**FORMATO REFERENCIAL PARA LA ELABORACIÓN DEL**

**INFORME DEL MONITOREO**

**DE DESEMPEÑO Y LOS INDICADORES DE GESTIÓN**

**(EGSI v3)**

**Tabla de contenido**

[1. Antecedentes 3](#_Toc185583105)

[2. Objetivo del documento 5](#_Toc185583106)

[3. Monitoreo, medición, análisis y evaluación del EGSI 5](#_Toc185583107)

[3.1. Objetivos 5](#_Toc185583108)

[3.2. Definición de Indicadores 5](#_Toc185583109)

[3.3. Establecimiento de Indicadores claves de gestión (KPIs) 6](#_Toc185583110)

[3.4. Resultados del Monitoreo 8](#_Toc185583111)

[3.5. Evaluación y Validación de Resultados 9](#_Toc185583112)

[3.6. Conclusiones y Recomendaciones del desempeño del EGSI 10](#_Toc185583113)

[4. Glosario de términos 10](#_Toc185583114)

[5. Documentos de referencia 10](#_Toc185583115)

[6. Firmas de responsabilidad 11](#_Toc185583116)

# Antecedentes

[INCLUIR EN CADA SECCIÓN, LA INFORMACIÓN QUE CORRESPONDE A SU INSTITUCIÓN; el texto del formato es una orientación para la elaboración de su propia documentación, que además requerirá de una investigación complementaria]

En esta sección se debe incluir el contexto necesario por el cual se realiza la actividad del monitoreo de los indicadores seleccionados en la fase de planificación. Cada uno de los objetivos descritos en el numeral **3.2. Declaración de los objetivos de seguridad de la información** del documento denominado **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN** deben tener indicadores susceptibles de medición capaz de realizar un seguimiento del desempeño hacia esos objetivos mediante la implementación de controles.

Este documento debe permitir analizar la evolución de los indicadores seleccionados en la fase de planificación del proceso de implementación del EGSI V3; esto es, por ejemplo: Reducción del riesgo de filtración de datos, Respuesta y manejo de incidentes de seguridad de la información, cumplir con los requisitos de otras normativas legales vigentes, como: Ley Orgánica de Protección de Datos Personales, otros.

*[Ejemplo:*

*Debido a la necesidad de gestionar la seguridad de la información acorde a la evolución normativa y tecnológica, considerando que actualmente los riesgos en seguridad de la información muestran continuos cambios, se desarrollan nuevas amenazas y se revelan vulnerabilidades e incidentes de seguridad que tienen efectos considerables en la sociedad; el Ministerio de Telecomunicaciones y de la Sociedad de la Información a través del Acuerdo Ministerial No. 2024-0003 expidió el Esquema Gubernamental de Seguridad de la Información -EGSI- (versión 3.0), el cual es de implementación obligatoria en las Instituciones del Sector Público.*

*En el ANEXO A: GUÍA PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN del ACUERDO Nro. MINTEL-MINTEL-2024-0003, se establece:*

*“(…)*

***Oficial de Seguridad de la Información (OSI)***

*La máxima autoridad designará al interior de su Institución a un funcionario como Oficial de Seguridad de la Información (OSI), será:*

*El responsable de la implementación y mejora continua del EGSI, así como el de coordinar las acciones del Comité de Seguridad de la Información en relación a la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información.*

 *El Oficial de Seguridad de la Información debe tener formación o especializado y con experiencia de al menos 2 años en áreas de seguridad de la información, ciberseguridad, de preferencia del nivel jerárquico superior, podrá ser el responsable del área de Seguridad de la Información (en el caso de existir) y no debe pertenecer a las áreas de procesos, riesgos, administrativo, financiero y tecnologías de la información.*

*Debe considerarse cualidades como: liderazgo, capacidad para lograr acuerdos, aceptación de sus pares, poder de gestión; son fundamentales para llevar con éxito la tarea de Oficial de Seguridad de la Información -OSI-.*

*Dentro de sus principales responsabilidades se encuentra:*

*(…)*

*o) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información y mejora continua (EGSI), así como las alertas que impidan su implementación:*

