Procedimiento de Gestión de Riesgos de Seguridad de la Información según ISO/IEC 27001:2013

Índice

1. Objetivo

El presente procedimiento tiene como objetivo establecer un marco estructurado y documentado para la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos relacionados con la seguridad de la información, en conformidad con la norma ISO/IEC 27001:2013. La finalidad es proteger la confidencialidad, integridad y disponibilidad de los activos de información y garantizar la continuidad del negocio.

2. Alcance

Este procedimiento aplica a todas las áreas, procesos, personas, tecnologías y activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización. Es de cumplimiento obligatorio para todos los empleados, contratistas y terceros que accedan a información crítica o sensible de la organización.

3. Evaluación de Riesgos de Seguridad de la Información

3.1 Criterios de Riesgo

La organización debe definir criterios para evaluar los riesgos de seguridad de la información. Estos criterios deben considerar:

- El nivel de impacto en caso de que se materialice una amenaza.

- La probabilidad de ocurrencia.

- El valor de los activos afectados.

- El apetito y la tolerancia al riesgo de la organización.

Se establecerán niveles (alto, medio, bajo) tanto para impacto como para probabilidad, y se utilizará una matriz de riesgo para obtener el nivel de riesgo resultante. Los criterios deben documentarse y revisarse periódicamente.

3.2 Identificación de Riesgos

La identificación de riesgos debe realizarse mediante un análisis sistemático de los procesos y activos incluidos en el SGSI. Se considerarán las amenazas potenciales (como accesos no autorizados, malware, desastres naturales, errores humanos) y las vulnerabilidades existentes (configuraciones débiles, falta de capacitación, obsolescencia tecnológica). Se asignará un dueño del riesgo a cada activo crítico, quien será responsable de su gestión.

3.3 Análisis de Riesgos

El análisis de riesgos debe evaluar:

- Las consecuencias potenciales de la materialización de un riesgo (pérdida económica, daño reputacional, sanciones legales).

- La probabilidad de ocurrencia del riesgo en función del entorno interno y externo.

El análisis puede realizarse de forma cualitativa (escalas subjetivas), cuantitativa (datos numéricos) o híbrida. Los resultados permitirán priorizar los riesgos según su nivel y criticidad.

3.4 Evaluación de Riesgos

Los niveles de riesgo identificados se compararán con los criterios de aceptación previamente definidos. Los riesgos se clasificarán en:

- Aceptables: no requieren tratamiento adicional.

- Aceptables con condiciones: requieren seguimiento o controles adicionales.

- No aceptables: requieren tratamiento inmediato.

El resultado de la evaluación se documentará en un informe de riesgos.

4. Tratamiento de Riesgos de Seguridad de la Información

4.1 Selección de Opciones de Tratamiento

Las opciones de tratamiento incluyen:

- Mitigar el riesgo mediante la implementación de controles.

- Transferir el riesgo (por ejemplo, mediante seguros o contratos).

- Evitar el riesgo eliminando la actividad que lo origina.

- Aceptar el riesgo si se considera dentro del umbral aceptable.

La selección se basa en un análisis costo-beneficio y en la criticidad del riesgo.

4.2 Determinación de Controles

Una vez seleccionada la opción de tratamiento, se identificarán los controles necesarios para aplicarla. Estos controles pueden ser técnicos, administrativos o físicos. Deben

alinearse con los objetivos del SGSI y ser comparados con los controles del Anexo A de la norma ISO/IEC 27001. Los controles omitidos deberán ser justificados.

4.3 Declaración de Aplicabilidad

Se generará un documento denominado 'Declaración de Aplicabilidad' (SoA), en el que se detallarán:

- Los controles seleccionados.

- Su estado de implementación.

- La justificación de su inclusión o exclusión.

La SoA es un documento vivo que debe mantenerse actualizado y estar disponible para auditorías internas o externas.

4.4 Planes de Acción y Aceptación del Riesgo Residual

Se definirán planes de acción para implementar los tratamientos seleccionados. Cada plan incluirá:

- Responsable del riesgo.

- Plazo de ejecución.

- Recursos necesarios.

- Indicadores de seguimiento.

Los riesgos que permanezcan tras el tratamiento (riesgos residuales) deberán ser formalmente aceptados por los propietarios del riesgo.

5. Revisión y Actualización

Este procedimiento debe revisarse al menos una vez al año o cada vez que se produzcan cambios significativos en:

- El contexto interno o externo de la organización.

- La infraestructura tecnológica.

- La legislación aplicable.

- Los resultados de auditorías o incidentes graves.

La mejora continua del SGSI debe incluir ajustes en la metodología de gestión de riesgos para garantizar su efectividad.

Bibliografía

Admin. (2023, 14 agosto). Análisis de riesgos en ciberseguridad - aggity. *aggity*. https://aggity.com/analisis-de-riesgo-ciberseguridad/

Normativa ISO/IEC 27005. (s. f.).

OTRS Group. (2024, 11 marzo). *SGSI – Sistema de Gestión de Seguridad de la Información | OTRS*. OTRS. https://otrs.com/es/casos-de-uso/sgsi/