

**07- Acceso Físico**

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

**Preguntas de Auditoría**

**Acceso Físico**

|  |
| --- |
| **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

La gestión de acceso físico en SIC permite proteger áreas críticas mediante controles estructurados y mecanismos de seguridad en puntos de acceso. Este proceso incluye medidas como registros y monitoreo de entrada, controles en áreas de carga y entrega, así como la protección de zonas de procesamiento de información, minimizando así el riesgo de acceso no autorizado. Las políticas de acceso físico requieren que todas las personas que ingresan a áreas sensibles sean identificadas, registradas y, en caso de visitantes, acompañadas en todo momento. Además, el diseño de seguridad considera tanto la visibilidad externa como la discreción de las instalaciones, y se implementan sistemas de videovigilancia y registros de auditoría en puntos de entrada para asegurar una supervisión constante. Estos controles se acompañan de procesos de capacitación continua en concientización sobre seguridad física.

**1.1 Control y Monitoreo de Accesos**

Para asegurar el acceso seguro, la organización establece una lista de personas autorizadas para ingresar a las instalaciones, revisándola periódicamente y asegurando que solo los individuos necesarios posean acceso. Esta lista de acceso es complementada con tecnologías y herramientas anti-manipulación en puntos de acceso clave, como entradas y áreas de carga, lo que asegura la protección de la infraestructura de procesamiento de información. Las credenciales de acceso se emiten y monitorean de manera estricta, con registros de auditoría física y un inventario actualizado de dispositivos de acceso para identificar y asegurar las herramientas y dispositivos en uso.

