

**GASIC 6 – Seguridad en Redes**

**Preguntas de Auditoría**

**Monitoreo y Registro**

**Competencias Básicas del Auditor**

1. **Conocimiento en seguridad de la información:** El auditor debe tener un profundo conocimiento de los principios y conceptos fundamentales de seguridad de la información, incluyendo la confidencialidad, integridad y disponibilidad de los datos.
2. **Conocimientos de redes:** Es esencial tener un conocimiento sólido de las redes de computadoras, incluyendo protocolos, topologías, componentes de red y arquitecturas.
3. **Comprensión de estándares y normativas:** Familiaridad con estándares de seguridad de la información como ISO 27001, NIST, CIS Controls y otras normativas aplicables. Debe comprender los requisitos de cumplimiento y saber cómo evaluar el cumplimiento de la organización.
4. **Herramientas de auditoría:** Ser capaz de utilizar herramientas de auditoría y análisis de seguridad, como escáneres de vulnerabilidades, herramientas de prueba de penetración, y sistemas de detección de intrusiones (IDS/IPS).
5. **Habilidades de análisis:** Ser capaz de analizar la configuración de dispositivos de red, registros de eventos y otros datos para identificar vulnerabilidades y problemas de seguridad.
6. **Gestión de riesgos:** Comprender cómo evaluar y gestionar los riesgos de seguridad en una infraestructura de red, incluyendo la identificación, análisis y mitigación de riesgos.

# Visión General

Para este control, se debe comprender la importancia y el proceso de monitoreo y registro en ciberseguridad, el cual es un proceso integral que involucra la supervisión constante de la infraestructura de tecnología de la información de una organización, la detección y análisis de eventos y actividades sospechosas, y la creación de registros detallados de estas actividades. Consiste en utilizar herramientas y técnicas para observar el tráfico de red, el acceso a sistemas y la actividad de usuarios con el fin de identificar posibles amenazas cibernéticas o brechas de seguridad. Se lleva a cabo para detectar incidentes de seguridad en tiempo real, analizar tendencias y patrones, y proporcionar una visión precisa de la postura de seguridad de la organización.

**1.1 Eventos que pueden ocurrir**

El monitoreo y registro en ciberseguridad son esenciales para detectar una amplia gama de eventos y actividades potencialmente peligrosas en entornos digitales. Estos eventos incluyen intentos de intrusiones o ataques cibernéticos, como escaneos de puertos, ataques de fuerza bruta y malware; comportamiento anómalo de usuarios, como intentos de acceso no autorizado o uso indebido de privilegios; fallos en sistemas y aplicaciones que puedan indicar vulnerabilidades; cambios no autorizados en configuraciones de seguridad; tráfico de red inusual o sospechoso; y cualquier otra actividad que pueda poner en riesgo la integridad, confidencialidad o disponibilidad de datos y sistemas de una organización. El monitoreo y registro permiten identificar estas amenazas y tomar medidas para proteger la infraestructura y los activos digitales.