*• Plan de comunicación de los beneficios de la Seguridad de la Información*

*• Proponer objetivos de Seguridad de la Información*

***• Informe de resultados sobre indicadores medibles***

*• Propuestas de mejoras en la Seguridad de la Información*

*• Evaluación de recursos necesarios para la Seguridad de la Información.”*

*“****Comité de Seguridad de la Información (CSI)***

*La máxima autoridad designará al interior de la Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes haga sus veces: Planificación quien lo presidirá, Talento Humano, Administrativa, Comunicación Social, Tecnologías de la Información, Jurídica y el Delegado de protección de datos.*

*(…)*

*El Comité tendrá como principales responsabilidades:*

*a) Establecer los objetivos de la seguridad de la información, alineados a los objetivos institucionales.*

*b) Gestionar la implementación, control y seguimiento de las iniciativas relacionadas a seguridad de la información.*

*• Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).*

*• Realizar el seguimiento a los indicadores de gestión definidos, para el buen funcionamiento del EGSI.”*

*En este contexto en función de los objetivos de seguridad de la información de la institución “X”, se definieron los siguientes indicadores:*

* *Cantidad de capacitaciones ejecutadas*
* *Número de auditorías realizadas*
* *Tasa de Éxito en Pruebas de Phishing*

*…].*

# Objetivo del documento

En esta sección se debe definir el objetivo del Informe del monitoreo de desempeño y los indicadores de gestión.

*[Ejemplo:*

*Informar el resultado de las actividades planificadas, a través de la evaluación del desempeño de la seguridad de la información, que permite determinar qué tan bien los procesos dentro del ESGSI cumplen con sus especificaciones; y a través de la evaluación de la eficacia del Sistema de Gestión, que permite determinar en qué medida los objetivos de seguridad de la información se lograron. (…)]*

# Monitoreo, medición, análisis y evaluación del EGSI

En esta sección se debe establecer la metodología usada para lograr que los datos recolectados sean relevantes, confiables y útiles para la toma de decisiones.

## Objetivos

En esta sección se debe redactar los objetivos planteados para determinar el estado del sistema de gestión.

*[Ejemplo:*

* ***Fortalecer la construcción de la cultura organizacional*** *con base en la seguridad de la información para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, a todo el personal de la institución.*
* ***Asegurar que los procesos de seguridad de la información cumplen con los requisitos establecidos****, analizando los indicadores que proporcionan información sobre la efectividad de las medidas de seguridad implementadas, así como sobre áreas que requieren atención adicional para mejorar la protección de la información sensible y crítica institucional.*
* *Identificar áreas de mejora en la gestión de la seguridad de la información.*
* *Cumplir con normativas o marcos de referencia como: EGSI v3, ISO/IEC 27001, otros.*
* *(…)]*

## Definición de Indicadores

En esta sección se debe describir los indicadores alineados a los objetivos estratégicos de seguridad de la información de cada organización, considerando que deben ser: específicos, medibles, alcanzables, relevantes, temporales.

**NOTA**: Es conveniente tomar como referencia y revisar la norma técnica NTE INEN-ISO/IEC 27004 – Anexo B para la identificación de los diferentes tipos de indicadores que se puedan ajustar a cada institución.

*[Ejemplo:*

*Indicadores de Desempeño:*

* *INDICADOR 1: Cantidad de capacitaciones ejecutadas*
	+ ***Descripción****: Capacitación, entrenamiento y toma de conciencia. Total, de capacitaciones ejecutadas en un periodo determinado.*
	+ ***Propósito****: Medir el nivel de sensibilidad de los empleados frente al EGSI*
* *INDICADOR 2: Número de Auditorías Realizadas*
	+ ***Descripción****: Auditorías internas y externas. Total, de auditorías internas y externas realizadas en un período determinado.*
	+ ***Propósito****: Evaluar la efectividad del EGSI y la adherencia a normas y regulaciones.*
* *Porcentaje de Cumplimiento de Políticas*
* *Tiempo Promedio para Resolver Incidentes*
* *Costo Promedio por Incidente*

*Indicadores de Eficacia:*

* *Tasa de Éxito en Pruebas de Phishing Simuladas*
* *Índice de Satisfacción del Usuario*
* *Porcentaje de Iniciativas Empresariales Apoyadas por el SGSI*
* *Tasa de Reducción en Incidentes Repetidos*
* *Índice de cobertura de clasificación de datos.*

*(…)]*

## Establecimiento de Indicadores claves de gestión (KPIs)

En esta sección se debe establecer los indicadores claves de manera específica, considerando: fuentes de datos, recolección de datos, metas- umbrales, frecuencia, otros.

