

**GASIC 6 – Seguridad en Redes**

**Preguntas de Auditoría**

**Políticas de Configuración, Instalación de Software y de Conectividad**

**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

Las políticas de configuración, instalación de software y conectividad son componentes fundamentales de la seguridad de una organización. Ya que estas proporcionan las directrices y reglas que explican cómo se tienen que configurar y operar los sistemas y redes de una empresa para proteger sus activos digitales y datos confidenciales, Además de que software es seguro de instalar sin que el equipo y los sistemas corran riesgos. Con esto se busca evitar cualquier tipo de amenaza que pueda comprometer tanto la conectividad como la información de la empresa, ya sean estas amenazas por la incorporación de un virus al sistema por una mala instalación de software o por una mala configuración.

**1.1 Políticas de Configuración**

Las políticas de configuración son esenciales para verificar si las configuraciones se ajustan a las políticas y si se siguen las mejores prácticas de seguridad. Además, ayuda a identificar posibles deficiencias y riesgos en la configuración que podrían ser explotadas por atacantes. mitigando riesgos, protegiendo activos digitales y asegurando la integridad y la confidencialidad de la información, contribuyendo una postura de seguridad cibernética más robusta .

**1.2 Políticas de Instalación de Software**

Una de las principales razones para implementar políticas de restricción de instalación de software es prevenir la instalación de software malicioso o malware. Si los empleados pueden instalar software sin restricciones, existe un riesgo significativo de que descarguen y ejecuten programas maliciosos que pueden dañar sistemas, robar datos o comprometer la seguridad de la empresa. No solo afectara negativamente a la empresa si este software tiene un virus, sino que también este podría no estar actualizado con los últimos parches de seguridad. Además, la instalación de software no necesario para el trabajo puede distraer a los empleados y afectar la productividad.

**1.3 Políticas de Conectividad**

Una política de conectividad es esencial para establecer un marco solido de seguridad informática en una organización. Ayuda a proteger la red, los datos y los sistemas contra amenazas cibernéticas y a garantizar que el acceso a la red sea seguro y controlado. Estas políticas ayudan a controlar el acceso, a prevenir intrusiones, a proteger la privacidad de los datos. Además, contribuyen a la resiliencia y la disponibilidad de la red, lo que es esencial para la continuidad del negocio.

