Fecha: 21-12-2012

Actualización medios de verificación: 28-12-2012

Pauta de Validación Técnica PMG/MEI 2012

Marco:	Marco Básico
Sistema:	Seguridad de la Información
Red de Experto:	Dirección de Presupuestos / Subsecretaría de Interior

<table>
<tr><th colspan="3">ETAPA I</th></tr>
<tr><th>Etapa</th><th>Pregunta</th><th>Medios de Verificación</th></tr>
<tr><td>1</td><td>1. ¿En el diagnóstico vigente al 31 de diciembre del 2012, la Institución realizó correctamente la selección de los procesos de provisión de bienes y servicios más relevantes (productos estratégicos declarados en el Formulario de Definiciones Estratégicas 2012-2014 A1), fundamentándola en base a los siguientes criterios de selección:
• Porcentaje dotación asociado al proceso,
• Alcance geográfico,
• Frecuencia de aplicación del proceso,
• Porcentaje del presupuesto asociado al proceso,
• Porcentaje de ciudadanos / clientes / usuarios / beneficiarios que reciben el producto del proceso?</td><td>- Formulario A1 de Definiciones Estratégicas 2012-2014
- Planilla Instrumentos 2012
- Oficio del Jefe de Servicio con fundamentación del Alcance</td></tr>
<tr><td>1</td><td>2. ¿Identifica correctamente activos de Información[1] para cada uno de sus procesos seleccionados, señalando su nivel de criticidad[2]?</td><td>- Planilla Instrumentos 2012</td></tr>
<tr><td>1</td><td>3. ¿La institución presenta un análisis de los riesgos de seguridad de los activos de información con criticidad media y alta?</td><td>- Planilla Instrumentos 2012</td></tr>
<tr><td>1</td><td>4. ¿Para los riesgos de seguridad de los activos de información con criticidad media y alta, se, se asocian correctamente los controles de la NCh-ISO 27001 que permitan mitigarlos, se declara su cumplimiento y de corresponder, su medio de verificación?</td><td>- Planilla Instrumentos 2012
- Medios de verificación para los siguientes controles que se declare cumplido, cuando corresponda:
<table>
<tr><th>Dominio</th><th>Ámbito</th><th>Control</th><th>Productos esperados y sus contenidos</th></tr>
<tr><td>Gestión de las comunicaciones y operaciones</td><td>Redes</td><td>A.10.6.1</td><td>Política/Procedimiento/Normativa de la Red que contenga a lo menos:
1. Alcance de las redes y Diagrama de red.
2. Definición de mecanismos de protección.
3. Segmentación de redes.
4. Segregación de funciones en redes y plataformas.</td></tr>
<tr><td>Control de acceso</td><td>Control de Acceso</td><td>A.11.2.2</td><td>Procedimiento y/o Normativa para la asignación y restricción del uso de privilegios.</td></tr>
<tr><td>Adquisición, desarrollo y mantenimiento de los sistemas de información</td><td>Desarrollo</td><td>A.12.5.1</td><td>Procedimientos y/o Formularios de Control del Cambios de Desarrollo.</td></tr>
</table></td></tr>
</table>

[1] Para activos de tipo documento, formulario, expediente, base de datos, software, sistema, equipos, infraestructura y persona.

[2] "Nivel de Criticidad": es alto, medio o bajo en función del grado de Confidencialidad, Integridad y Disponibilidad del activo de información.

<table>
<tr><th colspan="3">ETAPA II</th></tr>
<tr><th>Etapa</th><th>Pregunta</th><th>Medios de Verificación</th></tr>
<tr><td>2</td><td>5. ¿La institución, al 31 de diciembre de 2012, cuenta con una política de seguridad de la información aprobada por el Jefe Superior del Servicio, está nombrado un encargado de seguridad de la información y constituido el Comité de Seguridad?</td><td>- Resolución que aprueba la Política de Seguridad
- Resolución de Nombramiento Encargado de Seguridad
- Documento formal donde conste la constitución del Comité de Seguridad</td></tr>
<tr><td>2</td><td>6. ¿La institución presenta un Plan General de Seguridad de la Información que contenga los siguientes elementos:
• Acciones para el tratamiento de los riesgos de los activos con criticidad media y alta,
• Indicadores de desempeño para medir la efectividad de los controles o requisitos normativos a implementar, y
• Responsables de la implementación de los productos establecidos en el Plan?</td><td>- Planilla Instrumentos 2012</td></tr>
<tr><td>2</td><td>7. ¿La institución presenta un Programa de Trabajo Anual, coherente con el Plan General, que contiene al menos los siguientes elementos:
• Hitos,
• Actividades,
• Plazos,
• Responsables, y
• Actividades de difusión, sensibilización o capacitación a los funcionarios?</td><td>- Planilla Instrumentos 2012</td></tr>
<tr><th colspan="3">ETAPA III</th></tr>
<tr><th>Etapa</th><th>Pregunta</th><th>Medios de Verificación</th></tr>
<tr><td>3</td><td>8. ¿La institución cumple con el programa de trabajo comprometido para el período; y/o presenta justificación válida para aquellas actividades no cumplidas, canceladas o prorrogadas para el período siguiente; y presenta los resultados de los indicadores de desempeño definidos para medir la efectividad de los controles implementados?</td><td>- Planilla Instrumentos 2012
- Medios de verificación para los siguientes controles que se declare cumplido, cuando corresponda:
<table>
<tr><th>Dominio</th><th>Ámbito</th><th>Control</th><th>Productos esperados y sus contenidos</th></tr>
<tr><td>Gestión de las comunicaciones y operaciones</td><td>Redes</td><td>A.10.6.1</td><td>Política/Procedimiento/Normativa de la Red que contenga a lo menos:
1. Alcance de las redes y Diagrama de red.
2. Definición de mecanismos de protección.
3. Segmentación de redes.
4. Segregación de funciones en redes y plataformas.</td></tr>
<tr><td>Control de acceso</td><td>Control de Acceso</td><td>A.11.2.2</td><td>Procedimiento y/o Normativa para la asignación y restricción del uso de privilegios.</td></tr>
<tr><td>Adquisición, desarrollo y mantenimiento de los sistemas de información</td><td>Desarrollo</td><td>A.12.5.1</td><td>Procedimientos y/o Formularios de Control del Cambios de Desarrollo.</td></tr>
</table></td></tr>
<tr><th colspan="3">ETAPA IV</th></tr>
<tr><th>Etapa</th><th>Pregunta</th><th>Medios de Verificación</th></tr>
<tr><td>4</td><td>9. ¿La institución realizó un análisis del avance de los dominios de seguridad implementados, y presenta, para el período siguiente, recomendaciones de mejora (medidas correctivas y/o preventivas); establece revisiones regulares a la operación del sistema, cuando corresponda, y realiza difusión de resultados de la implementación?</td><td>- Planilla Instrumentos 2012
- Informe de Revisión del Comité de Seguridad de la Información (un archivo que incluye Acta de Comité de Seguridad e informes de evaluación que fueron revisado por el Comité y señalados en dicha acta).
- Un archivo con evidencia difusión de los resultados de la implementación</td></tr>
</table>