Guía de Evaluación del Desempeño

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 16

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	16/02/2017	Versión inicial del documento

TABLA DE CONTENIDO

1. DERECHOS DE AUTOR

2. AUDIENCIA

Este documento está elaborado para las entidades públicas de orden nacional, entidades públicas del orden territorial y entidades privadas que deseen una guía para implementar las políticas planteadas en el Modelo de Seguridad de la Información, así como proveedores de servicios de Gobierno en Línea y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la Información en el marco del Programa Gobierno en Línea.

3. INTRODUCCIÓN

El modelo de Seguridad y Privacidad de la Información cuyo propósito es servir como guía para la mejora de los estándares de Seguridad de la Información de las Entidades, cuenta con 5 fases para la gestión de la Seguridad y Privacidad de la información de las Entidades.

la fase de ***Evaluación de Desempeño*** es la fase donde se establecen los aspectos a ser desarrollados por los responsables de la gestión de seguridad de la información en todos los niveles de la entidad, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

4. PROPÓSITO

El propósito de este documento es ofrecer una guía de recomendaciones para la correcta evaluación del desempeño de la Seguridad y Privacidad de la Información de la Entidad que previamente ha planeado, implementado y gestionado el MSPI.

5. EVALUACION DEL DESEMPEÑO

5.1. REVISION Y SEGUIMIENTO DEL MSPI

En la definición del Modelo de Seguridad y Privacidad de la Información, la fase de evaluación del desempeño hace parte de la etapa de Verificar, donde se establecen los aspectos a ser desarrollados por los responsables de la gestión de seguridad y privacidad de la información en todos los niveles, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

Para el cumplimiento de esta fase, la organización deberá desarrollar un conjunto de actividades de seguimiento donde se mantenga de manera continua la medición y verificación del cumplimiento de los aspectos planteados en la fase de Planificación del modelo y la forma como estas actividades se han ido desarrollando o ejecutando.

Cabe notar, que estos aspectos de seguimiento y revisión deberán ser desarrollados con base en los resultados obtenidos; y se deberán ajustar los aspectos necesarios para que la seguridad y privacidad de la información sea eficiente y eficaz en el cumplimiento de los objetivos y metas trazados en la fase de planificación.

Para la fase de seguimiento y revisión las actividades detalladas a continuación, tendientes a la definición de procedimientos operacionales documentados.

5.1.1. REVISIÓN

Se deben llevar a cabo las siguientes actividades de revisión:

- De la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.

- De la evaluación de los riesgos desarrollada en la entidad, donde a su vez se validen los niveles aceptables de riesgo y el riesgo residual después de la aplicación de controles y medidas administrativas.

5.1.2. SEGUIMIENTO

Se deben llevar a cabo actividades para realizar seguimiento a:

- La programación y ejecución de las actividades de auditoria interna del MSPI
- La programación y ejecución de las revisiones por parte del encargado de seguridad y privacidad de la información.
- El alcance del MSPI y las mejoras del mismo.
- Los planes de seguridad tanto para el establecimiento como la ejecución y actualización de los mismos, como respuesta a los aspectos identificados a nivel de las revisiones y seguimientos realizados en esta fase de implementación.
- A los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o el desempeño de la seguridad y privacidad de la información.

5.2. ACTIVIDADES GENERALES DE SEGUIMIENTO Y REVISIÓN

Las siguientes son las actividades generales que soportan la etapa de Evaluación del Desempeño del MSPI:

- Revisión de la eficacia del MSPI.
- Medición de la efectividad de Controles.
- Revisión de las valoraciones de los riesgos.
- Medición de los indicadores de gestión del MSPI.
- Realización de auditorías.
- Revisiones del MSPI por parte de la dirección.
- Actualizar los planes de seguridad.
- Registro de las actividades del MSPI.
- Revisiones de Acciones o Planes de Mejora (Respuesta a no conformidades).

Desde el punto de vista del desarrollo de estas actividades, su cumplimiento deberá estar enmarcado en el modelo PHVA al interior de los procesos, donde se integran los aspectos de la gestión de la organización que establece para las etapas de verificación las siguientes tareas:

- Consolidar indicadores periódicamente.
- Evaluar indicadores frente a las metas.
- Graficar los Indicadores.
- Analizar causas de las desviaciones.
- Evaluar las No Conformidades ocurridas y su impacto en el cumplimiento de las metas y objetivos del MSPI.