**1.2 Evaluación desde la Auditoría en la Gestión de Acceso Físico**

La auditoría de SIC verifica la eficacia de los controles de acceso físico mediante métricas cuantitativas como incidentes reportados, evaluaciones de seguridad y registros de dispositivos de salida. Revisiones periódicas de registros y monitoreo en respuesta a eventos ayudan a identificar posibles vulnerabilidades en el control de acceso físico. Además, los resultados de estas evaluaciones se integran en los mecanismos de respuesta a incidentes, optimizando la seguridad y la capacidad de reacción ante intrusiones o riesgos potenciales, logrando una supervisión integral y asegurando la integridad de los activos físicos en la organización.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Proteger las áreas seguras por controles de entrada y puntos de acceso apropiados como vestíbulos de control de acceso, vallas, paredes y dispositivos de seguridad en puertas interiores y exteriores en ubicaciones definidas por la organización dentro de la instalación.  1.1 Registrar y monitorizar todos los puntos de entrada a las instalaciones de TI. Las medidas para el control físico incluyen:  1.2 Registrar a todos los visitantes al sitio, incluidos contratistas y proveedores.  1.2.1 Asegurar que todo el personal muestra una identificación debidamente autorizada en todo momento.  1.2.2 Requerir a los visitantes que estén acompañados en todo momento durante su estancia en las instalaciones.  1.4 Controlar el acceso físico a las líneas de transmisión y distribución del sistema dentro de las instalaciones de la organización utilizando controles de seguridad.  1.5 Controlar el acceso físico a la salida de dispositivos de salida para evitar que personas no autorizadas obtengan la salida.   2. Controlar los puntos de acceso como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a las instalaciones y, si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado. Se deben considerar las siguientes pautas:  2.2 Mantener y monitorear de forma segura un libro de registro físico o un registro de auditoría electrónico de todos los accesos y proteger todos los registros e información confidencial de autenticación.  2.4 Establecer un área de recepción monitoreada por personal u otros medios para controlar el acceso físico al sitio o edificio.  2.5 Inspeccionar y examinar las pertenencias personales del personal y de las partes interesadas a la entrada y salida.  2.6 Exigir que todo el personal y las partes interesadas usen algún tipo de identificación visible y que notifiquen de inmediato al personal de seguridad si encuentran visitantes sin escolta o cualquier persona que no use una identificación visible. Se deben considerar insignias fácilmente distinguibles para identificar mejor a los empleados permanentes, proveedores y visitantes.  2.7 Otorgar acceso restringido al personal del proveedor a áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario. Este acceso debe ser autorizado y monitoreado.  2.8 Prestar especial atención a la seguridad del acceso físico en el caso de edificios que contengan activos para múltiples organizaciones.  2.9 Diseñar medidas de seguridad física para que puedan reforzarse cuando aumente la probabilidad de incidentes físicos.  2.10 Proteger otros puntos de entrada, como salidas de emergencia, del acceso no autorizado.   2.11 Establecer un proceso de gestión de claves para garantizar la gestión de las claves físicas o la información de autenticación como códigos de bloqueo, cerraduras de combinación para oficinas, salas e instalaciones, como armarios de llaves para así garantizar un libro de registro o una auditoría anual de claves y que se controla el acceso a claves físicas o la información de autenticación.   3. Diseñar e implementar la seguridad física para la zonas de entrega y carga y entrada de material se deben considerar las siguientes pautas:  3.1 Restringir el acceso a las áreas de entrega y carga desde el exterior del edificio al personal identificado y autorizado.  3.2 Diseñar las áreas de entrega y cargas para que las entregas puedan cargarse y descargarse sin que el personal de entrega obtenga acceso no autorizado a otras partes del edificio.  3.3 Asegurar las puertas externas de las áreas de entrega y carga cuando se abren las puertas de las áreas restringidas.  3.4 Inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de que se muevan de las áreas de entrega y carga.  3.5 Registrar las entregas entrantes de acuerdo con los procedimientos de gestión de activos al ingresar al sitio.  3.6 Separar físicamente los envíos entrantes y salientes, cuando sea posible;  3.7 Inspeccionar las entregas entrantes en busca de evidencia de manipulación en el camino. Si se descubre una manipulación, se debe informar de inmediato al personal de seguridad.   4. Diseñar e implementar la seguridad física para las oficinas, salas e instalaciones. Se deben considerar las siguientes pautas:  4.1 Ubicar las instalaciones críticas para evitar el acceso del público.  4.2 Cuando corresponda, asegurarse de que los edificios sean discretos y den una indicación mínima de su propósito, sin señales evidentes, fuera o dentro del edificio, que identifiquen la presencia de actividades de procesamiento de información.  4.3 Configurar instalaciones para evitar que la información o actividades confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también debe considerarse apropiado.  4.4 No poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifiquen ubicaciones de instalaciones de procesamiento de información confidencial.   5. Emplear guardias para controlar los puntos de acceso físicos a la instalación donde reside el sistema las 24 horas del día, los 7 días de la semana. Incluir alarmas de intrusión física en instalaciones donde reside el sistema.  6. Monitorear el acceso físico con videovigilancia:  6.1 Emplear videovigilancia de áreas operativas.  6.2 Revisar grabaciones de video frecuentemente.  6.3 Conservar las grabaciones de video. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Gestionar y proteger el acceso físico a los activos a través de un proceso documentado que define:   1.1 El proceso para gestionar solicitudes para permitir el acceso debidamente autorizado a las instalaciones de cómputo.  1.2 Desarrollar, aprobar y mantener una lista de personas con acceso autorizado a las instalaciones donde reside el sistema.   1.3 Emitir credenciales de autorización para el acceso a las instalaciones.  1.4 La frecuencia para revisar la lista de acceso que detalla el acceso autorizado a las instalaciones por parte de los individuos para garantizar que los perfiles de acceso permanezcan actualizados.   1.5 Eliminar a las personas de la lista de acceso a las instalaciones cuando ya no se requiera el acceso.  1.6 Autorizar el acceso físico a las instalaciones donde reside el sistema según el puesto, cargo y la función.  1.7 Vincular la identidad individual a la recepción de la salida de los dispositivos de salida.   1.8 Levantar Inventario de los dispositivos de acceso físico.  1.9 Mantener registros de los componentes del sistema.  1.9.1 Autorizar y controlar los tipos de componentes del sistema que entran y salen de la instalación.  2. Realizar formación sobre concienciación de la seguridad de la información física de forma regular |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Cambiar combinaciones y llaves con una frecuencia definida por la organización y/o cuando las llaves se pierden, las combinaciones se ven comprometidas, o cuando las personas que poseen las llaves o combinaciones son transferidas o cesado.  2. Emplear tecnologías anti-manipulación para detectar o prevenir manipulación física o alteración de los componentes de hardware dentro del sistema.  3. Realizar controles de seguridad frecuentemente en el perímetro físico de las instalaciones o el sistema para la exfiltración de información o la eliminación de componentes del sistema.   4. Revisar los registros de acceso físico frecuentemente y ante la ocurrencia de eventos definidos por la organización o indicaciones potenciales de eventos. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Mantener registros de auditoría de acceso físico para los puntos de entrada o salida.  2. Establecer un sistema de indicadores cuantitativos con métricas específicas para medir la efectividad de los controles implementados. Algunas métricas sugeridas pueden ser:  - Calificación promedio de las evaluaciones de seguridad física.  - Número de incidentes relacionados con la seguridad de la información física.  - Número de dispositivos de salida robados.  - Porcentaje de documentos sensibles y dispositivos de salida identificados en el inventario.  3. Coordinar los resultados de las revisiones e investigaciones con la capacidad de respuesta a incidentes de la organización. Reconocer las clases o tipos de intrusiones e iniciar acciones de respuesta utilizando mecanismos automatizados. |

