

**GASIC 6 – Seguridad en Redes**

**Preguntas de Auditoría**

**Datos e Información**

**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

La gestión de datos e información implica implementar controles específicos para proteger la información en reposo y en tránsito, adaptándola a su nivel de sensibilidad. Esto incluye el uso de técnicas como cifrado, enmascaramiento y segmentación de datos para garantizar que solo usuarios autorizados accedan a los datos necesarios. Además, los procesos de prevención de fuga de información y eliminación segura se aplican de manera integral en sistemas, redes y dispositivos. Estas medidas permiten no solo proteger los datos sensibles de la organización, sino también cumplir con regulaciones específicas y minimizar riesgos operativos asociados a la exposición de información.

**1.1 Protección de Datos en Reposo y en Tránsito**

Los datos en reposo deben cifrarse según su clasificación y protegerse mediante técnicas como anonimización y enmascaramiento, adaptadas al control de acceso definido por la organización. En el caso de los datos en tránsito, es imprescindible utilizar cifrado robusto, como TLS o VPNs seguras, para prevenir intercepciones durante la transmisión. Para garantizar un acceso controlado, se debe diseñar un mecanismo que permita ofuscar datos sensibles, mostrando solo la información estrictamente necesaria para cada usuario o proceso, y asegurando que los datos ofuscados no revelen su contenido original.

**1.2 Prevención de Fuga de Datos y Almacenamiento Seguro**

La prevención de fuga de datos debe aplicarse a través de herramientas especializadas que detecten y bloqueen cualquier intento de divulgación no autorizada. Estas herramientas deben identificar y clasificar información crítica, controlar los canales de fuga y registrar las acciones de los usuarios asociados a intentos de exfiltración de datos. Paralelamente, los datos críticos deben almacenarse en ubicaciones seguras, preferiblemente fuera de línea, y las claves criptográficas deben estar protegidas en dispositivos especializados para evitar accesos no autorizados.

Cuando los datos ya no sean necesarios, su eliminación debe realizarse mediante métodos adecuados al tipo de almacenamiento, registrando el proceso como evidencia. En caso de externalizar este servicio, los proveedores deben garantizar la destrucción completa y entregar documentación como prueba del procedimiento realizado.

**1.3 Auditoría y Mejora Continua**

Desde el punto de vista de auditoría, es fundamental monitorear el uso de técnicas de protección y prevención de fugas, manteniendo indicadores que permitan evaluar su eficacia. Los mecanismos de transmisión segura deben garantizar la integridad de los datos durante su intercambio entre sistemas, utilizando atributos de seguridad vinculados a la información. Un proceso de mejora continua permitirá identificar desviaciones en las metas de protección, adaptando los controles para responder a nuevas amenazas o cambios en las políticas organizacionales, documentando las mejoras realizadas para garantizar un ciclo de seguridad sostenible.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Los datos en reposo y en tránsito deben estar protegidos.  1.1 Utilizar enmascaramiento de acuerdo con la política específica de la organización sobre control de acceso y otras políticas específicas relacionadas con el tema tales como:  ﻿ 1.1.1 seudonimización o la anonimización.  ﻿1.1.1 encriptación.  ﻿1.1.1 anulación o eliminación de caracteres.  ﻿1.1.1 sustitución.  ﻿1.1.1 sustitución de valores por su almohadilla.  1.2 Encriptar la información en tránsito y la información almacenada de acuerdo a su clasificación.  1.3 Al momento de aplicar las técnicas de enmascaramiento de datos se debería tener en cuenta lo siguiente:  1.3.1 no concesión a todos los usuarios acceso a todos los datos, por lo que se diseñan consultas y máscaras para mostrar solo datos mínimos necesarios al usuario.  1.3.2 diseño e implementación un mecanismo de ofuscación de datos, en este caso, hay casos en que algunos datos deberían no ser visibles para el usuario para algunos registros de un conjunto de datos.  1.3.3 cuando los datos están ofuscados, dando al mandante de PII la posibilidad de exigir que los usuarios no puedan ver si los datos están ofuscados.  2. Cifrar los datos en dispositivos de usuario final que contengan datos confidenciales.  3. Segmentar el procesamiento y almacenamiento de datos según la sensibilidad de los datos.  3.1 Los entornos de desarrollo y prueba(s) deben estar separados del entorno de producción.  4. Establecer mecanismos confiables para apoyar la transmisión y recepción segura de la información |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. La organización almacena fuera de línea en una ubicación segura información crítica.  1.1 Proporcionar almacenamiento protegido para claves criptográficas.  2. Aplicar medidas de prevención de fuga de datos a los sistemas, redes y cualesquiera otros dispositivos que procesen, almacenen o transmitan información sensible. La organización debería considerar lo siguiente para reducir el riesgo de fuga de datos.  2.1. identificar y clasificar información para protegerla contra las filtraciones.  2.2. controlar canales de fuga de datos.  2.3. actuar para evitar filtración de información.  Se deberían utilizar herramientas de prevención de fuga de datos para.  2.4. identificar y controlar información sensible que corre riesgo de ser revelada sin autorización.  2.5. detectar divulgación de información sensible.  2.6. bloquear acciones de usuarios o transmisiones de red que expongan información sensible.  3. Eliminar la información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento cuando ya no sea necesaria. Al momento de eliminar la información de los sistemas, aplicaciones y servicios, se debería tener en cuenta lo siguiente:  3.1. seleccionar un método de borrado.  3.2. registrar resultados de eliminación como prueba.  3.3 obtener pruebas de la eliminación de información de ellos, cuando se usen proveedores de servicios de eliminación de información.  4. Implementar mecanismos o técnicas definidos por la organización para vincular los atributos de seguridad y privacidad a la información transmitida.  4.1 El sistema de información asocia atributos de seguridad y privacidad definidos por la organización con información intercambiada entre sistemas y entre componentes del sistema.  4.2 Implemente mecanismos contra la suplantación de identidad para evitar que los adversarios falsifiquen los atributos de seguridad que indican la aplicación exitosa del proceso de seguridad. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Implementar sistemas de distribución protegido definido por la organización para evitar la divulgación no autorizada de información, detectar cambios en la información durante la transmisión. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer metas y objetivos de protección y prevención de fuga de datos.  1.1 Se deben establecer indicadores que permitan medir 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. Mantener un proceso de mejora continua para establecer mejoras en el resguardo de la seguridad de datos e información según las desviaciones identificadas según los objetivos y metas establecidas.  2. Documentar hallazgos y cambios en los procesos de mejora. |