Además, considerar agrupar aquellos indicadores que **miden el desempeño** (medidas que expresan los resultados planificados en términos de las características de la actividad planificada, como el recuento de personas, el logro de hitos o el grado en que se han implementado los controles de seguridad de la información) y aquellos que **miden la eficacia** (medidas que expresan el efecto que la realización de las actividades planificadas tiene sobre los objetivos de seguridad de la información de la organización).

**NOTA**: En el Anexo 1 del presente documento se incluye una descripción de varios grupos de indicadores, que permiten establecer los indicadores claves de gestión.

*[Ejemplo:*

*Indicadores de Desempeño*

*INDICADOR 1: Cantidad de capacitaciones ejecutadas*

|  |  |
| --- | --- |
| **Número de indicador** | **1** |
| **Descripción del indicador** | Capacitación, entrenamiento y toma de conciencia |
| **Propósito del indicador** | Medir el nivel de sensibilidad de los funcionarios frente al SGSI |
| **Cláusulas o controles asociados (EGSI V3)** | 2.3 Concienciación, educación y formación en seguridadde la información |
| PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado |
| **Partes Responsables** | Dirección de Talento humano, Oficial de Seguridad de la Información |
| **Formula** | Cantidad de capacitaciones programadas / capacitaciones ejecutadas |
| **Escala** | Porcentaje |
| **Nivel para el cumplimiento / meta** | 80% |
| **Frecuencia de medición** | Anual |
| **Fuente de datos** | Programa de capacitaciones y/o entrenamiento. |
|  |  |
| Medición |
| Cantidad de capacitaciones programadas | 15 |
| capacitaciones ejecutadas | 13 |
| **NIVEL DE CUMPLIMIENTO** | **87%** |

*INDICADOR 2: Número de auditorías realizadas*

|  |  |
| --- | --- |
| **Número de indicador** | **2** |
| **Descripción del indicador** | Auditorías internas y externas |
| **Propósito del indicador** | Evaluar la efectividad del EGSI y la adherencia a normas y regulaciones |
| **Cláusulas o controles asociados (EGSI V3)** | PLANEACIÓN: 0.4 Plan de evaluación Interna, documentado y aprobado |
| EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado |
| 1.35. Revisión independiente de seguridad de la información |
| **Partes responsables** | Comité de Seguridad de la Información, Oficial de Seguridad de la Información, Equipo de Evaluación. |
| **Fórmula** | Número de auditorías realizadas / Número de auditorías planificadas |
| **Escala** | Porcentaje |
| **Nivel para el cumplimiento / meta** | 60% |
| **Frecuencia de medición** | Anual |
| **Fuente de datos** | Programa de auditoría e informes de auditoría |
|  |  |
| Medición |
| Número de auditorías planificadas | 2 |
| auditorías realizadas | 1 |
| **NIVEL DE CUMPLIMIENTO** | **50%** |

*Indicadores de Eficacia*

*INDICADOR 3: Tasa de Éxito en Pruebas de Phishing*

|  |  |
| --- | --- |
| **Número de indicador** | **3** |
| **Descripción del indicador** | Tasa de Éxito en Pruebas de Phishing Simuladas |
| **Propósito del indicador** | Evaluar si el personal de la organización reacciona de manera adecuada a los ataques de ingeniería social. |
| **Cláusulas o controles asociados (EGSI V3)** | PLANEACIÓN: 0.3 Plan de Comunicación y Sensibilización, documentado y aprobado |
| EJECUCIÓN: 0.11 Informe de la evaluación interna del EGSI v3, documentado y aprobado |
| 1.35. Revisión independiente de seguridad de la información |
| **Partes responsables** | Dirección de Tecnologías de la Información, Oficial de Seguridad. |
| **Fórmula** | Número de miembros de la organización que no dieron clic en el enlace /Número de miembros de la organización que participaron en la prueba |
| **Escala** | Porcentaje |
| **Nivel para el cumplimiento / meta** | 80% |
| **Frecuencia de medición** | Semestral |
| **Fuente de datos** | Herramienta automatizada de pruebas de phishing |
|  |  |
| Medición |
| Número de miembros de la organización que dieron clic en el enlace | 40 |
| Número de miembros de la organización que participaron en la prueba | 100 |
| **NIVEL DE CUMPLIMIENTO** | **40%** |

*(…)]*

## Resultados del Monitoreo

En esta sección los resultados deben presentarse en un formato claro, generalmente utilizando tablas y gráficos que faciliten la visualización.