# Preguntas de Auditoría para el Acceso Físico

|  |
| --- |
| 3.1 Temática: Evaluar la gestión y credenciales del Acceso Físico |
| Estas prácticas son esenciales para prevenir el acceso no autorizado a áreas sensibles, salvaguardar activos valiosos y garantizar la integridad de las operaciones. En primer lugar, se debe enfocar en el desarrollo, aprobación y mantenimiento de una lista precisa de personas con acceso autorizado a las instalaciones. Esto implica una gestión cuidadosa de quiénes tienen permiso para acceder físicamente a los activos. Las organizaciones deben asegurarse de que las credenciales emitidas sean seguras y únicas para cada individuo autorizado. Estas credenciales no solo permiten el acceso, sino que también ayudan a rastrear quién ha ingresado a las instalaciones y cuándo.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización mantiene un registro actualizado de las personas con acceso físico autorizado a los activos? * Revise la información con la lista de empleados y contratistas para asegurarse de que esté completa y precisa. * ¿Se emiten credenciales de acceso físico únicas y seguras para cada individuo autorizado? * Verifique si incluyen características de seguridad, como códigos de barras, tecnología RFID, Geometría de la mano, Voz, Iris del ojo, Escritura o Huellas Dactilares. * ¿Se establece un proceso para otorgar acceso restringido a áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario? * Revise que cada credencial esté asociada con una persona específica. * ¿Se realiza la revisión de la lista de acceso según la frecuencia establecida en las políticas? * ¿Existe un proceso establecido para mantener actualizados los perfiles de acceso a sistemas y recursos? * Revise los registros de cambios en perfiles de acceso y verificar si se documentan las fechas y las razones de las actualizaciones. * Revise el inventario de credenciales y acceso físico. * ¿La organización realiza el inventario y señaliza las áreas seguras de acuerdo con el inventario establecido? * Revise los registros de acceso físico para identificar patrones o actividades inusuales. * ¿La organización tiene un proceso formal establecido para desarrollar, aprobar y eliminar la lista de personas con acceso autorizado a las instalaciones? * ¿La organización realiza revisiones periódicas de la lista de acceso físico para mantenerla actualizada? * ¿Se establece un procedimiento formal de revisión periódica de los accesos al centro de datos? * Verifique si la información del sistema de control de acceso contempla: registros de ingresos al centro de datos, personal con acceso permanente y personal con acceso temporal. * Verifique si se ha eliminado a personas que ya no requieren acceso y si se han agregado nuevas personas con autorización. * ¿Se realiza la deshabilitación o modificación de manera inmediata de los privilegios de acceso físico en la entidad y a las áreas seguras, en los eventos de desvinculación o ausencia transitoria? * ¿Las personas que ya no necesitan acceso son eliminadas de la lista de acceso de manera oportuna? * ¿Se notifica a las personas cuando se las elimina de la lista de acceso? * ¿Se mantiene un registro histórico de las personas eliminadas de la lista de acceso? * ¿La lista de acceso incluye detalles sobre las personas autorizadas, su puesto o función, y las áreas específicas a las que tienen acceso? * Examine los registros de acceso para verificar si se documentan los nombres de las personas autorizadas, sus puestos o funciones, así como las fechas de autorización y el encargado que autorizo el acceso. * Verifique si las autorizaciones de acceso físico cuentan con la aprobación de la administración o personal autorizado, como los supervisores o gerentes de departamento. * ¿Las autorizaciones de acceso físico se otorgan de acuerdo con los principios de "necesidad de conocer" y "menor privilegio"? * ¿La organización tiene un proceso formal para emitir credenciales de autorización para el acceso a las instalaciones? * Verifique si se describe el flujo de trabajo y las responsabilidades de las partes involucradas. * Verifique si las credenciales de acceso físico, como tarjetas de identificación, están emitidas de manera apropiada y siguen los procedimientos establecidos. * Evalúe el proceso de emisión de credenciales para verificar si se lleva a cabo un proceso de verificación de identidad, como la presentación de documentos de identificación válidos como Carnet de Identidad, Contrato vigente, etc. * ¿La organización ha establecido una lista definida de formas de identificación aceptables para los visitantes y empleados que desean acceder a las instalaciones donde reside el sistema? * ¿Se exige que el personal y las partes interesadas usen identificación visible? * ¿Se utiliza un documento especial, emitido por una autoridad calificada, que acredita la identidad como las Tarjeta de Identificación de Empresa (TIE)? * Verifique los Controles a Contratistas en la Entidad, para la evaluación, el auditor debe tener en consideración: * Identificación con Cédula de Identidad. * Verificación con nómina autorizada. * Tarjeta de Acceso para Contratista o Tarjeta de Identificación de Contratistas. * Verificación de actividades. * Registro en un libro de novedades. * Declaración de herramientas e inventarios. * ¿Para los visitantes cuales son los procedimientos de seguridad? * Identificación con la cédula de identidad. * Autorización de acceso al jefe de Área. Credencial de pase. * Formulario de acceso con antecedentes de interés. * ¿La organización en la Fase de registros ocupa métodos actualizados? Para la evaluación, el auditor debe tener en consideración: * Registro en base de datos computarizada. * Registro cuantitativo de ingresos y salidas: molinete con numeral. * Registro con respaldo fotográfico u otro. |