1. **Preguntas de Auditoría para los Datos e Información**

|  |
| --- |
| Temática: Protección de Datos en Reposo y Tránsito |
| Un auditor debe revisar cómo se protegen los datos almacenados y transmitidos, ya que esto es crucial para asegurarse de que una empresa cumple con las leyes, protege la privacidad de las personas y mantiene la integridad de la información, además de preservar su reputación. Asegurar que los datos estén seguros no solo evita problemas legales y protege información personal y valiosa, sino que también ayuda a fortalecer la seguridad cibernética en general. La auditoría ayuda a encontrar debilidades en la protección de datos, lo que permite tomar medidas para mejorar y, en última instancia, mantener la confianza de los clientes y socios comerciales en la organización.  Para ello, el auditor debe considerar lo siguiente:  **3.1.1 Auditar el Enmascaramiento de Datos**  La práctica del enmascaramiento de datos es esencial para garantizar la seguridad y la privacidad de la información sensible. A través de la revisión y verificación constante de los métodos de enmascaramiento de datos, las organizaciones pueden asegurarse de que los datos confidenciales estén protegidos de manera efectiva contra accesos no autorizados y exposiciones indebidas  Esto es particularmente importante para cumplir con las regulaciones de privacidad de información y para mantener la integridad de los datos durante las pruebas y el desarrollo de aplicaciones. Además, la auditoría proporciona una oportunidad para identificar y abordar posibles problemas de seguridad, asegurando que las políticas y procedimientos relacionados con la seguridad de datos estén actualizados y sean efectivos en todo momento.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen políticas y procedimientos claros para determinar qué técnicas de enmascaramiento se aplican a diferentes tipos de datos? * ¿Cómo se asegura que las consultas y las máscaras de datos muestren solo la información mínima necesaria para los usuarios? * ¿Se revisan y actualizan periódicamente las políticas de enmascaramiento de datos para asegurarse de que sigan siendo efectivas? * ¿Existe un proceso para revisar y aprobar los cambios propuestos en las políticas de enmascaramiento de datos antes de su implementación? * ¿Qué medidas se toman para garantizar que las técnicas de enmascaramiento de datos no afecten negativamente a la funcionalidad de las aplicaciones que utilizan los datos? * ¿Se lleva a cabo una evaluación de riesgos periódica para identificar posibles vulnerabilidades en la implementación de las técnicas de enmascaramiento?   **3.1.2 Auditar la encriptación**  La práctica de la encriptación de datos es esencial para garantizar la seguridad y la protección de la información en un entorno digital. La encriptación juega un papel crucial en la preservación de la confidencialidad e integridad de los datos, y una auditoría asegura que se esté aplicando adecuadamente. Es vital para el cumplimiento normativo, ya que muchas leyes y regulaciones exigen medidas sólidas de seguridad de datos. También contribuye a la gestión de riesgos, la eficiencia operativa y la confianza del cliente al demostrar un compromiso serio con la protección de la información sensible, ayudando a mantener la reputación de la organización y a prepararse para posibles incidentes de seguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se determina el nivel adecuado de encriptación para los diferentes tipos de datos según su clasificación? * ¿Existen procesos de gestión de claves sólidos para respaldar la encriptación? * ¿Qué algoritmos de encriptación se utilizan para proteger los datos en tránsito y en reposo? * ¿Existen políticas claras sobre cuándo y cómo se debe aplicar la encriptación a los diferentes tipos de datos? * ¿Se realiza un seguimiento y gestión adecuada de las claves de encriptación, incluyendo su rotación periódica? * ¿Se cifra la información de respaldo y se almacena de manera segura? * ¿Cómo se gestiona el proceso de desencriptación cuando se necesita acceder a datos cifrados? * ¿Se realizan pruebas regulares para evaluar la efectividad de la encriptación en la protección de los datos?   **3.1.3 Auditar el Enmascaramiento de Datos Detallado**  La auditoría del enmascaramiento de datos detallado es de vital importancia en el ámbito de protección de la privacidad. Esta práctica garantiza que los datos sensibles se protejan adecuadamente mediante la ocultación o reemplazo de información confidencial.  Cabe señalar, que las auditorías respaldan la gestión al proporcionar evidencia objetiva de que los controles de enmascaramiento de datos funcionan correctamente, al tiempo que generan confianza en los clientes al demostrar el compromiso de la organización con la seguridad y la privacidad de los datos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han implementado mecanismos de ofuscación de datos cuando es necesario ocultar cierta información para algunos registros? * ¿Se ha realizado un análisis exhaustivo de quiénes tienen acceso a los datos y cuáles son sus necesidades de acceso específicas? * ¿Cuáles son los criterios utilizados para determinar qué datos deben enmascararse y en qué situaciones? * ¿Se lleva un registro de las consultas y máscaras de datos aplicadas a diferentes usuarios y para qué fines? * ¿Se realizan pruebas periódicas para verificar que las máscaras de datos están funcionando según lo previsto y que los usuarios no pueden acceder a información sensible? * ¿Cómo se manejan los casos en los que ciertos datos deberían ser completamente invisibles para algunos registros de un conjunto de datos? * ¿Se han definido políticas o restricciones para la desenmascarar los datos en ciertas situaciones, y cuáles son esas situaciones? |

