ANEXO 4:

DOCUMENTO ESTÁNDAR DE UNA POLÍTICA DE SEGURIDAD

DOCUMENTO ESTÁNDAR DE UNA POLÍTICA DE SEGURIDAD

Una política de seguridad debe tener una estructura dividida en secciones. Cada sección debería incorporar como mínimo los cuatro aspectos siguientes:

1. Un resumen de la declaración del tema que se toca en ese punto, esta declaración indica que se realiza sin indicar el como se realiza
2. Identificación de la persona o comisión responsable de determinar y aprobar la Política de Seguridad
3. Identificación de la persona o comisión responsable de implementar la Política de Seguridad.
4. Referencias sobre los documentos de soporte o apoyo sobre las que se basa la Política de Seguridad, tales como guías de implementación, políticas relacionadas, etc.

Secciones:

1. Organización.
   Explica en términos generales, los diferentes aspectos relativos a la organización de procedimientos y roles que componen el sistema de seguridad de la institución.
   Describe toda relación existente con otras instituciones o servicios en materia de seguridad.
   Establece a la persona o comisión responsable de realizar evaluación, monitoreo o auditorías en temas se seguridad.

2. Evaluación de riesgos.
   Esta sección describe de manera general (sin revelar vulnerabilidades) la evaluación y el tratamiento de riesgos para los cuales la política de seguridad establece controles con el objetivo de reducir el impacto de estos riesgos y la frecuencia con la que pueden ocurrir.

3. Control de Acceso.
   Establece las políticas de acceso a documentos sensibles tanto electrónicos como manuscritos, así como el acceso a los ambientes donde se almacena y/o procesa la información.
   Define la clasificación de la información de acuerdo a la importancia de la misma.
   Establece el tipo de personal debe tener acceso tanto a la información como a los activos de la entidad.

4. Seguridad de Personal (relacionado con seguridad TI).
   Describe en términos generales los métodos de verificación de datos y antecedentes, así como los perfiles considerados para la selección tanto del personal que ocupa roles de confianza, incluyendo al Responsable de Seguridad.
   Detalla las responsabilidades del personal, así como los medios y mecanismos de comunicación y capacitación.

5. Seguridad Física.
   Establece de manera general los elementos que integran la seguridad física tales como alarmas de seguridad física, cerco perimetral, guardias, eliminación de material en desuso, llaves, etc.
   Establece de manera general los procedimientos para asegurar la seguridad física .

6. Seguridad de Comunicaciones y Redes.
   Especifica los objetivos de la seguridad de comunicaciones y redes.
   Establece de manera general las medidas de seguridad en el tema de comunicaciones y redes tanto a nivel interno como a nivel externo.
   Describe el mecanismo de aprobación de las políticas de seguridad en tema de comunicaciones y redes.
   Indica los requerimientos de seguridad que deben cumplirse cuando existe una relación con para otros medios de comunicación

7. Mantenimiento de equipos y su desecho.
   Especifica los objetivos de la manutención de equipos y desecho.
   Describe las normas y procedimientos para asegurar la correcta utilización así como su mantenimiento.
   Describe las normas y procedimientos cuando el equipo es reemplazado, decomisado, manipulado, desechado(hardware y software).
   Debe describir que tipo de personal esta autorizado para el mantenimiento del equipo.

8. Control de Cambios y Configuración.
   Detalla los responsables que tienen autorización para la aprobación de cambios a los sistemas.
   Detalla los procesos de aprobación de cambios a los sistemas.

9. Planificación de Contingencias.
   Establece de manera general la relación entre la valoración de riesgos y el plan de contingencias.
   Debe describir tanto las terminologías, procesos y mecanismos del Plan de Contingencias.
   Debe existir una correlación al Plan de Continuidad de Negocios.

10. Respuesta a Incidentes.
    Detalla las definiciones de los tipos de incidentes.
    Describe de manera general los procedimientos a seguir en caso de incidentes.
    Establece el responsable o comisión responsable de investigación, así como su alcance en caso de incidentes.

11. Auditorías y Detección de Intrusiones.
    Especifica los objetivos de la auditorías y detección de intrusiones.
    Establece de manera general los mecanismos de detección de intrusiones.
    Especifica la métodos de administración para las auditorías.

12. Medios de Almacenamiento.
    Especifica los objetivos del gobierno de medios de almacenamiento.
    Establece de manera general los procedimientos para asegurar la información de los medios de almacenamiento, tales como respaldo y recuperación.