*[Ejemplo:*

|  |
| --- |
| **ESTADO DE LOS INDICADORES** |
| Descripción | Medido | Meta |
| Indicador 1: Cantidad de capacitaciones ejecutadas | 87% | 80% |
| Indicador 2: Número de auditorías realizadas | 50% | 60% |
| Indicador 3: Tasa de Éxito en Pruebas de Phishing | 40% | 80% |
| Indicador 4: Indicador 4 | 0% | 80% |
| Indicador 5: Indicador 5 | 0% | 80% |
| Indicador 6: Indicador 6 | 0% | 85% |
| Indicador 7: Indicador 7 | 0% | 85% |
| Indicador 8: Indicador 8 | 0% | 85% |
| Indicador 9: Indicador 9 | 0% | 85% |
| Indicador 10: Indicador 10 | 0% | 85% |

*]:*

## Evaluación y Validación de Resultados

En esta sección se debe comparar con períodos anteriores, a fin de identificar tendencias y patrones. Además, realizar un análisis de causa raíz, para los indicadores que no alcanzaron sus metas.

*[Ejemplo:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Indicador*** | ***Meta*** | ***Valor actual*** | ***Valor anterior (inicial)*** | ***Tendencia*** | ***Observaciones*** |
| *Cantidad de capacitaciones programadas* | *80%* | *87%* | *50%* | *Superado* | *Se ha logrado ejecutar más del 80% de las capacitaciones programadas* |
| *Número de auditorías realizadas* | *60%* | *50%* | *0%* | *Mejorando* | *Se ha logrado ejecutar parte del plan de auditorías*  |

*]:*

## Conclusiones y Recomendaciones del desempeño del EGSI

En esta sección se debe concluir con un resumen del desempeño general del Sistema de Gestión (EGSI v3), destacando logros significativos y áreas que requieren atención, tomando como referencia los ítems 3.4 & 3.5.

*[Ejemplo:*

*Conclusiones:*

* *El análisis realizado sobre el desempeño del Esquema Gubernamental de Seguridad de la Información (EGSI V3), se ha observado el cumplimiento del plan de formación continua del personal en temas de seguridad; sin embargo, ha expuesto varios aspectos críticos que requieren atención inmediata, por ejemplo: se identificaron deficiencias significativas en la formación del personal, lo que expone a la organización a riesgos innecesarios, como la baja capacidad del equipo para responder ante incidentes y adoptar buenas prácticas en el manejo de información sensible.*
* *El compromiso con estos aspectos es necesario para garantizar una protección efectiva de los activos informáticos y cumplir con las normativas vigentes.*
* *(…)*

*Recomendaciones:*

* *Mantener el Plan de Capacitación actualizado y reforzar la capacitación en diferentes temas de seguridad de la información para todos los miembros de la organización.*
* *Revisar y actualizar el plan de auditorías/evaluación interna, este debe cumplirse en su totalidad a fin de obtener los resultados esperados.*
* *(…)*

*]*

# Glosario de términos

|  |  |
| --- | --- |
| Término | Definición |
| **EGSI** | Esquema Gubernamental de Seguridad de la Información |
| **KPI** | Indicadores Claves de Gestión |

# Documentos de referencia

En esta sección incluir las referencias documentales o normativas usadas para la elaborar el informe.

*[Ejemplo:*

* *Acuerdo Ministerial Nro. 2024-0003.*
* *Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)*
* *Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, NTE INEN-ISO/IEC 27002, NTE INEN-ISO/IEC 27003, NTE INEN-ISO/IEC 27004, NTE INEN-ISO/IEC 27007*
* *(…)*

*]*

# Firmas de responsabilidad

|  |  |  |
| --- | --- | --- |
|  | Nombre/Cargo | Firma |
| **Elaborado por:** | Quién elaboró el documento |  |
| **Revisado por:** | Quién revisó el documento |  |
| **Aprobado por:** | Quién aprobó el documento |  |

# Control de versiones del formato referencial

|  |  |
| --- | --- |
| **Versión**: | 1.0 |
| **Fecha de la versión**: | 20-12-2024 |
| **Creado por**: | Dirección de Infraestructura, Interoperabilidad, Seguridad de la Información y Registro Civil |
| **Aprobado por**: | Subsecretaría de Gobierno Electrónico y Registro Civil |
| **Nivel de confidencialidad**: | Bajo |

