

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



**CASIG 1– Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Reconocer la Infraestructura Crítica**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimiento en Gestión de Riesgos. 2. Conocimientos en normativa de seguridad de la información y ciberseguridad. 3. Conocimiento en normativa específica de riesgos: ISO 27005, NIST 800-30, MAGERIT y en los procesos de riesgos propios de la organización 4. Conocimiento en la normativa propia de la Industria o Sector. |

# Visión General

Reconocer la infraestructura crítica en el contexto de seguridad de la información y ciberseguridad (SIC) incluye componentes como redes de comunicación, sistemas de TI, bases de datos esenciales, y activos de alta sensibilidad que respaldan la operación continua y la resiliencia de la empresa. Comprender qué constituye infraestructura crítica permite a SIC priorizar los recursos de protección y establecer medidas de seguridad adaptadas a la importancia de estos activos, minimizando así el riesgo de interrupciones que afecten negativamente a la empresa.

**1.1 Evaluación y Priorización de la Infraestructura Crítica**

Para gestionar adecuadamente la infraestructura crítica, es fundamental definir un conjunto claro de criterios que guíen la identificación y evaluación de estos activos clave, asegurando que se consideren factores como la criticidad operativa, la exposición al riesgo y la dependencia interdepartamental. Estos criterios permiten establecer una lista priorizada de infraestructura crítica y diseñar planes específicos de protección que incluyan estrategias de redundancia, control de acceso y monitoreo constante. La alineación de estos planes con las metas y normativas de la organización asegura que las medidas de SIC protejan eficazmente los activos más valiosos, maximizando la seguridad y continuidad operativa.

**1.2 Rol de la Auditoría en el Reconocimiento y Gestión de la Infraestructura Crítica**

Desde la perspectiva de auditoría, el reconocimiento y gestión de la infraestructura crítica implica revisar los criterios y procesos utilizados para identificar estos activos, asegurando que se sigan las mejores prácticas de evaluación y que la infraestructura crítica esté debidamente protegida. Los auditores verifican que los sistemas de monitoreo, control de acceso y recuperación implementados se alineen con los objetivos de seguridad, revisando los informes y análisis de riesgos asociados a la infraestructura crítica. Al documentar los hallazgos y recomendar mejoras, la auditoría respalda la optimización de los planes de protección, garantizando que la infraestructura crítica esté preparada para responder a emergencias y que los recursos de SIC se asignen de manera estratégica para proteger los elementos más vitales de la organización.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar y comprender los diversos tipos de riesgos a los que la organización está expuesta. ***[Complementar con CONTROL: ANALISIS DEL ENTORNO INTERNO Y EXTERNO]***  2. Evaluar el estado actual de la determinación y expresión de la tolerancia al riesgo organizacional.  3. Establecer, definir y comunicar claramente la tolerancia y apetito de riesgo organizacional.  3.1 Definir la forma en la que el apetito de riesgo organizacional se expresa en los procesos y directrices de la función de SIC |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir y documentar la tolerancia al riesgo organizacional en función de la evaluación de riesgos realizada.  2. Comunicar de manera clara y precisa la tolerancia al riesgo organizacional a todas las partes interesadas relevantes.  3. Establecer mecanismos para monitorear y revisar periódicamente la tolerancia al riesgo organizacional, asegurando que siga siendo válida y adecuada. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Incorporar la tolerancia al riesgo organizacional en los procesos de toma de decisiones y planificación estratégica de la organización. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles |  |
| 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. Utilizar la información obtenida de todos los análisis de monitoreo y evaluar para revisar la tolerancia y apetito al riesgo de la organización, redefinirla en consideración de los hallazgos obtenidos, utilizando un mecanismo que apunte a la mejora continua. |

