ANEXO 3:
MODELO DE POLÍTICA DE SEGURIDAD DE LA ER

MODELO DE POLÍTICA DE SEGURIDAD DE LA ER

Una política de seguridad es el resultado de la elaboración de un conjunto de documentos basados en el estudio de la estructura del negocio. Cada documento 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.

Para el proceso de acreditación ante el INDECOPI deberá presentarse una Política de Seguridad basada en términos que garanticen la seguridad de los procesos de registro en la ER, dichos términos deben estar basados del estudio presentado en los documentos que se explican a continuación, los cuales deben ser presentados en la visita comprobatoria.

Documentos

1. Evaluación de riesgos.

Definición del alcance del área o proceso a evaluar. Identificación y valoración de los activos que corresponden al alcance. Identificación de amenazas y vulnerabilidades de los activos críticos. Evaluación del impacto de los riesgos. Tratamiento de los riesgos de impacto grave y moderado que puedan presentarse en los procesos de registro contemplados por la ER.

2. Política de Control de Acceso.

Detalle de los controles de acceso implementados para la protección de la información sensible, considerando el acceso a equipos informáticos, software, lectura y escritura de documentos tanto físicos como electrónicos. Asimismo se deben considerar los controles de acceso a los ambientes donde se encuentra la información sensible. Todos los controles que se implementen deben estar basados en los resultados de la evaluación de riesgos.

3. Seguridad de Personal (relacionado con seguridad IT).

Descripción de 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.
Detalle de las responsabilidades del personal, así como los medios y mecanismos de comunicación y capacitación.

4. Seguridad Física.

Descripción de los elementos que integran la seguridad física tales como alarmas de seguridad física, cerco perimetral, guardias, eliminación de material en desuso, llaves, etc. Descripción de los procedimientos para asegurar la seguridad física y ambiental.

5. Seguridad de Comunicaciones y Redes.

Descripción de las medidas de seguridad en el tema de comunicaciones y redes tanto a nivel interno como a nivel externo. Establecimiento de los requerimientos de seguridad que deben cumplirse cuando existe una relación con otros medios de comunicación.

6. **Mantenimiento de equipos y su desecho.**

Descripción de las normas y procedimientos para asegurar la correcta utilización de los equipos informáticos así como su mantenimiento. Descripción de las normas y procedimientos cuando el equipo es reemplazado, decomisado, manipulado, desechado (hardware y software). Descripción del tipo de personal que está autorizado para el mantenimiento del equipo.

7. Control de Cambios y Configuración.

Establecimiento de los responsables que tienen autorización para la aprobación de cambios a los sistemas. Detalle de los procesos de aprobación de cambios a los sistemas.

8. Planificación de Contingencias.

Descripción de la relación entre la valoración de riesgos y las acciones que se deben tomar como contingencia.

9. Auditorias y Detección de Intrusiones.

Establecimiento de los objetivos de la auditorias. Su frecuencia y sistemas implicados.

10. Medios de Almacenamiento.

Detalle de todos los procedimientos de los medios de almacenamiento para asegurar la información, tales como respaldo y recuperación.