|  |
| --- |
| **3.2 Temática: Monitoreo, registros y mecanismos para el Acceso Físico** |
| La práctica consiste en evaluar rigurosamente las medidas implementadas por la organización para controlar y supervisar el acceso a sus instalaciones y recursos físicos, el objetivo es garantizar la seguridad, integridad y confidencialidad de los activos físicos, así como prevenir el acceso no autorizado a áreas sensibles o críticas. Se analiza la efectividad de los sistemas utilizados para controlar el acceso físico, como tarjetas de identificación, códigos de acceso o sistemas biométricos, para verificar si estos sistemas son seguros, confiables y si se mantienen actualizados.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización emplea sistemas de videovigilancia en áreas operativas específicas? * Revise los lugares físicos donde se ubican las cámaras de videovigilancia y verificar si están instaladas en las áreas operativas definidas por la organización. * ¿La organización ha establecido una frecuencia definida para revisar las grabaciones de video de la videovigilancia? * ¿La organización conserva las grabaciones de video durante un período de tiempo definido? * Verifique que el perímetro de seguridad de las áreas seguras debe contar con vigilancia   mediante CCTV, contar con sistemas de control de acceso y monitoreado por el personal de vigilancia.   * ¿Los puntos de acceso a las instalaciones tienen un área de recepción con vigilancia y medios para controlar el acceso físico (Personal interno, externo o visitantes) a las instalaciones? ¿Está todo debidamente documentado? * ¿Las áreas operativas con videovigilancia están claramente señalizadas? * ¿Existe un sistema de supervisión establecido para controlar y registrar el acceso físico a las instalaciones donde reside el sistema? * Revise los registros de acceso físico a las instalaciones para verificar si se registran entradas y salidas, incluyendo el nombre del individuo, la hora y la ubicación. * ¿Se establecen alertas o notificaciones para eventos de acceso no autorizado o inusual a las instalaciones? * ¿El personal está capacitado en la detección y respuesta a incidentes de seguridad relacionados con el acceso físico? * ¿Existen alarmas de intrusión física instaladas en las instalaciones donde reside el sistema? * Realice pruebas de funcionamiento en un conjunto de alarmas de intrusión para verificar si se activan correctamente y generan alertas. * ¿Se implementa una supervisión efectiva del acceso físico al sistema y las instalaciones definidas por la organización? * ¿Existe un sistema de registro de acceso físico al sistema y a las instalaciones? * ¿Se realizan revisiones regulares de los registros de acceso físico para identificar actividades sospechosas o no autorizadas? * ¿Existe un procedimiento o política establecida para controlar el acceso físico a la salida de dispositivos de salida definidos por la organización? * Solicite al personal responsable que describa el procedimiento de control de acceso a la salida de dispositivos de salida y cómo se implementa. * ¿La organización establece y documenta los planos de áreas críticas? * ¿Los dispositivos de salida definidos por la organización están claramente identificados? * ¿Existen medidas para prevenir la remoción no autorizada de los dispositivos de salida? * ¿Existe un mecanismo implementado para vincular de manera efectiva la identidad de cada individuo con la recepción de la salida de un dispositivo? * ¿Qué tecnologías o métodos se utilizan para vincular la identidad individual con la recepción de la salida del dispositivo? * ¿Los individuos deben autenticarse de manera única para recibir la salida del dispositivo? * ¿La organización registra en una bitácora o sistema de información el ingreso y retiro de todo equipo, servidores, equipos activos de red o smartphone/celular? * ¿Se lleva un registro de cuándo se han cambiado las combinaciones y las llaves, y cuáles son los motivos de los cambios? * ¿Existe un procedimiento definido para cambiar las combinaciones y llaves cuando se pierden o comprometen? * ¿Las áreas seguras cuentan con controles de entrada y puntos de acceso apropiados, como vestíbulos de control de acceso, vallas y dispositivos de seguridad en puertas? * Realice un recorrido físico por las instalaciones y verificar la presencia de dispositivos de seguridad en las áreas seguras, como vallas, puertas con cerraduras y sistemas de control de acceso. * ¿Se registran y monitorizan todos los puntos de entrada a las