# Preguntas de Auditoría para Dirigir la Tolerancia al Riesgo

|  |
| --- |
| 3.1 Temática: Revisar el rol de la organización en la Infraestructura Crítica |
| El objetivo principal de revisar el rol de la organización en la infraestructura crítica es identificar sus responsabilidades y obligaciones específicas en la protección y continuidad de los activos críticos. Esto implica entender cómo las operaciones y servicios de la organización están interconectados con otros sectores y cómo su funcionamiento contribuye al funcionamiento general de la sociedad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Los documentos estratégicos de la organización mencionan explícitamente su importancia en la infraestructura crítica y el sector industrial? * ¿La organización ha evaluado su lugar en la infraestructura y sus funciones críticas afectadas por interrupciones? * ¿Se han realizado entrevistas o encuestas para obtener la percepción de los responsables y empleados sobre la importancia de la organización en la infraestructura crítica? |

|  |
| --- |
| 3.2 Temática: Identificar y gestión de dependencias y funciones críticas |
| Revisar la identificación y gestión de dependencias y funciones críticas tiene como objetivo evaluar la vulnerabilidad y riesgo asociado con cada uno de estos aspectos. Identificar las dependencias y funciones críticas permite a la organización comprender cuáles son los elementos fundamentales para su operación y cómo están conectados entre sí. Esto facilita la toma de decisiones informadas para garantizar que se establezcan medidas de protección y contingencia adecuadas para mitigar posibles impactos negativos en caso de eventos inesperados.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Los documentos estratégicos de la organización mencionan las dependencias y funciones críticas para la entrega de servicios críticos? * ¿La evaluación de riesgos de la organización incluye el análisis de impacto en el negocio (BIA) y análisis de riesgos relacionados con diferentes estados operativos? * ¿Las políticas y procedimientos de la organización abordan específicamente la resiliencia de los servicios críticos en diferentes estados operativos? |

|  |
| --- |
| 3.3 Temática: Planes de riesgos, incidentes y continuidad del negocio |
| El objetivo principal de mantener estos planes es anticipar y prevenir posibles problemas y riesgos antes de que ocurran. La gestión de riesgos permite identificar y evaluar las amenazas potenciales que podrían afectar la infraestructura crítica y desarrollar estrategias para minimizar su impacto. La implementación de medidas preventivas y de mitigación adecuadas reduce la probabilidad de que los riesgos se conviertan en incidentes graves.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene un plan estratégico de gestión de riesgos, incidentes y continuidad que aborde explícitamente su papel en la infraestructura crítica? * ¿Se ha establecido una política clara de gestión de riesgos que incluya la importancia de abordar riesgos relacionados con la infraestructura crítica? * ¿Se ha desarrollado un plan de comunicación específico para la infraestructura crítica y se ha comunicado de manera efectiva a todas las partes interesadas pertinentes? * ¿Existe una forma de medir sus conocimientos y compresión? Es importante que el auditor pueda verificar que el plan de comunicaciones contenga:   + Objetivos   + Responsabilidades   + Procedimientos de comunicación con las entidades de la infraestructura crítica   El auditor debe verificar si se han establecido medidas y controles específicos en los procesos y procedimientos para abordar la gestión de riesgos, la gestión de  incidentes y la continuidad del negocio de la organización en la infraestructura crítica. Para esto se deben abordar los siguientes puntos:  **3.3.1 – Revisión de los planes de gestión de riesgos**   * ¿Se ha realizado un análisis de riesgos específico que aborde las amenazas y vulnerabilidades relacionadas con la infraestructura crítica? * ¿El análisis de riesgos identifica y documenta de manera adecuada las amenazas y vulnerabilidades asociadas al papel de la organización en la infraestructura crítica? * ¿El análisis de riesgos incluye medidas de mitigación específicas para abordar las amenazas y vulnerabilidades identificadas?   **3.3.2 – Revisión de los planes de gestión de incidentes**   * ¿La organización cuenta con un plan de respuesta a incidentes que aborde escenarios relacionados con la infraestructura crítica? * ¿El plan de respuesta a incidentes incluye procedimientos específicos para hacer frente a los escenarios relacionados con la infraestructura crítica? ¿Existe una descripción clara de los posibles incidentes que podrían afectar la infraestructura crítica y cómo se deben abordar? * ¿Se han llevado a cabo simulacros y pruebas del plan de respuesta a incidentes? * ¿Se ha coordinado con las partes interesadas pertinentes en la infraestructura crítica para gestionar situaciones de emergencia o interrupciones?   **3.3.3 – Revisión de los planes de continuidad de negocio**   * ¿Se ha desarrollado estrategias de continuidad del negocio que aborde los escenarios identificados en el análisis de impacto empresarial? * ¿Las estrategias seleccionadas cumplen con los requisitos para continuar y recuperar actividades prioritarias dentro del tiempo acordado * ¿Se han considerado los costos, beneficios y posición de la organización en la cadena de suministro crítico al seleccionar las estrategias? |