

**1- Políticas de Control de Acceso e Identidad**



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

**Preguntas de Auditoría**

**Políticas de Control de Acceso e Identidades**

|  |
| --- |
| **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

Las Políticas de Control de Acceso e Identidad representan un componente vital en la estrategia de seguridad de la información de cualquier organización. Estas políticas definen las reglas y procedimientos que rigen quién tiene acceso a los sistemas, datos y recursos de la organización, así como se gestiona y protege la identidad digital de los usuarios. La implementación efectiva de estas políticas contribuye a salvaguardar la confidencialidad, integridad y disponibilidad de los activos críticos.

La gestión de identidades y accesos principalmente controla el acceso a los activos de información y gestiona las identidades, estos activos incluyen computadoras, equipos, redes, aplicaciones, usuarios que pueden extenderse más allá de los empleados corporativos. Por ejemplo, pueden incluir proveedores, clientes, máquinas, cuentas de administrador genéricas y credenciales electrónicas de acceso físico. IAM (Identity and Access Management) es una función crítica de seguridad que permite a las organizaciones no solo responder a los cambios, sino ser más proactivas y anticiparse a los riesgos de accesos relacionados a la identidad que se producen como resultado de un entorno organizacional dinámico.

**1.1 Lineamientos generales del control de Acceso e Identidad**

Los lineamientos generales de los procesos IAM implica establecer un conjunto de directrices y normas que rigen cómo se gestionan y protegen los accesos a sistemas, datos y recursos dentro de una organización. Estos lineamientos proporcionan un enfoque estructurado para garantizar que solo las personas autorizadas tengan acceso a la información y los activos críticos de la organización, al tiempo que se protege la privacidad y la integridad de la información.

1. Establecer políticas de control de acceso e identidad necesarios en base a los requisitos de seguridad de la información y de los objetivos propios de la Organización.
2. Definir, implementar y monitorear controles de identidad y acceso adecuados para proteger la información y/o las instalaciones.
3. Otorgar acceso a los recursos de información, servicios y recursos tecnológicos proporcionados por la organización únicamente a aquellos usuarios que estén autorizados de acuerdo con el objeto de sus funciones y responsabilidades, y verificar los privilegios otorgados a los recursos.
4. Analizar y realizar un seguimiento continuo y permanente de las medidas de control de acceso e identidad desplegadas y verificar su eficiencia y eficacia.
5. La asignación del privilegio mínimo debe ser frente a los activos de la organización. Se les debe otorgar el tiempo necesario para llevar a cabo las actividades propias de sus funciones y roles definidos.
6. Mantener registros de las actividades relacionadas con el acceso e identidad de los activos de la organización, realizar auditorías continuas para verificar el cumplimiento de los lineamientos y la efectiva ejecución de los procedimientos.

**1.2 Política del proceso IAM**

La política del Control de Acceso e Identidad definen las reglas y controles, así como las restricciones de acceso a la información. Es necesario que la política tenga a consideración lo siguiente:

* La necesidad de documentar y revisar periódicamente la política de control de acceso, lo que indica que una política documentada es obligatoria.
* La Dirección debe determinar estas políticas de control de acceso e identidad de acuerdo con las normas de seguridad de la información y los análisis de riesgos y amenazas.
* Una buena práctica que se puede observar incluso desde al nivel de la política de control de acceso es: “todo está prohibido a menos que esté permitido”.

Se debe considerar los siguientes principios generales al momento de implementar controles y definir restricciones.