**1.4 Auditoría y Monitoreo de Cumplimiento**

Es fundamental mantener indicadores de cumplimiento que midan la adherencia a las políticas y establecer procesos de mejora continua para abordar desviaciones detectadas. Los registros de auditoría deben incluir detalles de todas las actualizaciones y configuraciones realizadas, mientras que las metas de cumplimiento deben ser revisadas periódicamente para adaptarse a cambios tecnológicos o de negocio. Finalmente, la supervisión debe considerar aspectos como el análisis del comportamiento del usuario, el control de dispositivos extraíbles, y la protección contra malware para garantizar un entorno seguro y eficiente.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Se debe establecer y mantener una política para la seguridad de la conectividad con base en las evaluaciones de riesgo y los requisitos del negocio. la política debe incluir:  1.1 Que el intercambio de información entre el sistema y otros sistemas utilice, además:  1.1.1 Contratos de seguridad de interconexión.  1.1.2 Acuerdos de seguridad de intercambio de información.  1.1.3 memorandos de entendimiento o acuerdo.  1.1.4 Acuerdos de nivel de servicio.  1.1.5 Acuerdos de usuario.  1.1.6 Acuerdos de divulgación.  1.2 Documentar, como parte de cada acuerdo de intercambio, las características de la interfaz, los requisitos de seguridad y privacidad, los controles y las responsabilidades de cada sistema, y el nivel de impacto de la información comunicada.  1.3 Revisar y actualizar los acuerdos con una frecuencia definida por la organización.  1.4 Verifique que las personas o los sistemas que transfieren datos entre sistemas que se interconectan tengan las autorizaciones necesarias (es decir, permisos o privilegios de escritura) antes de aceptar dichos datos.  1.5 Identificar los intercambios de información transitiva (descendente) con otros sistemas a través de los sistemas identificados.  1.6 Tomar medidas para garantizar que los intercambios de información transitiva (descendentes) cese cuando los controles de los sistemas transitivos (descendentes) identificados no puedan verificarse o validarse.  2. Desarrollar, documentar e implementar un plan de gestión de configuración para el sistema que:  2.1 Aborda los roles, las responsabilidades y los procesos y procedimientos de gestión de la configuración.  2.2 Establece un proceso para identificar elementos de configuración a lo largo del ciclo de vida de desarrollo del sistema y para administrar la configuración de los elementos de configuración.  2.3 Define los elementos de configuración para el sistema y coloca los elementos de configuración bajo la gestión de configuración.  2.4 Es revisado y aprobado por la alta dirección.  2.5 Protege el plan de gestión de la configuración de la divulgación y modificación no autorizadas.  3. Establecer políticas que rigen la instalación de software por parte de los usuarios. Esta política debe incluir procedimientos y medidas para gestionar de forma segura la instalación de “software” en los sistemas operativos como:  3.1Realizar actualizaciones de “software” operativo solo por parte de administradores capacitados previa autorización de la dirección.  3.2 Garantizar que solo se instale en los sistemas operativos el código ejecutable aprobado y ningún código de desarrollo o compilador.  3.3 Instalar y actualizar “software” solo después de haber realizado pruebas exhaustivas y satisfactorias.  3.4 Actualizar todas las bibliotecas de fuentes de programas correspondientes.  3.5 Usar un sistema de control de la configuración para mantener control de todo “software” operativo, así como documentación de sistema.  3.6 Definir una estrategia de reversión antes de aplicar cambios.  3.7 Mantener un registro de auditoría de todas las actualizaciones de “software” operativo.  3.8 Archivar versiones antiguas de “software”, junto con toda información y parámetros necesarios, procedimientos, detalles de configuración y “software” de apoyo como medida de contingencia y mientras “software” sea necesario para leer o procesar los datos archivados. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Asignar la responsabilidad de desarrollar el proceso de gestión de la configuración al personal de la organización que no esté directamente involucrado en el desarrollo del sistema.  2. Comunicar la política específica del tema a todo el personal relevante y considerar lo siguiente:  2.1 El tipo de información y el nivel de clasificación que los dispositivos terminales del usuario pueden manejar, procesar, almacenar o soportar.  2.2 Registro de los dispositivos de los usuarios.  2.3 Requisitos de protección física.  2.4 Restricción de la instalación de “software”  2.5 Requisitos para el software del dispositivo terminales del usuario y para aplicar las actualizaciones.  2.6 Normas de conexión a servicios de información, a redes públicas o a cualquier otra red fuera de instalaciones.  2.7 Controles de acceso.  2.8 Encriptación del dispositivo de almacenamiento.  2.9 Protección contra “malware”.  2.10 Desactivación, borrado o bloqueo a distancia.  2.11 Copias de seguridad.  2.12 Uso de servicios y aplicaciones web.  2.13 Análisis de comportamiento del usuario final.  2.14 Uso de dispositivos extraíbles, incluyendo dispositivos de memoria extraíbles y posibilidad de desactivar puertos físicos.  2.15 El uso de capacidades de partición, si el dispositivo terminal de usuario admite, que puede separar de forma segura la información de la organización y otros activos asociados de otra información y otros activos activos asociados en el dispositivos. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Hacer y supervisar el cumplimiento de la política de instalación de software, preferiblemente a través de mecanismos automatizados. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer objetivos y metas de cumplimiento de la políticas.  1.1 Mantener indicadores de cumplimiento de las políticas para evaluar su cumplimiento |
| 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. Establecer un proceso de mejora continua que incluya la revisión de desviaciones respecto a metas y objetivos establecidos. Se deben documentar los cambios en las mejoras. |

1. **Preguntas de Auditoría para las Políticas de Configuración, Instalación de Software y Conectividad**