instalaciones de TI? * ¿Se registra a todos los visitantes al sitio, incluidos contratistas y proveedores? * Evalúe si los registros de visitantes tienen campos específicos para detalles como nombres, razones de visita y duración de la visita. * ¿Se requiere que los visitantes estén acompañados en todo momento durante su estancia en las instalaciones? * ¿Se controlan los puntos de acceso como áreas de entrega, carga y otros donde personas no autorizadas podrían ingresar a las instalaciones? * ¿Se mantiene un libro de registro físico o un registro de auditoría electrónico de todos los accesos de manera segura? * ¿Se inspeccionan y examinan las pertenencias personales de los empleados y partes interesadas a la entrada y salida? * ¿La organización establece mecanismos para inspeccionar y examinar las mochilas, bolsos, carteras, cajas, etc. de los colaboradores o visitantes que ingresen y salen de las instalaciones? * ¿Los paquetes y correos se inspeccionan antes de ser recibidos para distribuirlos, manteniendo un registro (quién recibe y a quién está destinado)? * ¿Se inspeccionan los vehículos que entren y salgan del recinto, hay un registro actualizado? * Considere los accesos a autoridades y vehículos de atención de emergencia. * ¿Se restringe el acceso a las áreas de entrega y carga desde el exterior del edificio al personal identificado y autorizado? * ¿Las áreas de entrega y carga están diseñadas para prevenir que el personal de entrega obtenga acceso no autorizado a otras partes del edificio? * Entreviste al personal de seguridad o al equipo de diseño para obtener información sobre cómo se ha implementado el diseño de las áreas de entrega y carga. * ¿Se llevan a cabo inspecciones y exámenes de las entregas entrantes en busca de materiales peligrosos antes de que se muevan de las áreas de entrega y carga? * ¿La organización ha diseñado e implementado medidas de seguridad física en sus oficinas, salas e instalaciones? * ¿Se han considerado las pautas especificadas para asegurar las oficinas, salas e instalaciones? * ¿Las instalaciones críticas están ubicadas de manera que eviten el acceso del público? * ¿Se han implementado medidas para evitar que los edificios revelen el propósito de las actividades de procesamiento de información? * ¿Las instalaciones están configuradas para evitar la visibilidad y audibilidad de información confidencial desde el exterior? * ¿Se restringe el acceso a directorios, guías telefónicas internas y mapas que identifiquen ubicaciones de instalaciones confidenciales? * ¿El personal asignado tiene los derechos de inspeccionar la propiedad y los vehículos colocando los letreros requeridos? * ¿La organización emplea tecnologías anti manipulación para detectar y prevenir alteraciones físicas en los componentes de hardware? * Solicite información sobre las tecnologías anti manipulación utilizadas, como sellos de garantía, sensores de vibración o detección de apertura de carcasas. * ¿Las tecnologías anti manipulación están implementadas en los componentes de hardware críticos y sensibles? * Evalúe registros de revisiones anteriores y verificar si se realizaron evaluaciones periódicas de las tecnologías implementadas. * ¿La instalación cuenta con guardias presentes en los puntos de acceso físicos definidos por la organización las 24 horas del día, los 7 días de la semana? * Realice una visita a la instalación en diferentes momentos del día y de la semana para verificar la presencia de guardias en los puntos de acceso. * ¿Se implementan carcasas físicas con cerradura para proteger los componentes del sistema definidos por la organización contra acceso físico no autorizado? * Considerar los siguientes puntos: * La organización minimiza los puntos de acceso y salida. * ¿Se usan pasarelas, túneles y pasos elevados para evitar puntos de acceso adicionales? * ¿Se utilizan cercas, asegure o controle el acceso a todas las puertas? * ¿La organización mantiene registros de auditoría de acceso físico en los puntos de entrada o salida especificados? * Examine una muestra de los registros de auditoría de acceso físico en los puntos de entrada o salida y verificar si están completos y detallados, incluyendo fecha, hora, nombre del individuo y propósito de la entrada o salida. * Revise los registros de auditoría con las cámaras de seguridad u otros sistemas de monitoreo para confirmar la precisión y consistencia de la información registrada. * ¿Se lleva a cabo una revisión periódica de los registros de auditoría de acceso físico? |