|  |
| --- |
| Temática: Prevención de Fuga de Datos |
| La organización se debe asegurar de que no exista fuga de datos e información, ya que garantiza el cumplimiento de regulaciones que exigen la protección de datos confidenciales. Además, la auditoría de este control preserva la reputación del negocio al verificar que se implementen controles efectivos, evitando incidentes perjudiciales. También protege activos valiosos, previene pérdidas financieras derivadas de multas y compensaciones, y mejora la seguridad interna al detectar y prevenir actividades maliciosas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene políticas y procedimientos documentados para la prevención de fuga de datos? y en caso de existir, ¿Están estos documentos disponibles para todo el personal y se comunican de manera efectiva? * ¿Se proporciona capacitación y concienciación regular a los empleados sobre las políticas y procedimientos de prevención de fuga de información? * ¿Cómo se verifica que los empleados comprendan y sigan estas políticas? * ¿Se implementan sistemas de monitoreo y detección de fuga para identificar comportamientos inusuales o actividades sospechosas? * ¿Cuál es el proceso de respuesta ante una posible fuga de datos? * ¿Quién tiene autorización para acceder a datos sensibles y cómo se controla esta autorización? * ¿Se mantienen registros de acceso y actividades relacionadas con información sensible? * ¿Se realizan evaluaciones periódicas de riesgos para identificar las áreas y los sistemas más vulnerables a fuga de información? * ¿Se realizan análisis posteriores a incidentes para aprender de las brechas de seguridad? * ¿Existen acuerdos y controles específicos para garantizar la seguridad de los datos compartidos externamente? * ¿La organización tiene un proceso documentado y definido para la eliminación segura de datos almacenados? * ¿Se siguen los procedimientos establecidos para eliminar datos cuando ya no son necesarios? * ¿Qué métodos de borrado se utilizan para eliminar datos? * ¿Se emplean métodos adecuados de acuerdo con la clasificación de los datos? * ¿Existen pruebas de que se utilizan métodos efectivos de borrado? * ¿Se mantienen registros de todas las eliminaciones de datos? * ¿Se registran los resultados de las operaciones de eliminación, incluyendo la fecha y la hora de la eliminación y los datos eliminados? * ¿La organización tiene un sistema para asociar atributos de seguridad y privacidad con la información transmitida? ¿Cómo se asegura de que estos atributos se apliquen correctamente? * ¿Qué mecanismos se han implementado para prevenir la suplantación de identidad y garantizar la autenticidad de los atributos de seguridad? ¿Se realizan pruebas para verificar la efectividad de estos mecanismos? * ¿Cómo se protege la información durante la transmisión para evitar la divulgación no autorizada o cambios en la información? |