|  |
| --- |
| Temática: Políticas de Configuración |
| La política de configuración se refiere a un conjunto de reglas y directrices que establecen como se deben configurar y mantener los sistemas y las redes para garantizar la seguridad y la integridad de los activos de información de la organización. Auditando se busca evaluar la robustez y la efectividad de las políticas de configuración de los datos de la empresa que tan aplicada están y si cubre completamente las vulnerabilidades de los sistemas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene documentadas políticas de configuración claramente definidas y comunicadas a todo el personal relevante?   + ¿Existe evidencia que efectivamente están documentadas?¿ Existe evidencia de que fueron comunicadas?   + Revise la documentación de políticas y procedimientos de configuración para identificar la existencia de políticas documentadas.   + ¿Las políticas de configuración abordan una variedad de aspectos, como la seguridad, el rendimiento y la disponibilidad?   + ¿El personal relevante comprende las políticas de configuración y su importancia? * ¿Dónde se encuentran almacenadas las políticas de configuración?¿Las políticas son solo accesibles por personal autorizado?   + ¿Las políticas de configuración están respaldadas y protegidas contra pérdida o acceso no autorizado?     - Verifique si se han implementado controles de acceso para restringir el acceso a las políticas de configuración a personal autorizado. Esto podría incluir contraseñas, autenticación de dos factores o permisos de archivo.     - Revise la documentación que describe las medidas de seguridad implementadas, como listas de control de acceso (ACL), políticas de grupos de seguridad, etc.   + Solicite una lista de ubicaciones físicas o digitales donde se almacenan las políticas de configuración, como sistemas de archivos, servidores, carpetas específicas, etc   + ¿Se mantienen registros de acceso a las políticas de configuración para verificar quién las consulta? * ¿Cómo se gestiona el acceso a sistemas y datos sensibles?   + ¿Se aplica un principio de menor privilegio al otorgar acceso a sistemas y datos sensibles?   + ¿Se realiza una revisión periódica y una auditoría de los accesos a sistemas y datos sensibles?   + ¿Existe un proceso definido para revocar el acceso a sistemas y datos sensibles cuando ya no es necesario? * ¿Se lleva a cabo un seguimiento y registro de cambios en la configuración de sistemas y redes?   + ¿Existe un proceso formal para el seguimiento y registro de cambios en la configuración de sistemas y redes?   + Evalúe si se han establecido roles y responsabilidades claros en relación con el seguimiento y registro de cambios, y si se han asignado personas específicas para estas funciones.   + ¿Se documentan adecuadamente los cambios realizados en la configuración de sistemas y redes?   + ¿Los cambios en la configuración son revisados y aprobados antes de su implementación?   + ¿Se retienen los registros de cambios en la configuración durante un período de tiempo adecuado? * ¿Se aplican políticas de cifrado para proteger datos sensibles en reposo y en tránsito?   + ¿La organización tiene políticas documentadas que establecen la necesidad de cifrar datos sensibles tanto en reposo como en tránsito?   + ¿Existe un inventario de datos sensibles que debe ser cifrado, junto con una clasificación adecuada de su nivel de sensibilidad?   + ¿Se implementan medidas de cifrado para proteger datos sensibles almacenados en servidores y dispositivos de almacenamiento?   + ¿Se utiliza cifrado de datos en las comunicaciones internas y externas para proteger datos sensibles durante la transmisión?     - Examine la configuración de redes y sistemas para verificar la implementación de cifrado en las comunicaciones, como el uso de protocolos seguros (por ejemplo, HTTPS, VPN) en las transferencias de datos. * ¿Se segmentan las redes para aislar los activos críticos y datos sensibles?   + ¿La organización tiene políticas o directrices documentadas para la segmentación de redes con el objetivo de aislar activos críticos y datos sensibles?   + Realice un mapeo de la red y comparar con las políticas de segmentación establecidas para confirmar que se están aplicando.   + Verifique la configuración de los dispositivos de red (como firewalls o routers) para revisar las reglas de segmentación y las restricciones de tráfico entre redes.   + ¿Se realizan evaluaciones regulares de seguridad de las redes segmentadas para garantizar el cumplimiento continuo de las políticas de segmentación?   + ¿Se documentan y revisan regularmente los cambios en la configuración? * ¿La organización cuenta con políticas documentadas de configuración de firewalls?   + ¿Están claramente definidos los roles y responsabilidades relacionados con la configuración de los firewalls?   + ¿Las políticas de configuración de firewalls establecen directrices específicas para la apertura y cierre de puertos y la gestión de reglas de seguridad?   + ¿Se realiza una revisión periódica y una actualización de las políticas de configuración de firewalls? |

|  |
| --- |
| Temática: Políticas de Instalación de Software |
| Se busca tener bien definidas las reglas de instalación de software no validado por la empresa con fin de proteger a esta de posibles aplicaciones que puedan contener archivos malignos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un proceso definido para autorizar la instalación de nuevo software?   + ¿Está documentado y es comunicado al personal relevante?   + Revise la documentación de políticas y procedimientos de instalación de software para identificar la existencia de políticas documentadas.   + ¿Las políticas de instalación de software abordan una variedad de aspectos, como si estas son seguras, no afectaran el rendimiento, está debidamente licenciado y cumple los términos de la licencia ?   + ¿El personal relevante comprende las políticas de instalación de software y su importancia? * ¿ Se asignan responsabilidades claras para la aprobación y supervisión de la instalación de software?   + ¿Se tiene constancia de quienes son los responsables y estos lo tienen claro?     - Verifique que los responsables sepan que son los encargados de realizar esta tarea.   + ¿ Se tiene constancia de los software aprobados y los que no?     - Verifique que tanto software aprobados como los rechazado sean documentados de manera clara y que esta información sea conocimiento y esté al alcance de todos dentro de la empresa.   + ¿Cuándo un software es rechazado estos se bloquean directamente desde la fuente de descarga? * ¿ Cómo se evalúa la seguridad y la conveniencia de un software antes de su instalación?   + ¿ Se verifica si el software cumple con la normativas de privacidad y seguridad de los datos?   + ¿ Se prohíbe la instalación de software descargado de sitios no autorizados o de dudosa procedencia?   + ¿Se verifica que el software instalado este debidamente licenciado y en cumplimiento con los términos de licencia?   + ¿Existen un plan con pasos a seguir a la hora de la verificación y validación de un software a la hora de aprobarlo o rechazarlo?     - Revisar plan de aceptación o rechazo de nuevo software.     - Verificar que los puntos mencionados se encuentren en este plan. * ¿ Cómo se manejan las actualizaciones y las transiciones de versión?   + ¿Se tienen controles a seguir a la hora de que se necesite actualizar o cambiar de versión?     - Verifique la existencia de controles de actualización.   + ¿ Se tienen respaldos de versiones anteriores por si existe un problema a la hora de la instalación?     - ¿Estos cada cuanto se actualizan con los nuevos estados de las maquinas?     - ¿ Se revisa regularmente que estos estén en buen estado?     - Revise respaldos de versiones anteriormente   + ¿Las actualizaciones solo se emplean cuando el personal de la empresa no está realizando sus labores?     - ¿Generalmente en que horario se emplean estas actualizaciones?   + ¿Se espera a la comprobación de que la actualización es segura y no afecta el rendimiento?     - ¿Cómo se comprueba esto? |