5.3. DOCUMENTACIÓN DE LA ETAPA DE EVALUACIÓN DEL DESEMPEÑO

En esta etapa se definen las actividades que permiten medir el avance de los elementos definidos en la etapa anterior, se deben generar o actualizar los siguientes documentos necesarios para el MSPI:

- Revisión de la eficiencia del MSPI
- Medición de efectividad de controles
- Revisión de valoraciones de riesgos
- Realización de auditorías internas
- Revisiones del MSPI por la dirección
- Actualización de los planes de seguridad
- Registro de actividades del MSPI
- Revisiones de acciones o planes de incidentes

5.4. EJEMPLO DE PROCEDIEMITO DE EVALUACIÓN DEL DESEMPEÑO DEL MSPI

A continuación, se da un ejemplo de cómo deberían ser los procedimientos para realizar la evaluación de desempaño del MSPI.

NOMBRE	REVISIÓN DE LA EFICACIA DEL MSPI
Objetivo	Revisión de la eficacia del MSPI de tal forma que la Entidad tome las acciones necesarias para mejorar el sistema, y en consecuencia la seguridad de los activos de información.
Alcance	Controles de seguridad y medidas establecidas en el marco de tratamiento de riesgos de seguridad de la información para los activos definidos en el alcance del MSPI.
Descripción	La eficacia del MSPI incluye el cumplimiento de la política y objetivos del MSPI, y la revisión de los controles de seguridad, teniendo en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
Entradas	- Política de seguridad y Objetivos del MSPI. - Informes de auditoría anteriores. - Informes de incidentes de seguridad y medidas implementadas. - Informes de planes de mejoramiento ejecutados. - Indicadores definidos.
Salidas	- Informe de resultados de eficacia del MSPI.
Actividades	- Identificar la política y objetivos del MSPI. - Recolección de resultados de auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas. - Recolección y Consolidación de indicadores de cumplimiento definidos para el MSPI. - Evaluar indicadores frente a las metas de cumplimiento definidas y compararlos con los resultados identificados previamente. - Graficar los indicadores. - Analizar causas de las desviaciones. o Si es debido a un problema: Aplicar modelo PHVA para análisis de problemas.

	- Preparar informes de efectividad para la alta dirección
Frecuencia	(a consideración de la entidad "es recomendable Bimestral")
Indicadores	Evaluación de la efectividad de los controles definidos para cada riesgo.
Roles y Responsabilidades	1) Alta Dirección a) Establecimiento y aprobación de la política general de seguridad en la Entidad, del MSPI y los objetivos a ser alcanzados. b) Demostrar Compromiso con el MSPI. 2) Oficial de Seguridad de la Información o quien haga sus veces y equipo de trabajo. a) Mantener actualizado el procedimiento. b) Definir y coordinar con los administradores de los componentes tecnológicos los aspectos a evaluar de cada sistema de información y controles los eventos a auditar. c) Definir los indicadores para los controles y la forma de tomar la medición. d) Programación de pruebas específicas periódicas sobre los controles. e) Seguimiento y participación en las pruebas a controles. f) Revisión de resultados de auditorías e incidentes. 3) Control Interno. a) Programar revisiones internas del MSPI. b) Generar informes de auditoría del MSPI. c) Generar planes de mejoramiento de acuerdo a los resultados de auditorías de seguridad. 4) Grupo de Sistemas: Soporte/ Administradores de Plataforma y BD / Desarrolladores. a) Activar/Preparar Logs de auditoría en los Componentes Tecnológicos. b) Revisar en forma periódica los Logs de eventos registrados en cada componente de la plataforma tecnológica c) Clasificar los eventos de seguridad detectados como eventos de criticidad alta, media o baja. (***depende de la clasificación de incidentes al interior de la entidad***) d) Clasificar y depurar periódicamente, la información registrada en los Logs de Auditoría.

	5) Todos los usuarios a) Utilizar el sistema de reporte de incidentes de seguridad (***Depende de la metodología usa en la entidad para gestionar los incidentes***). b) Reportar actividades sospechosas/extrañas que puedan afectar la seguridad de la información.
Relaciones con procedimientos	- Gestión de incidentes (***Depende de la metodología de gestión de incidentes***) - Registro de No Conformidades (Calidad y Seguridad)
Observaciones	Las actividades de medición de los controles deberán estar enmarcado en las actividades del día a día, donde las áreas de administración de los controles (Tecnológicos, Administrativos) registrarán el avance.