**1.2 Herramientas y técnicas**

Entre las herramientas clave se encuentran los sistemas de Gestión de Información y Eventos de Seguridad (SIEM), que permiten recopilar, correlacionar y analizar registros de eventos de diferentes fuentes. Las soluciones de análisis de comportamiento y detección de amenazas (UEBA) son fundamentales para identificar patrones anómalos de actividad. Además, las herramientas de análisis de registros y tráfico de red, como Wireshark, son útiles para la inspección profunda de paquetes y la identificación de problemas. En cuanto a las técnicas, la normalización y correlación de datos, la creación de alertas personalizadas, la revisión periódica de registros y el análisis de tendencias a largo plazo son prácticas esenciales. También se utilizan técnicas de análisis de datos avanzados y aprendizaje automático para detectar amenazas complejas.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Determinar criterios para actividades o condiciones inusuales o no autorizadas para el tráfico de comunicaciones entrantes y salientes.  2. Asegurar que dentro del proceso de monitoreo se monitoree y detecten las siguientes dimensiones:  2.1 la red para detectar posibles eventos de seguridad cibernética.  2.2 la actividad del personal para detectar posibles eventos de seguridad cibernética.  2.3 código malicioso.  2.4 código móvil no autorizado.  2.5 personal, conexiones, dispositivos y software no autorizados.  3. Detectar comportamientos anómalos y posibles incidentes de seguridad de la información. Se debería considerar la inclusión de los siguientes elementos en sistema de control.  3.1 tráfico de salida y entrada de red, de sistema y de aplicaciones.  3.2 acceso a sistemas, servidores, equipos de red, sistema de supervisión, aplicaciones críticas, otro.  3.3 archivos de configuración de sistema y de red de nivel crítico o de administrador.  3.4 registros de herramientas de seguridad.  3.5 registros de eventos relacionados con actividad de sistema y de red.  3.6 comprobar que el código que se ejecuta está autorizado para funcionar en el sistema y que no fue manipulado .  3.7 uso de recursos |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Se deben centralizar las alertas de eventos de seguridad en todos los activos empresariales para la correlación y el análisis de registros.  1.1 La implementación de mejores prácticas requiere el uso de un SIEM, que incluye alertas de correlación de eventos definidas por el proveedor.  1.1.1 Una plataforma de análisis de registros configurada con alertas de correlación relevantes para la seguridad  también cumple con esta protección.  2. Invoque capacidades de monitoreo interno o implemente dispositivos de monitoreo:  2.1 Estratégicamente dentro del sistema para recopilar información esencial determinada por la organización;  2.2 En ubicaciones ad hoc dentro del sistema para rastrear tipos específicos de transacciones de interés para la organización.  3. Producir, almacenar y proteger registros que graban actividades, excepciones, fallos y otros eventos relevantes.  3.1 Los registros de eventos deberían incluir para cada evento, según sea el caso:  3.1.1 identificaciones de usuario.  3.1.2 actividades de sistema.  3.1.3 fechas, horas y detalles de eventos relevantes (por ejemplo, inicio y cierre de sesión).  3.1.4 identidad del dispositivo, identificador de sistema y ubicación.  3.1.5 direcciones y protocolos de red.  3.2 Los siguientes eventos se deberían considerar para el registro:  3.2.1 intentos de acceso al sistema exitosos y rechazados.  3.2.2 intentos de acceso a los datos y a otros recursos, tanto los realizados con éxito como los rechazados.  3.2.3 cambios en la configuración de sistema.  3.2.4 uso de privilegios.  3.2.5 uso de programas y aplicaciones de utilidad.  3.2.6 archivos a los que se accedió y tipo de acceso, incluyendo el borrado de archivos de datos importantes.  3.2.7 alarmas emitidas por sistema de control de acceso.  3.2.8 activación y desactivación de los sistemas de seguridad, como los sistemas antivirus y los sistemas de detección de intrusos.  3.2.9 creación, modificación o supresión de identidades |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Emplee herramientas y mecanismos automatizados para respaldar el análisis de eventos casi en tiempo real.  1.1 Se deben ajustar los umbrales de alertas de eventos de seguridad mensualmente o con mayor frecuencia  1.2 Ajustar el nivel de actividad de monitoreo del sistema cuando haya un cambio en el riesgo para las operaciones y activos organizacionales, personas, otras organizaciones o la Nación.  2. Notificar a personal de respuesta a incidentes definido por la organización (identificado por nombre y/o función)] de eventos sospechosos detectados. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Analizar eventos y anomalías detectados:  1.1 Recopilar registros de flujo de tráfico de red y/o tráfico de red para revisarlos y alertarlos desde dispositivos de red.  1.2 Registrar eventos relacionados con la seguridad y conservar los registros durante el periodo de tiempo apropiado.  2. Revisar regularmente los logs de eventos para detectar posibles incidentes.  3. Implementar un monitoreo continuo a nivel de organización que incluye:  3.1.Establecimiento de métricas definidas por la organización que serán monitoreadas.  3.2 Establecimiento de frecuencias definidas por la organización para el seguimiento y para la evaluación de la eficacia del control.  3.3 Evaluaciones de control continuo de acuerdo con la estrategia de monitoreo continuo.  3.4 Monitoreo continuo de métricas definidas por el sistema y la organización de acuerdo con la estrategia de monitoreo continuo.  3.5 Correlación y análisis de la información generada por las evaluaciones de control y seguimiento;  3.6 Acciones de respuesta para abordar los resultados del análisis de la evaluación de control y la información de seguimiento.  3.7 Emplear evaluadores independientes o equipos de evaluación para monitorear los controles en el sistema de manera continua. |
| NIVEL 5 [Optimizado]: La organización se centra en la mejora continua y está diseñada para girar y responder a las oportunidades y los cambios. | 1. Emplear análisis de tendencias para determinar si las implementaciones de control, la frecuencia de las actividades de monitoreo continuo y los tipos de actividades utilizadas en el proceso de monitoreo continuo deben modificarse en función de los datos empíricos.  2. Garantice la precisión, vigencia y disponibilidad de los resultados de monitoreo para el sistema usando mecanismos automatizados |