|  |
| --- |
| 3.3 Temática: Políticas de Conectividad |
| Se busca impedir o minimizar las conexiones no autorizadas tanto de dispositivos externos a la empresa, así como conexiones dentro de la empresa a información clasificada o que no deberían de ser accesible. Para esto se pueden incluir preguntas tales como:  Este levantamiento puede incluir análisis específicos tales como:   * ¿ Existe una política enfocada en el uso de dispositivos extraíbles tanto dentro como fuera de la empresa?   + ¿Está documentado y es comunicado al personal relevante?   + Revise la documentación de políticas y procedimientos de conectividad para identificar la existencia de políticas documentadas.   + ¿Las políticas de conectividad abordan una variedad de aspectos, como se manejan los dispositivos extraíbles, la conexión a servicios que no sean necesarios para los procesos de la empresa, monitoreo de red para evitar intrusiones y cómo reaccionar a estos ?   + ¿El personal relevante comprende las políticas de instalación de software y su importancia? * ¿ Se evalúan, permiten o rechazan servicios y páginas web que no sean necesaria para los procesos de la empresa o no sean de confianza?   + Revise quien evalúa esto.   + Revise que servicios y páginas web han sido rechazadas. * ¿ Se tiene un registro de cada dispositivo de los usuarios para evitar intrusiones de usuarios desconocidos?   + ¿Son todos los dispositivos aprobados o existen cualidades que estos deben de cumplir para ser aprobado?     - Revise cualidades que estos deban de cumplir para ser actualizados.   + Revise si existe evidencia de cada dispositivo de los usuarios aprobados.     - ¿Se encuentran estos seguros solo accesible a personal autorizado? * ¿ Existen roles dentro de la organización que permitan o no el acceso a información sensible?   + ¿ Estos son constantemente actualizados en caso de una renuncia o despido?   + ¿ Cada rol es mantenido en secreto?   + Revise asignación de roles dentro de los sistemas de la organización. * ¿ Se segmentan las redes para aislar los activos críticos y datos sensibles?   + ¿La organización tiene políticas o directrices documentadas para la segmentación de redes con el objetivo de aislar activos críticos y datos sensibles?   + Realice un mapeo de la red y comparar con las políticas de segmentación establecidas para confirmar que se están aplicando.   + Verifique la configuración de los dispositivos de red (como firewalls o routers) para revisar las reglas de segmentación y las restricciones de tráfico entre redes.   + ¿Se realizan evaluaciones regulares de seguridad de las redes segmentadas para garantizar el cumplimiento continuo de las políticas de segmentación?   + ¿Se documentan y revisan regularmente los cambios en la configuración? * ¿ Se emplean sistemas de detección de intrusiones para monitorear y alertar sobre actividades sospechosas en la red?   + ¿La organización tiene políticas o directrices documentadas para el monitoreo de las actividades sospechosas en la red?   + Realice una verificación del sistema de monitoreo   + ¿Se verifica regularmente el correcto funcionamiento del sistema de monitoreo? * ¿ Cuál es el proceso para responder a alertas de intrusiones?   + ¿Existe un plan de respuesta frente a una intrusión?   + ¿ Quién es el responsable para hacer frente a la intrusión?     - Revise plan de respuesta frente a intrusión y que este tenga información clara y concisa.   + ¿Se documentan todos los sucesos sospechosos y que método se utilizó para frenarlos?     - Revise documentación sobre sucesos. |