

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



**CASIG 1– Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Definir la Tolerancia al Riesgo**

|  |
| --- |
| **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

Definir la tolerancia al riesgo en el contexto de seguridad de la información y ciberseguridad (SIC) comienza con la identificación y comprensión de los diversos tipos de riesgos a los que la organización está expuesta, considerando tanto el entorno interno como externo. Evaluar el estado actual de la tolerancia al riesgo permite a la organización definir claramente el nivel de riesgo que puede tolerar y comunicar esta tolerancia de manera precisa a todos los departamentos y áreas involucradas. Una definición bien fundamentada de la tolerancia y el apetito de riesgo permite que SIC diseñe directrices y controles acordes con los límites de riesgo establecidos.

**1.1 Documentación, Comunicación y Monitoreo de la Tolerancia al Riesgo**

Una vez definida la tolerancia al riesgo, es crucial documentarla en función de la evaluación de riesgos realizada y comunicarla de manera clara a todas las partes interesadas, incluyendo al equipo de SIC, TI y la alta dirección. Además, es fundamental implementar mecanismos de monitoreo y revisión periódica que permitan evaluar si la tolerancia al riesgo sigue siendo adecuada en función de los cambios en el entorno y los resultados de los análisis de riesgos. Este monitoreo asegura que la organización pueda ajustar su apetito de riesgo según las necesidades estratégicas y las lecciones aprendidas, manteniendo una postura proactiva frente a los riesgos emergentes.

**1.2 Rol de la Auditoría en la Definición y Revisión de la Tolerancia al Riesgo**

Desde la perspectiva de auditoría, la definición y revisión de la tolerancia al riesgo involucra una evaluación de los procesos empleados para identificar y comunicar el apetito de riesgo. Los auditores revisan que la tolerancia al riesgo esté incorporada en los procesos de toma de decisiones y planificación estratégica, verificando que los criterios de tolerancia estén debidamente documentados y aplicados en toda la organización. Además, la auditoría asegura que se implementen sistemas de monitoreo efectivos que respalden una revisión periódica de la tolerancia al riesgo, permitiendo ajustes basados en datos y en los hallazgos de monitoreo continuo. Al documentar los hallazgos y recomendaciones, la auditoría contribuye a la mejora continua en la gestión del riesgo, asegurando que los niveles de exposición aceptables estén alineados con los objetivos de la organización y las mejores prácticas en seguridad.

# Matriz de Controles

|  |  |
| --- | --- |
| 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: Definir la Tolerancia al Riesgo |
| En primer lugar, es necesario verificar si la organización a realizado un análisis en donde identifique y documente los diferentes tipos de riesgos a los que está expuesta. Esto puede incluir riesgos relacionados con la seguridad de la información, riesgos operativos, riesgos financieros, riesgos legales y regulatorios, riesgos de reputación, entre otros.  El auditor deberá realizar entrevistas a los responsables de la gestión de riesgos, líderes de la organización y otros miembros relevantes del equipo, para corroborar que hay un entendimiento y una comprensión de los diversos tipos de riesgos mencionados.  Para establecer una definición precisa de Tolerancia la Riesgo, el auditor debe verificar los siguientes puntos:  **3.1.1 Establecimiento y Comunicación de Tolerancia al Riesgo**  Se debe asegurar que todos los miembros de la organización comprendan y estén comprometidos con los niveles de riesgo establecidos. La comunicación efectiva de la tolerancia al riesgo garantiza que todos los empleados, desde la alta dirección hasta el personal operativo, tengan una comprensión clara de los riesgos aceptables y no aceptables.   * ¿La documentación de gestión de riesgos aborda explícitamente la determinación y expresión de la tolerancia al riesgo organizacional? * ¿Existe en los informes de gestión de riesgos anteriores una evaluación y comunicación de los niveles de tolerancia al riesgo? (Estos informes pueden incluir información sobre los riesgos identificados, la evaluación de riesgos y las medidas de mitigación implementadas)   **3.1.2 Considerar la tolerancia al riesgo en la toma de decisiones**  Al evaluar cada decisión considerando la tolerancia al riesgo, se asegura que las opciones elegidas no comprometan la viabilidad y estabilidad de la organización. Esto ayuda a evitar situaciones de riesgo desmedido que podrían llevar a pérdidas financieras significativas, dañar la reputación de la organización o poner en peligro su capacidad para cumplir con sus objetivos.   * ¿La organización tiene un marco o metodología para incorporar la consideración de la tolerancia al riesgo en el proceso de toma de decisiones? * ¿Los registros de decisiones importantes muestran evidencia de la consideración de la tolerancia al riesgo?   **3.1.3 Monitoreo y revisión de tolerancia al riesgo**  El objetivo principal de tener procesos de monitoreo y revisión de la tolerancia al riesgo es asegurar que los límites de riesgo definidos sigan siendo relevantes y adecuados. El entorno empresarial es dinámico y está sujeto a cambios constantes, como avances tecnológicos, cambios regulatorios, fluctuaciones económicas o eventos imprevistos. Por lo tanto, es esencial que la organización evalúe periódicamente si sus niveles de tolerancia al riesgo siguen siendo apropiados para enfrentar los desafíos actuales y futuros.   * ¿Las políticas y procedimientos de gestión de riesgos establecen mecanismos para monitorear y revisar periódicamente la tolerancia al riesgo? * En los registros de monitoreo ¿se documentan las actividades realizadas, los resultados obtenidos y las acciones tomadas? * ¿Los informes de monitoreo y evaluación recopilan datos relevantes sobre los riesgos identificados y se utilizan para revisar y redefinir la tolerancia al riesgo? |