# Historial de cambios del formato referencial

|  |  |  |
| --- | --- | --- |
| **Versión** | **Fecha** | **Detalle del cambio** |
| 1.0 | 20/12/2024 | Emisión inicial del documento |

**ANEXO 1:**

# Indicadores de Gestión referenciales del Esquema Gubernamental de Seguridad de la Información

A continuación, se agrupan distintos indicadores que permiten evaluar la efectividad de un Sistema de Gestión de Seguridad de la Información (para el caso del sector público ecuatoriano el EGSI v3). A continuación, se presentan ejemplos de indicadores relevantes que pueden ayudar a las instituciones a medir su desempeño en este ámbito:

## Plan de sensibilización (Entrenamiento y concientización en Seguridad de la Información)

Corresponde al nivel del cumplimiento del Plan de sensibilización y capacitaciones en materia de Seguridad de la Información. Identificar aquellos puntos de mejora, como también los resultados de las evaluaciones y auditorías a los cuales ha sido sometido el personal para medir su respuesta.

Entre los indicadores que se puede seleccionar, se hacen constar los siguientes:

* **Cantidad de capacitaciones:** Total de capacitaciones ejecutadas al interior de la institución en un periodo determinado.
* **Porcentaje de empleados capacitados:** Porcentaje de empleados que completaron la capacitación de seguridad de la información requerida.
* **Índice de éxito de las simulaciones de phishing:** porcentaje de empleados que no aprobaron las simulaciones de phishing (cuanto menor sea el índice, mejor).
* **Número de capacitaciones especializadas para del área de Seguridad Informática.**

## Resultados a las auditorías del Sistema de Gestión de Seguridad de la Información (SGSI)

Corresponde a las auditorías internas o externas realizadas al cumplimiento de los requisitos o los controles de seguridad del Sistema de Gestión, durante el período de tiempo del reporte, que incluya hallazgos claves y las acciones correctivas necesarias.

Entre los indicadores que se pueden seleccionar para medir y evaluar este aspecto, se hacen constar los siguientes:

* **Número de auditorías realizadas:** Auditorías internas y externas. Total de auditorías internas y externas realizadas en un período determinado.
* **No conformidades de auditoría:** Número de no-conformidades identificadas en auditorías internas o externas.
* **Tasa de cumplimiento de la política:** Porcentaje de usuarios, unidades o departamentos que cumplen con las políticas de seguridad.
* **Efectividad de los controles de seguridad:** Porcentaje de controles evaluados como efectivos durante las auditorías.

## Estructura Organizacional de Seguridad en la Información en la institución

Corresponde a todas las gestiones y actos administrativos que han dado lugar a formar una estructura de Seguridad de la Información en la institución (designación del Oficial de Seguridad, Comité de Seguridad de la Información, Implementación de una Unidad de Seguridad de la Información de ser el caso).

Entre los indicadores que se pueden seleccionar para medir y evaluar este aspecto, se hacen constar los siguientes:

* **Asignación de recursos:** Medición del recurso humano, hardware, software y servicios dentro del presupuesto anual destinado a Seguridad de la Información.
* **Número de reuniones del Comité de Seguridad de la Información.** Permite medir el cumplimiento de la norma que indica al menos 1 reunión bimestral de dicho comité.

## Activos de Información

Corresponde a la medición de aquellas actividades, políticas, procedimientos y metodologías que evidencien la identificación y clasificación de los activos de información, así como las actividades enmarcadas en la evaluación de riesgos; esto es: identificación de riesgos, estado de tratamiento y cualquier cambio en el panorama de riesgos.

Entre los indicadores que pueden aportar a la medición del EGSI en este aspecto se hace constar el siguiente:

* **Exposición al riesgo:** Cantidad de riesgos altos y medios más allá del umbral aceptable.
* **Índice de cobertura de clasificación de datos*:*** Porcentaje de activos de datos críticos con clasificación y protección adecuadas.
* **Porcentaje de sistemas de información críticos sobre los cuales se ha ejecutado pruebas de penetración o evaluación de vulnerabilidades desde su última actualización importante.**

## Tratamiento de eventos de seguridad de la información

Corresponden aquellos indicadores de Gestión que hacen referencia a la Respuesta y Manejo de Incidentes de Seguridad de la Información. Entre algunos de los indicadores que se puede seleccionar se mencionan los siguientes:

* **Tiempo de respuesta de incidentes:** Tiempo promedio para la detección, respuesta y resolución de incidentes.
* **Número de incidentes de seguridad:** Número total de incidentes de seguridad reportados y resueltos en un período de tiempo.
* **Porcentaje de incidentes resueltos en el punto de contacto inicial:** útil para mesas de ayuda o SOC.