* **Responsabilidades de la Seguridad y Privacidad de la Información:** El empleado responsable estará a cargo de definir normas y procedimientos para la gestión de accesos e identidad a todos los activos de información.
* **Responsabilidades de los activos de información:** Los propietarios de los activos de información deben determinar las normas de control de acceso e identidad y la asignación de los privilegios, de acuerdo con la política y los análisis de riesgos.
* **Responsabilidades del usuario**: Los usuarios que hacen uso de los activos de información de la organización son responsables de las acciones, realizadas sobre los mismos, así como de las credenciales de acceso, mantener a salvo sus contraseñas o información de autenticación que le sean asignadas para su uso.
* **Gestión de acceso a los usuarios:** Se trata de un requisito para gestionar la autorización de los usuarios que acceden a los recursos de la organización como sistemas, redes, datos, tecnología y servicios. La Entidad debe implementar controles y procedimientos formales con el objetivo de impedir el acceso no autorizado a la información.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Designar un funcionario para gestionar el desarrollo, la documentación y la difusión de la política y los procedimientos de control de acceso.  2. Desarrollar, documentar y difundir al personal:  2.1. La política de control de acceso, identificación y autenticación que:  2.1.1 aborde el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la dirección, la coordinación entre las entidades de la organización y el cumplimiento.  2.1.2 sea coherente con las leyes aplicables, órdenes ejecutivas, directivas, reglamentos, políticas, normas y directrices.  2.2. Los procedimientos para facilitar la implementación de la política de control de acceso, identificación y autenticación y los controles de identificación, autenticación y acceso asociados.  3. Definir una política específica de tema sobre el control de acceso. Estos requisitos y la política específica del tema deben considerar lo siguiente:  3.1. Definir cómo comunicar la creación, eliminación y cambio de identidades de usuario.  3.2. Establecer una ubicación o departamento centralizado, separado de TI, para iniciar las comunicaciones de identidad a TI. . 3.3 Determinar qué entidades requieren qué tipo de acceso a la información y otros activos asociados.  3.3.1 Aplicar una política de control de acceso basada en roles sobre sujetos y objetos definidos  3.3.2 Controlar el acceso en función de roles definidos por la organización y usuarios autorizados para asumir dichos roles  3.4 Seguridad de las aplicaciones.  3.5 Acceso físico, que debe estar respaldado por controles de entrada físicos apropiados.  3.6 Diseminación y autorización de la información (p. ej., el principio de necesidad de saber) y niveles de seguridad de la información y clasificación de la información.  3.7 Restricciones al acceso privilegiado.  3.8 Legislación, reglamentos y obligaciones contractuales pertinentes con respecto a la limitación del acceso a datos o servicios.  4. Considerar los tipos de identidad dentro de la política de identidad y control de acceso. Estos incluyen, entre otros, cualquiera o todos los siguientes:  4.1 Empleados que utilizan recursos de TI.  4.2 Proveedores (p. ej., subcontratistas).  4.3 Dispositivos de TI (p. ej., dispositivos de hardware que realizan funciones similares a las de un usuario, como aplicaciones fijas y móviles).  4.4 Cuentas de servicio de aplicaciones (p. ej., cuentas predefinidas proporcionadas por el proveedor de software).  4.5 Cuentas de máquinas (p. ej., dispositivos de hardware de TI que realizan funciones dentro y entre entornos o aplicaciones de TI, como una máquina de piso).  4.6 Cuentas funcionales o por lotes (p. ej., las que se utilizan para ejecutar procesos por lotes, como la generación de lotes de informes nocturnos).  5. Los procesos utilizados en el contexto de la gestión de la identidad deben garantizar que:  5.1 Para las identidades asignadas a personas, una identidad específica solo este vinculada a una única persona, para poder responsabilizar a la persona por las acciones realizadas con esta identidad específica.  5.2 Las identidades asignadas a múltiples personas (por ejemplo, identidades compartidas) solo se permiten cuando son necesarias por razones empresariales u operativas y están sujetas a aprobación y documentación específicas.  5.3 Las identidades asignadas a entidades no humanas están sujetas a una aprobación debidamente segregada y a una supervisión continua independiente.  5.4 Las identidades se inhabilitan o eliminan de manera oportuna si ya no son necesarias (por ejemplo, si sus entidades asociadas se eliminan o ya no se utilizan, o si la persona vinculada a una identidad ha abandonado la organización o ha cambiado de función).  5.5 En un dominio específico, una sola identidad se asigna a una sola entidad, [es decir, se evita la asignación de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas)].  5.6 Se mantienen registros de todos los eventos significativos relacionados con el uso y la gestión de las identidades de los usuarios y de la información de autenticación. |
|  |  |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Abordar, dentro del plan de seguridad de los controles de acceso e identidad y autenticación, cómo procederá la organización:  1.1 Con el proceso de IAM  1.2 Los riesgos de IAM presentes y futuros  1.3 Si los procesos de IAM y las actividades relacionadas consistirán en soluciones manuales o electrónicas  1.3 Si todas las áreas de la organización serán incorporadas en el proceso de IAM,    2. Aplicar la política de control de acceso sobre el conjunto de sujetos y objetos cubiertos especificados en la política, y cuando la política:  2.1 Se aplica de manera uniforme en todos los sujetos y objetos cubiertos dentro del sistema.  2.2 Especifica que un sujeto al que se le ha concedido acceso a la información no puede realizar  ninguna de las siguientes acciones.  2.2.1 Pasar la información a sujetos u objetos no autorizados.  2.2.2 Conceder sus privilegios a otros sujetos.  2.2.3 Cambiar uno o más atributos de seguridad especificados por la política en sujetos, objetos, el sistema o componentes del sistema.  2.3 Elegir los atributos de seguridad y los valores de los atributos especificados por la política para asociarlos con objetos recién creados o modificados.  2.4 Cambiar las reglas que rigen el control de acceso.  2.5 Especificar que los sujetos definidos por la organización se puede otorgar explícitamente privilegios definidos por la organización de modo que no estén limitados por ningún subconjunto definido (o todas) de las restricciones anteriores.    3. Hacer cumplir la política de control de acceso discrecional definida por la organización sobre el conjunto de sujetos y objetos cubiertos especificados en la política, y donde la política especifica que un sujeto al que se le ha otorgado acceso a la información puede hacer una o más de las siguientes cosas:  3.1 Pasar la información a otros sujetos u objetos.  3.2 Otorgar sus privilegios a otros sujetos.  3.3 Cambiar atributos de seguridad en sujetos, objetos, el sistema o los componentes del  sistema.  3.4 Elegir los atributos de seguridad que se asociarán con los objetos recién creados o revisados.  3.5 Cambiar las reglas que rigen el control de acceso. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Mantener un medio para revisar periódicamente y revisar la declaración de política de IAM para garantizar que refleje los procesos y actividades actuales relevantes.  2. Revisar y actualizar la política de control de acceso, identificación y autenticación actual frecuentemente para ajustarse a los cambios del entorno interno y externo |

