## Gestión de Indicadores

*Objetivo*

Establecer un marco para la gestión de indicadores de seguridad de la información en EMPRESA asegurando la monitorización, medición, análisis y evaluación efectivos del desempeño del SGSI.

*Alcance*

Este anexo se aplica a todos los empleados, directivos y partes interesadas involucradas en la gestión de la seguridad de la información en EMPRESA

*Marco normativo*

Norma ISO 27001:2022.

*Descripción*

Este procedimiento establece un marco para la gestión de indicadores de seguridad de la información en EMPRESA, conforme a ISO 27001:2022. Se aplica a la identificación, seguimiento, medición, análisis y evaluación de indicadores donde:

* la alta dirección aprueba KPIs y proporciona recursos;
* el responsable de seguridad coordina la gestión;
* los departamentos suministran datos;
* se identifican KPIs según ISO 27001:2022, se establecen métodos, calendario y responsabilidades. Se analizan resultados y se documenta evidencia.

Este procedimiento será revisado periódicamente para garantizar su adecuación y mejora continua.

A continuación, en la Tabla adjunta, se muestran los indicadores que se tendrán en cuenta para medir la eficacia de los controles de seguridad implantados por EMPRESA:

* **ID**. Nomenclatura establecida por EMPRESA para identificar el indicador.
* **Descripción del indicador**. Explicación del objetivo de medida de dicho indicador.
* **Control**. Definido en el Anexo A1.
* **Periodicidad**. Cada cuánto tiempo se debe recoger la medición.
* **Valor objetivo y valor umbral**. Cuál es el valor que sería correcto para la empresa y cuál es el valor por debajo del cual se debiera levantar una alarma.
* **Responsable de la medida**. Sobre qué cargo recae la responsabilidad de proporcionar el resultado de la medida.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Nombre** | **Descripción** | **Control**  **A1** | **Periodicidad** | **Valor objetivo/**  **Valor umbral** | **Responsable** |
|  |  |  |  |
| **IN1** | Políticas para la seguridad de la información | Verificar que se realiza la revisión de las políticas de seguridad por parte de la Dirección. | 5.1 | Anual | 2 / 1 | Comité de Seguridad |
| **IN2** | Roles y responsabilidades en seguridad de la información | Verificar si los roles y responsabilidades en cuanto a seguridad de la información están definidos. | 5.2 | Anual | 100% / 90% | Comité de Seguridad |
| **IN3** | Segregación de tareas | Verificar que se implementa la segregación de tareas para limitar el acceso a la información y evitar conflictos de interés. | 5.3 | Semestral | 100% / 95% | Comité de Seguridad |
| **IN5** | Inventario de información y otros activos asociados | Verificar la existencia y actualización del inventario de información y activos asociados. | 5.9 | Trimestral | 100% / 90% | Comité de Seguridad |
| **IN6** | Control de acceso | Verificar la efectividad de los controles de acceso implementados para proteger la información. | 5.15 | Mensual | 100% / 95% | Comité de Seguridad |
| **IN8** | Seguridad de la información en las relaciones con proveedores | Verificar que se cumplen los requisitos de seguridad de la información en las relaciones con proveedores. | 5.19 | Semestral | 100% / 90% | Comité de Seguridad |
| **IN9** | Identificación de requisitos legales, reglamentarios y contractuales | Verificar la identificación y cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con la seguridad de la información. | 5.31 | Anual | 100% / 95% | Comité de Seguridad |
| **IN12** | Copia de seguridad de la información | Verificar la realización y efectividad de las copias de seguridad de la información. | 8.13 | Semanal | 100% / 95% | Dpto. TI |
| **IN13** | Redundancia recursos de tratamiento de la información | Verificar la implementación y operatividad de la redundancia de recursos para asegurar la | 8.14 | Mensual | 100% / 95% | Dpto. TI |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | disponibilidad de la información. |  |  |  |  |
| **IN14** | Seguridad de redes | Verificar la efectividad de los controles de seguridad implementados en las redes de la empresa. | 8.20 | Trimestral | 100% / 95% | Dpto. TI |
| **IN15** | Seguridad de los servicios de red | Verificar la seguridad de los servicios críticos de red contra amenazas como el acceso no autorizado y el malware. | 8.21 | Mensual | 100% / 95% | Dpto. TI |
| **IN16** | Segregación de redes | Verificar la implementación y efectividad de la segregación de redes para limitar la exposición a amenazas. | 8.22 | Semestral | 100% / 95% | Dpto. TI |
| **IN17** | Filtrado webs | Verificar la implementación y operatividad del filtrado web para controlar y proteger el acceso a sitios potencialmente maliciosos o inseguros. | 8.23 | Mensual | 100% / 95% | Dpto. TI |

*Medios de divulgación*

El medio de comunicación por el cual se divulgará este documento será exclusivamente a través del correo electrónico asignado por la propia empresa.