|  |
| --- |
| **3.3 Temática: Concientización, sistema de indicadores cuantitativos y mejora continua para el Acceso Físico** |
| El objetivo es evaluar las prácticas y enfoques implementados por una organización para educar a su personal en seguridad física, medir cuantitativamente la eficacia de las medidas implementadas y garantizar una evolución constante de los procedimientos. Es importante analizar si la organización tiene programas educativos para sensibilizar al personal sobre las mejores prácticas de seguridad física y el acceso adecuado a las áreas restringidas, revisar el contenido y la calidad del material de capacitación utilizado para educar al personal y si participa activamente en los programas de concientización aplicando los conceptos aprendidos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se proporciona formación periódica sobre concienciación de la seguridad de la información física a todos los empleados? * Revise los registros de formación o sesiones de concienciación anteriores para verificar si se documenta la participación de los empleados. * ¿Los contenidos de la formación incluyen aspectos relevantes de la seguridad de la información física, como acceso a instalaciones, manejo de credenciales y prevención de intrusiones? * Entreviste a un grupo de empleados al azar y preguntarles sobre los temas cubiertos en la formación para verificar si están al tanto de estos aspectos. * ¿La formación se adapta a las necesidades cambiantes de la organización y a las nuevas amenazas y vulnerabilidades? * ¿Se concientiza al personal en sus responsabilidades de reconocer las vulnerabilidades de la organización en la Seguridad Física? * ¿Se establece una coordinación efectiva entre los equipos de revisión e investigación y el equipo de respuesta a incidentes de la organización? * ¿Se documentan los resultados de las revisiones e investigaciones de manera adecuada y se comparten con el equipo de respuesta a incidentes? * ¿La organización ha definido clases o tipos de intrusiones y tiene mecanismos automatizados para iniciar respuestas a incidentes basadas en estas clases? * ¿Se evalúa la efectividad de las acciones de respuesta automatizadas en relación con las clases de intrusiones? * Revise registros de incidentes pasados para determinar si las acciones automatizadas fueron efectivas en la mitigación de intrusiones y si se realizaron ajustes en los mecanismos automatizados en función de los resultados. * ¿Se ha establecido un sistema de indicadores cuantitativos con métricas específicas para medir la efectividad de los controles de seguridad física implementados? * ¿Qué métricas se están utilizando para medir la efectividad de los controles   implementados? Para la evaluación, el auditor debe tener en consideración los siguientes datos:   * Número de incidentes relacionados con la seguridad de la información física. * Número de dispositivos de salida robados o extraviados. * Porcentaje de documentos y dispositivos de salida identificados en el inventario. * Tiempo de respuesta a incidentes de seguridad física. Porcentaje de acceso no autorizado detectado. * Porcentaje de empleados capacitados en seguridad física. Tasa de falsos positivos de alarmas. * Tiempo promedio de recuperación después de un incidente. * ¿Se recopilan y registran los datos necesarios para calcular las métricas de forma regular? * ¿Las métricas están siendo utilizadas para identificar áreas de mejora y tomar decisiones informadas para fortalecer los controles físicos? * Analice las acciones tomadas como resultado de los análisis de métricas anteriores para verificar si se han implementado mejoras o cambios en los controles físicos. |