de sesiones simultáneas que una cuenta puede tener? * ¿El límite se basa en políticas y consideraciones de seguridad de la organización? * ¿El límite de sesiones simultáneas varía según el tipo de cuenta o roles definidos por la organización? * ¿Los diferentes tipos de cuentas tienen límites específicos establecidos? * ¿El sistema está configurado para monitorear y aplicar automáticamente el límite de sesiones simultáneas por cuenta? * ¿Se utiliza tecnología adecuada para rastrear y controlar la cantidad de sesiones activas por cuenta? * ¿El sistema bloquea automáticamente una cuenta o nodo después de un número definido por la organización de intentos fallidos de inicio de sesión? * ¿El bloqueo se activa automáticamente sin intervención manual? * ¿El sistema bloquea la cuenta o el nodo durante un período de tiempo definido por la organización después de intentos fallidos? * ¿La duración del bloqueo es razonable y basada en políticas de seguridad? * ¿Existe la capacidad de bloquear una cuenta o nodo hasta que un administrador autorizado lo libere manualmente? * ¿El proceso de liberación se lleva a cabo mediante procedimientos de autenticación seguros? * ¿El dispositivo permanece bloqueado durante un período de tiempo definido por la organización después de cierto número de intentos de acceso fallidos? * ¿El tiempo de bloqueo se basa en consideraciones de seguridad y protección de la cuenta? * ¿Los usuarios deben seguir los procedimientos de identificación y autenticación establecidos para restablecer el acceso después de un bloqueo? * ¿Se utiliza un proceso seguro y confiable para verificar la identidad del usuario antes de restablecer el acceso? * ¿La organización ha establecido un período de tiempo definido de inactividad después del cual se activa automáticamente el bloqueo del dispositivo? * ¿El período de inactividad está en línea con las políticas de seguridad y la naturaleza de la información manejada? * ¿El sistema bloquea automáticamente el dispositivo después de que haya transcurrido el período de inactividad definido? * ¿El bloqueo se activa sin intervención del usuario después de la inactividad? * ¿Los usuarios deben autenticarse nuevamente después del bloqueo por inactividad para acceder al sistema? * ¿El acceso se protege con métodos de autenticación apropiados después del bloqueo? |