## Políticas de Integridad de la Información

Corresponden los indicadores que permiten evaluar las medidas implementadas para preservar la integridad de la información en la institución. Entre algunos de los indicadores que se puede seleccionar se mencionan los siguientes:

* **Frecuencia de actualizaciones de los sistemas de respaldo (backups):** Frecuencia con la que se realizan y verifican copias de seguridad.
* **Cumplimiento de las políticas de control de cambios:** Porcentaje de los cambios realizados en sistemas o datos que cumplen con los procedimientos de gestión de cambios documentados.

## Políticas de Disponibilidad de la Información

Corresponde a aquellos indicadores que permiten evaluar las medidas implementadas para asegurar un nivel de disponibilidad de los servicios críticos institucionales enmarcados en los SLA (Acuerdo de Nivel de Servicio) acordados con la comunidad objetivo y/o de atención. Entre algunos de los indicadores que se puede seleccionar se mencionan los siguientes:

* **Disponibilidad de los servicios de TI vs. el tiempo de inactividad máximo definido.**
* **Número de mantenimientos ejecutados vs. Planificados**.
* **Número de equipos que cuentan con la protección de antivirus vs. Número total de equipos institucionales.**

## Control de acceso (Políticas de Confidencialidad de la Información)

Corresponde a aquellos indicadores que permiten evaluar la existencia y la aplicación de procedimientos relacionados con el acceso a los recursos y sistemas de información en la institución; esto implica el acceso físico a instalaciones y dispositivos; así como también el acceso lógico a redes, sistemas informáticos y bases de datos. Además se deberá evaluar el cumplimiento de acuerdos con terceras partes que acceden a la información institucional.

Entre los indicadores que se pueden seleccionar, se hacen constar los siguientes:

* **Tasa de violación de control de accesos:** Número de accesos no autorizados a un recurso detectados en el período del reporte.
* **Revisiones de accesos privilegiados completados:** Porcentaje de revisiones de acceso privilegiado completadas según lo programado.
* **Número de afectaciones a las bases de datos autorizadas y documentadas:** Un número bajo de estas afectaciones indica que los datos son confiables y por ende hay reducción en la interrupción de las actividades operativas.
* **Porcentaje promedio de los requisitos de seguridad relevantes tratados en acuerdos con terceras partes:** Porcentaje de cláusulas de seguridad de la información que se dan cumplimiento y seguimiento en los acuerdos de confidencialidad.

## Adquisición y actualización de software

Corresponden a aquellos indicadores que permiten evaluar aquellas acciones, actividades, procedimientos y políticas implementadas en la institución con el objetivo de proteger la infraestructura tecnológica institucional en la cual se hará constar también las acciones efectuadas para el manejo de las vulnerabilidades técnicas.

Entre los indicadores que se pueden seleccionar para medir y evaluar este aspecto, se hacen constar los siguientes:

* **Tiempo parcheo de vulnerabilidades:** Tiempo promedio para el parcheo de vulnerabilidades después de ser identificadas.
* **Tasa de recurrencia de vulnerabilidad:** Porcentaje de vulnerabilidades previamente resueltas que vuelven a ocurrir.
* **Tasa de parcheo:** Porcentaje de sistemas o equipos que han sido parchados ante una vulnerabilidad declarada.

## Cumplimiento de políticas

Corresponde a los indicadores que permiten medir el cumplimiento y verificar la aplicación efectiva del marco jurídico de políticas de seguridad de la información (Ley Orgánica de Protección de Datos Personales, Ley de Comercio Electrónico, Firmas y Mensajes de datos, otras), cumplimiento de estándares relevantes (ej. NTE-ISO/IEC 27001, otros), requerimientos legales y políticas internas.

Entre los indicadores que se pueden seleccionar para medir y evaluar este aspecto, se hacen constar los siguientes:

* **Frecuencia de actualización de políticas internas:** Intervalo con el que se actualizan las políticas internas para adaptarse a cambios en leyes o normativas.
* **Porcentaje de cumplimiento de requerimientos de protección de datos:** Proporción de requerimientos cumplidos vs. los requerimientos de la LOPDP.