# Preguntas de Auditoría para Políticas de control de Acceso e Identidad

|  |
| --- |
| 3.1 Temática: Definición de una política específica del Control de Acceso e Identidad |
| El presente punto establece la revisión, evaluación y verificación de las políticas diseñadas para garantizar y regular un adecuado control de acceso a los sistemas y recursos de la entidad, así como cómo se manejan y protegen las identidades de los usuarios. Estas prácticas se enfocan en garantizar que la política sea coherente y cumpla con los requisitos legales y de seguridad, y se ajuste a las necesidades de la organización. Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La Política establece claramente los siguientes puntos enumerados?   1. Identificación de usuarios.  2. Autenticación de usuarios.  3. Autorización de accesos.  4. Control de accesos basado en roles (RBAC) o atributos (ABAC).  5. Privilegios de acceso en la administración de recursos.  6. Registro y auditoría de accesos.  7. Gestión del ciclo de vida de los accesos.  8. Revisión periódica de accesos.  9. Gestión de usuarios privilegiados.  10. Usuarios de servicio.   * ¿La política de control de acceso e identidad tiene una definición (objetivos y alcance) y su importancia como sistema de gestión de la información en la organización?   + ¿Contiene detalles de un marco de la seguridad de los factores a evaluar y un plan de la gerencia de riesgo?   + ¿Incluye una explicación de las leyes, principios, prácticas y obligaciones de seguridad frente a los requisitos legales, los planes de continuidad del negocio y las consecuencias del incumplimiento? * ¿Existe un proceso de revisión y cambio, incluidas las fechas/horas de revisión de los documentos de política?   + ¿La revisión de la política control de acceso e identidad incluye una evaluación del costo-beneficio de los controles clave existentes y los cambios técnicos propuestos por la organización?   + ¿Describe los pasos y procedimientos para realizar ajustes a la política?   + El procedimiento de gestión de cambios y versiones debe contener: Responsable, versión, fecha y firma. * ¿La política tiene responsables claros, el cual han aceptado sus responsabilidades en la administración y aprobación de ésta, queda registrada en un acta o libro?   + Determine si los roles y responsabilidades de seguridad de la información están definidos.   + Los roles y responsabilidades deben estar definidos por descripciones de trabajo, acuerdos, matriz RACI, cuadros jerárquicos y/o contratos. * ¿El personal encargado de la administración de acceso y cuentas es responsable de administrar, actualizar, mantener y brindar acceso a todas los activos físicos y lógicos?   + ¿Existen documentos donde se evidencia la aceptación de las responsabilidades en el manejo de los activos físicos y lógicos en la organización? * ¿Existe un documento escrito de las políticas disponible para todo trabajador, usuario o personal en la organización?   + ¿Se realizan actividades para aclarar dudas y preocupaciones acerca de la política comunicada a los empleados, para garantizar su comprensión? * ¿Hay una política definida para el proceso de gestión de incidentes?   + ¿Para el manejo de incidentes se detalla los roles y responsabilidades en la identificación y manejo de esos incidentes?   + ¿Se establece en la política el manejo de incidentes la cancelación de los accesos a los sistemas e instalaciones de la organización?   + ¿El proceso de manejo de incidentes incluye una clasificación de los tipos de incidentes y sus respectivos planes de acción en caso de que ocurra?   + Revise contratos y acuerdos de confidencialidad, y nivel de servicio con proveedores para determinar si los controles de incidentes de ciberseguridad se abordan de forma oportuna. * ¿Hay un procedimiento establecido en la organización para desarrollar y mantener la continuidad del negocio en caso de incidentes?   + ¿Se definen y aprueban responsabilidades y órdenes de emergencia? * ¿Los administradores se aseguran de que los contratistas apliquen la seguridad de los acceso y credenciales de acuerdo con las políticas de la organización?   + ¿Cuenta la organización con un programa de seguridad para facilitar el uso eficiente de los recursos y sistemas de la información?   + ¿La política de control de acceso está alineada con la clasificación e inventario de los activos? * La Política comprende y se rige por los requisitos legales y reglamentarios de la ciberseguridad, incluidos la privacidad y legislación vigente.   + Verifique la lista de todos los requisitos legales y reglamentarios para la organización.   + Revise los informes de auditoría reglamentarias recientes. Revise que la excepciones fueron observadas en las auditorías, determine cómo la organización respondió ante estos hechos.   + Determine si los contratos con terceros son revisados por un asesor legal previamente a su ejecución.   + Verifique si existe un proceso formal para monitorear y revisar los cambios en leyes y regulaciones de ciberseguridad. * ¿Está considerado dentro de la política de acceso e identidad la difusión de información? * ¿Hay reportes desarrollados a partir de los indicadores de medición donde se presenta el desempeño de las políticas de acceso e identidad? * ¿En las políticas se define que los usuarios deben tener un identificador único para uso de los sistemas de información y en las aplicaciones?   + ¿La política o procedimientos exigen que los usuarios tengan un identificador único para el acceso a los sistemas y aplicaciones?   + Verifique que el procedimiento y la configuración de los sistemas establecen la imposibilidad de reasignar o reutilizar los identificadores únicos.   + Evalué que la organización revise que las cuentas y credenciales de usuario son personales e intransferibles.   + Verifique que la organización asigne a los empleado, proveedores y contratistas un identificador único para el uso de los sistemas, aplicaciones y recursos, el cual debe ser creado de acuerdo con las normas establecidas en los Procedimientos de Gestión de Accesos. * ¿Se determina los procedimientos y directrices que deben construirse para la gestión de asignaciones de identificadores, su modificación, revisión o eliminación de derechos y/o privilegios de los usuarios creado?   + ¿En la política de control de acceso se considera la segregación de roles, las peticiones de acceso, las revisiones periódicas y la eliminación de derechos de acceso?   + ¿Hay una declaración de las política o norma de acceso que definan los privilegios de acceso de los usuarios o grupos? * ¿Se tiene una declaración o documentación escrita de los privilegios de acceso, ya sea, física o lógica, la cual es leída y firmada por los usuarios para garantizar que entienden las condiciones? * ¿En los procesos de registro de usuarios se garantiza que estos solo accedan a las operaciones autorizadas, se realiza la correcta validación del usuario con su identificador único y contraseña? ¿Hay registros de estos procedimientos? * ¿En los sistemas de información utilizados, se realizarán procesos de validación de la identidad de los usuarios (autenticación)? * ¿Los lineamientos de la política establecen la importancia de la definición de roles, para asegurar un nivel de acceso a la información acorde con el perfil del usuario?   + Debe estar alineados con los permisos y atribuciones requeridos en las matrices de roles definidas en cada proceso.   + Permite la asignación de permisos en base a los requerimientos de la organización.   + ¿Se aplica los principios de menor privilegio y segregación de funciones?   + ¿Existe en la organización perfiles estándares de acceso de usuario para las categorías comunes de trabajo, o que realicen la misma función? * ¿Está documentado y definidos en los lineamientos en cuanto a la calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a recursos de la organización?   + ¿Se establece los parámetros mínimos para que la contraseña sea válida a los funcionarios, contratistas y/o terceros? * ¿La política define los perímetros físicos de seguridad donde se encuentra la información crítica o sensible en los cuales se realice el almacenamiento y/o procesamiento de información? |