1. **Preguntas de Auditoría para los Monitoreo y Registro**

|  |
| --- |
| Temática: Proceso de Monitoreo y Detección |
| El proceso de monitoreo y detección implica la evaluación minuciosa de las herramientas, tecnologías y procedimientos utilizados para supervisar la infraestructura de tecnología de la información en busca de posibles amenazas cibernéticas. Esto incluye la revisión de registros de eventos, análisis de alertas, pruebas de respuesta a incidentes y aseguramiento de que se cumplan las políticas y regulaciones de seguridad. El objetivo principal es identificar vulnerabilidades, deficiencias en la detección de amenazas y oportunidades de mejora en la capacidad de respuesta a incidentes, contribuyendo así a fortalecer la postura de seguridad de la organización y reducir el riesgo de brechas de seguridad cibernética.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha establecido un sistema de monitoreo de seguridad que abarque toda la infraestructura de tecnología de la información de la organización?   + Revise la configuración y el alcance del sistema de monitoreo de seguridad para determinar si cubre adecuadamente todas las áreas críticas de la infraestructura de TI. Identifique cualquier omisión y evalúe la justificación de la cobertura de monitoreo.   + ¿El sistema de monitoreo de seguridad actual abarca todas las áreas críticas de la infraestructura de tecnología de la información de la organización de acuerdo con las políticas y necesidades de seguridad, y se han identificado y justificado claramente las omisiones en la cobertura de monitoreo? * ¿Existen procedimientos documentados para la recolección y el almacenamiento de registros de eventos de seguridad?   + Solicite y revise los procedimientos documentados para la recolección y almacenamiento de registros de eventos de seguridad. Verifique si están actualizados y en cumplimiento con las mejores prácticas.   + ¿Los procedimientos documentados para la recolección y el almacenamiento de registros de eventos de seguridad están actualizados y en cumplimiento con las mejores prácticas de seguridad de la información, y se asegura su aplicación en la práctica? * ¿Se realiza un análisis periódico de los registros de eventos en busca de actividades sospechosas o incidentes de seguridad?   + Revise los registros de eventos pasados y verifique si se han realizado análisis periódicos para identificar actividades sospechosas. Evalúe la eficacia de estos análisis en la detección de incidentes de seguridad.   + ¿Se han realizado análisis periódicos de los registros de eventos pasados con el propósito de identificar actividades sospechosas o incidentes de seguridad, y cuál ha sido la efectividad de estos análisis en la detección de amenazas cibernéticas en la organización? * ¿Se han implementado herramientas de detección de intrusiones, sistemas de gestión de registros de seguridad (SIEM) u otras tecnologías similares?   + Verifique la existencia e implementación de estas herramientas y evalúe si están configuradas para funcionar eficazmente en la detección de amenazas.   + ¿Están configuradas y en uso herramientas de detección de intrusiones, sistemas de gestión de registros de seguridad (SIEM) u otras tecnologías similares de manera efectiva para la detección de amenazas, y se han documentado los procedimientos para su correcta operación y mantenimiento? * ¿Existe un proceso formal para evaluar y aplicar actualizaciones de seguridad en las herramientas de monitoreo y detección?   + Evalúe el proceso de gestión de actualizaciones de seguridad en las herramientas de monitoreo y detección. Verifique si se aplican actualizaciones de manera oportuna y si se realiza un seguimiento de las vulnerabilidades corregidas.   + ¿Existe un proceso formal y documentado para evaluar, aplicar y gestionar las actualizaciones de seguridad en las herramientas de monitoreo y detección de amenazas, y se realiza un seguimiento para verificar que las vulnerabilidades corregidas estén siendo abordadas de manera oportuna? * ¿Se llevan a cabo pruebas de respuesta a incidentes de seguridad para evaluar la efectividad de los procedimientos de detección y respuesta?   + Solicite y revise los resultados de pruebas de respuesta a incidentes pasadas y evalúe si se han realizado pruebas de manera regular. Analice las lecciones aprendidas y las mejoras implementadas.   + ¿Se han realizado pruebas de respuesta a incidentes de seguridad de manera regular para evaluar la capacidad de la organización para detectar, responder y recuperarse de amenazas cibernéticas, y cuáles fueron las principales lecciones aprendidas y mejoras implementadas como resultado de estas pruebas?   Para la evaluación, el auditor debe tener en consideración:  **3.1.1 Auditar las herramientas y mecanismos automatizados a emplear**  La práctica implica una evaluación exhaustiva de las soluciones tecnológicas utilizadas para proteger y fortalecer la seguridad de la infraestructura de TI de una organización. Esto abarca desde firewalls y sistemas de detección de intrusiones hasta soluciones de gestión de registros y antivirus, asegurando que estén correctamente configurados, actualizados y alineados con las políticas de seguridad. Además, implica evaluar la eficacia de los mecanismos automatizados en la detección de amenazas y en la respuesta a incidentes, identificando posibles debilidades y garantizando que se sigan las mejores prácticas de seguridad. Este proceso es esencial para mantener una postura de seguridad sólida y adaptarse a la evolución constante de las amenazas cibernéticas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha realizado una evaluación exhaustiva de las herramientas y mecanismos automatizados utilizados en ciberseguridad?   + Iniciar la auditoría revisando la lista de herramientas y mecanismos automatizados utilizados en ciberseguridad y comparándola con la documentación de políticas de seguridad para verificar que estén alineados.   + ¿Se ha realizado una evaluación exhaustiva de todas las herramientas y mecanismos automatizados utilizados en ciberseguridad, y existe una documentación completa que enumera y describe estas herramientas junto con sus funciones y configuraciones asociadas? * ¿Están configuradas las herramientas de acuerdo con las mejores prácticas y las políticas de seguridad de la organización?   + Evaluar la configuración de cada herramienta de seguridad de acuerdo con las políticas y mejores prácticas de la industria. Identificar y documentar cualquier configuración que esté en desacuerdo o represente un riesgo de seguridad.   + ¿Las herramientas de seguridad automatizadas, como los firewalls y sistemas de detección de intrusiones, están configuradas de acuerdo con las mejores prácticas de seguridad y las políticas de la organización, y se han identificado y documentado las configuraciones que están en desacuerdo o que representan un riesgo de seguridad? * ¿Se aplican actualizaciones y parches de seguridad de manera regular en todas las herramientas y mecanismos automatizados?   + Verificar que exista un proceso formal de gestión de parches y actualizaciones para todas las herramientas de seguridad. Evaluar si se siguen las mejores prácticas y si las actualizaciones se aplican de manera oportuna.   + ¿Existe un proceso formal y documentado para aplicar actualizaciones y parches de seguridad de manera regular en todas las herramientas y mecanismos automatizados utilizados en ciberseguridad, y cómo se asegura que estas actualizaciones se apliquen de manera oportuna y eficaz? * ¿Se monitorean las alertas y registros generados por las herramientas de seguridad, y se responden a ellas de manera adecuada?   + Examinar los registros de eventos y alertas generados por las herramientas de seguridad y verificar que se estén monitoreando de manera regular. Evaluar la eficacia de las respuestas a las alertas y eventos.   + ¿Se monitorean de manera regular las alertas y registros generados por las herramientas de seguridad automatizadas, y existe un proceso documentado para responder de manera adecuada a estas alertas y eventos de seguridad, incluyendo la asignación de responsabilidades específicas? * ¿Se realiza un seguimiento y análisis periódico de las métricas de seguridad generadas por estas herramientas?   + Evaluar si se lleva a cabo un seguimiento de las métricas de seguridad proporcionadas por las herramientas y si se utilizan para mejorar continuamente la postura de seguridad de la organización.   + ¿Se realiza un seguimiento y análisis periódico de las métricas de seguridad generadas por las herramientas y mecanismos automatizados, y se utilizan estos datos para mejorar continuamente las medidas de seguridad de la organización? * ¿Se han implementado herramientas de automatización de la respuesta a incidentes?   + Verificar la existencia de herramientas de automatización de la respuesta a incidentes y evaluar su configuración y eficacia en la gestión de incidentes de seguridad.   + ¿Se han implementado herramientas de automatización de la respuesta a incidentes, y en caso afirmativo, cuál es su capacidad para identificar, mitigar y documentar las acciones tomadas en respuesta a incidentes de seguridad cibernética? * ¿Se realiza una evaluación periódica de la efectividad de las herramientas y mecanismos automatizados en la detección y prevención de amenazas?   + Solicitar y revisar informes de evaluaciones periódicas de la efectividad de las herramientas de seguridad y verificar si se implementan mejoras basadas en los resultados.   + ¿Se realiza una evaluación periódica de la efectividad de las herramientas y mecanismos automatizados en la detección y prevención de amenazas, y cómo se implementan mejoras basadas en los resultados de estas evaluaciones para fortalecer la seguridad cibernética de la organización? * ¿Existe un proceso formal para la adquisición, evaluación y despliegue de nuevas herramientas de seguridad?   + Evaluar el proceso de adquisición y despliegue de nuevas herramientas de seguridad para asegurarse de que cumplan con los requisitos de seguridad y se integren adecuadamente en el entorno existente.   + ¿Existe un proceso formal y documentado para la adquisición, evaluación y despliegue de nuevas herramientas de seguridad automatizadas, y cómo se asegura la integración efectiva de estas herramientas en el entorno existente y su cumplimiento con los requisitos de seguridad de la organización?   **3.1.2 Auditar la precisión, vigencia y disponibilidad**  implica la evaluación crítica de la exactitud y actualidad de la información y recursos relacionados con la seguridad de la información en una organización. Esto abarca desde la revisión de la precisión de las bases de datos de usuarios y activos hasta la actualización de las políticas y procedimientos de seguridad. Además, se verifica que los sistemas y servicios críticos estén disponibles y funcionando de manera óptima. Esta auditoría es esencial para garantizar que la información de seguridad sea confiable, que las políticas estén actualizadas frente a las amenazas actuales y que los sistemas clave estén disponibles cuando se necesiten, contribuyendo a mantener la integridad, confidencialidad y disponibilidad de los activos de información de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza una revisión periódica de la precisión de las bases de datos de usuarios y activos de la organización?   + Solicitar una muestra de registros de usuarios y activos, y compararlos con la realidad operativa para verificar la precisión de la información. Documentar discrepancias y evaluar cómo se abordan.   + ¿Con qué frecuencia se lleva a cabo la revisión de la precisión de las bases de datos de usuarios y activos, y cómo se documentan y abordan las discrepancias identificadas durante estas revisiones? * ¿Existen políticas y procedimientos actualizados relacionados con la seguridad de la información?   + Revisar la documentación de políticas y procedimientos de seguridad para verificar que estén actualizados y en cumplimiento con las mejores prácticas y regulaciones actuales.   + ¿Cómo se asegura que las políticas y procedimientos de seguridad de la información se mantengan actualizados y en cumplimiento con las mejores prácticas y regulaciones actuales, y cuál es el proceso para su revisión y actualización? * ¿Se lleva a cabo una evaluación periódica de la vigencia de contraseñas y credenciales de acceso?   + Evaluar los registros de contraseñas y credenciales de acceso para verificar que se realicen evaluaciones periódicas de la vigencia y se apliquen políticas de cambio de contraseñas cuando sea necesario.   + ¿Cuál es el proceso para realizar evaluaciones periódicas de la vigencia de contraseñas y credenciales de acceso, y cómo se asegura que las políticas de cambio de contraseñas se apliquen de manera eficaz cuando sea necesario? * ¿Se implementan medidas para garantizar la disponibilidad de sistemas y servicios críticos?   + Evaluar las medidas de disponibilidad, como sistemas de respaldo y redundancia, y verificar que se realicen pruebas periódicas para garantizar la disponibilidad de sistemas y servicios críticos.   + ¿Qué medidas específicas se han implementado para asegurar la disponibilidad de sistemas y servicios críticos, y cómo se realizan pruebas periódicas para verificar su efectividad en situaciones de interrupción o fallo? * ¿Se mantiene un registro de incidentes de seguridad y se analizan para tomar medidas correctivas?   + Revisar los registros de incidentes de seguridad pasados y evaluar si se han registrado y analizado adecuadamente, y si se han tomado medidas correctivas para evitar su repetición.   + ¿Cómo se asegura que los incidentes de seguridad se registren de manera adecuada y que se realice un análisis efectivo para identificar las causas raíz y tomar medidas correctivas para prevenir futuros incidentes similares? * ¿Se realizan pruebas regulares de recuperación ante desastres y continuidad de operaciones?   + Verificar la existencia de planes y pruebas de recuperación ante desastres y continuidad de operaciones, y evaluar la efectividad de estos planes en la restauración de la disponibilidad de sistemas críticos.   + ¿Qué tipos de pruebas se realizan para evaluar la efectividad de los planes de recuperación ante desastres y continuidad de operaciones, y cómo se utilizan los resultados de estas pruebas para mejorar la capacidad de la organización para mantener la disponibilidad de sistemas críticos en situaciones adversas?   **3.1.3 Auditar los eventos y anomalías**  implica la revisión y análisis de registros de eventos de seguridad, alertas y comportamientos anómalos en los sistemas de una organización para detectar posibles amenazas cibernéticas. Esta auditoría se enfoca en evaluar la efectividad de las medidas de detección y respuesta de la organización, así como en identificar posibles brechas de seguridad. Además, implica la revisión de políticas y procedimientos relacionados con la gestión de eventos de seguridad y la capacitación del personal para abordar eficazmente los incidentes. Esta revisión constante es fundamental para mantener una postura de seguridad sólida y responder de manera efectiva a las amenazas en constante evolución.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se mantienen registros de eventos de seguridad y alertas generadas por sistemas y dispositivos clave?   + Revisar los registros de eventos y alertas para verificar su existencia y cómo se registran y almacenan.   + ¿Cómo se asegura que se mantengan registros de eventos de seguridad y alertas, y cuál es el proceso para registrar y almacenar esta información de manera adecuada y segura? * ¿Existe una política documentada para la gestión de eventos de seguridad y anomalías?   + Evaluar la documentación de políticas y procedimientos relacionados con la gestión de eventos de seguridad y anomalías para verificar su existencia y actualización.   + ¿Cómo se asegura que esta política esté actualizada y en cumplimiento con las mejores prácticas de gestión de eventos de seguridad y anomalías, y cuál es el proceso para su revisión y actualización? * ¿Se realiza una revisión periódica de registros para identificar comportamientos anómalos y posibles amenazas?   + Evaluar si se llevan a cabo revisiones regulares de registros de eventos y alertas, y cómo se detectan y responden a posibles amenazas.   + ¿Cómo se llevan a cabo estas revisiones periódicas de registros de eventos y alertas, y cuál es el proceso para detectar y responder a posibles amenazas identificadas durante estas revisiones? * ¿Existen procedimientos definidos para la notificación y respuesta a incidentes relacionados con eventos y anomalías?   + Verificar si se han establecido procedimientos claros para notificar, investigar y responder a incidentes relacionados con eventos y anomalías.   + ¿Cómo se asegura que los procedimientos para la notificación y respuesta a incidentes relacionados con eventos y anomalías estén bien definidos, documentados y sean efectivos en la práctica? * ¿Se utiliza alguna herramienta de análisis de comportamiento para detectar anomalías en sistemas y redes?   + Evaluar la implementación y efectividad de las herramientas de análisis de comportamiento utilizadas para detectar anomalías.   + ¿Cómo se seleccionan, implementan y configuran estas herramientas de análisis de comportamiento, y cuál es su efectividad en la detección temprana de anomalías y amenazas en sistemas y redes? |