|  |
| --- |
| 3.2 Temática: Distribución, documentación y capacitación de la Política de IAM |
| Esta práctica busca asegurar que todas las partes involucradas en la gestión de identidad y acceso estén informadas y conscientes de las políticas y procedimientos de seguridad establecidos. Se evalúa cómo se distribuye la política de seguridad relacionada con el control de Acceso e Identidad dentro de la organización. Esto incluye asegurarse que esté disponible en un formato accesible para todos, como documentos digitales en el sistema interno, y que se haya comunicado su disponibilidad a todo el personal relevante. También se debe verificar si se proporciona capacitación adecuada al personal involucrado en los procesos, incluye administradores de sistemas, responsables de recursos humanos y otros usuarios clave. La capacitación debe abarcar el contenido y los requisitos de la política, así como las mejores prácticas y realizar evaluaciones para medir el nivel de comprensión y si se toman medidas para abordar posibles lagunas.  Es importante que la política de seguridad se mantenga actualizadas garantizando la aprobación y apoyo por parte de la Órgano de Gobierno, es importante verificar si los cambios o actualizaciones se comunican de manera efectiva al personal y a las partes interesadas, esto garantiza que sean relevantes en un entorno en constante evolución.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen programas de capacitación para los empleados y trabajadores, con los cuales se pueda dar a conocer los aspectos más importantes de los procesos IAM? * ¿Todos los usuarios han recibido una adecuada capacitación y entrenamiento de seguridad, ya sea teórico, técnico y de sus responsabilidades? * ¿La capacitación y el entrenamiento incluyen políticas, controles y procedimientos del control de Acceso e identidad, así como el uso correcto de los controles físicos y lógicos del procesamiento de información antes de que se conceda el acceso a instalaciones, sistemas y aplicaciones? * ¿Estas actividades de capacitación y entrenamiento se ejecutan de forma periódica o sisTema para garantizar el aprendizaje continuo? * Entreviste a miembros del equipo involucrados en los procesos IAM para confirmar que han recibido capacitación sobre la política de seguridad y sus implicaciones. * ¿Se ha documentado una política de seguridad específica para los procesos de Identidad y Acceso?   + ¿La política de seguridad se encuentra actualizada y refleja los requisitos y las mejores prácticas actuales? * ¿Se han establecido procedimientos claros para distribuir y comunicar la política de seguridad IAM al personal correspondiente?   + Evalúe registros de comunicación interna o anuncios que respalden la distribución efectiva de la política de seguridad IAM.   + ¿Se mantiene un registro de la distribución de la política, la asistencia a sesiones de capacitación y la comprensión del personal? |