|  |
| --- |
| Temática: Centralización de Alertas de Eventos de Seguridad |
| La centralización de alerta de eventos de seguridad implica revisar y evaluar el proceso de recopilación, correlación y gestión de alertas generadas por sistemas y dispositivos de seguridad en una organización. Esta auditoría se enfoca en garantizar que las alertas se centralicen de manera eficiente, se analicen adecuadamente y se tomen las acciones necesarias en respuesta a posibles amenazas cibernéticas. Además, se verifica la eficacia de las herramientas de gestión de eventos de seguridad y se evalúa la capacidad de la organización para responder de manera oportuna y efectiva a las alertas, contribuyendo así a fortalecer la postura de seguridad y reducir los riesgos cibernéticos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un sistema centralizado para la recopilación y correlación de alertas de eventos de seguridad de diferentes sistemas y dispositivos?   + Evaluar la existencia y efectividad del sistema centralizado de recopilación y correlación de alertas, y verificar cómo se gestionan las alertas procedentes de diversas fuentes.   + ¿Cómo se asegura que todas las alertas de eventos de seguridad de los sistemas y dispositivos de la organización se integren de manera efectiva en este sistema centralizado, y cuál es la capacidad de este sistema para gestionar alertas de diversas fuentes? * ¿Se cuentan con políticas y procedimientos documentados para la gestión de alertas de eventos de seguridad?   + Revisar la documentación de políticas y procedimientos relacionados con la gestión de alertas de eventos de seguridad para verificar su existencia, actualización y cumplimiento.   + ¿Cómo se asegura que estas políticas y procedimientos de gestión de alertas de eventos de seguridad estén actualizados y en cumplimiento con las mejores prácticas, y cuál es el proceso para su revisión y actualización? * ¿Se asignan roles y responsabilidades claros para la gestión de alertas de eventos de seguridad?   + Evaluar cómo se asignan roles y responsabilidades para la gestión de alertas y si hay un proceso documentado para la toma de decisiones y la respuesta a las alertas.   + ¿Cómo se documenta y comunica la asignación de roles y responsabilidades para la gestión de alertas de eventos de seguridad, y existe un proceso formal para la toma de decisiones y la respuesta a las alertas? * ¿Se lleva a cabo un análisis y categorización de alertas para priorizar la respuesta?   + Revisar cómo se analizan y categorizan las alertas, y verificar si se sigue un proceso para priorizar la respuesta en función de la gravedad y el impacto potencial.   + ¿Cómo se realiza el análisis y categorización de las alertas de eventos de seguridad, y cuál es el proceso para determinar la prioridad de respuesta en función de la gravedad y el impacto potencial de cada alerta? * ¿Existe un registro de incidentes relacionados con alertas de eventos de seguridad?   + Evaluar si se mantiene un registro de incidentes relacionados con alertas, y cómo se documentan, analizan y abordan estos incidentes.   + ¿Cómo se lleva a cabo el registro de incidentes relacionados con alertas de eventos de seguridad, y qué procedimientos se siguen para documentar, analizar y abordar estos incidentes de manera efectiva? |