ANEXO I

PROGRAMA PROFESIONALIZANTE DE DELEGADOS DE PROTECCIÓN DE DATOS PERSONALES

BLOQUE 1: DERECHO DE PROTECCIÓN DE DATOS PERSONALES

1. Naturaleza jurídica
    a. Derecho de protección de datos: constitución, ley, reglamento, resoluciones
    b. Historia y evolución normativa del derecho a la protección de datos personales.
    c. Modelos de regulación mundial sobre protección de datos personales
    d. Análisis del derecho a la protección de datos personales en el derecho constitucional ecuatoriano.
    e. Ética digital y objetivos de la Ley Orgánica de Protección de Datos Personales.
    f. Conceptos básicos de la Ley Orgánica de Protección de Datos Personales.
        i. Datos personales
        ii. Titular
        iii. Tratamiento
        iv. Clasificación de los datos
        v. Transferencia
2. Ámbito territorial y material de aplicación de la Ley Orgánica de Protección de Datos Personales.
3. Integrantes y roles del sistema de protección de datos personales
    a. Titular
    b. Responsables
    c. Encargados
    d. Delegados de protección de datos personales
    e. Terceros
    f. Autoridad de protección de datos personales
4. Bases legitimadoras de tratamiento
    a. Aplicación de cada base dependiente cada caso concreto.
    b. Validez de consentimiento Art. 8 Ley Orgánica de Protección de Datos Personales.
5. Principios
    a. Interpretación en tratamiento de datos personales
    b. Aplicación en el tratamiento de datos personales

c. Responsabilidad proactiva y demostrada

d. Protección de datos personales desde el diseño y por defecto

6. Finalidades del tratamiento

a. Objeto y Fundamentos prácticos

b. Tutela en el tratamiento de datos personales

7. Derechos de los titulares de datos personales

a. Alcance de los derechos (énfasis en casos prácticos de datos sensibles)

b. Excepciones a los derechos

c. Atención a los derechos

d. Canales de atención de derechos

e. Mecanismos de respuesta al ejercicio de derechos

f. Reglamento Denuncias vigente

g. Reglamento Consultas vigente

8. Transferencia de datos personales

a. Puerto seguro

b. Garantías adecuadas

c. Normas corporativas vinculantes

d. Autorización para ejecución

e. Excepcionalidades

f. Registro de información de Transferencias Internacionales

9. Obligaciones con la Superintendencia de protección de datos personales de Responsables, Encargados, Terceros y Delegado de protección de datos personales

a. Notificaciones de brechas

b. Registros ante la autoridad

c. Denuncias

d. Ejercicio de derechos

e. Apoderados

10. Régimen sancionador

a. Proceso Administrativo Sancionador

b. Infracciones Leves y Graves

c. Sanciones Leves y Graves

d. Responsabilidad administrativa y aproximación a otras responsabilidades

Tema Optativo:

11. Fenómenos:

a. Cultural: Resaltar cómo la privacidad varía según las culturas y su impacto en las regulaciones locales e internacionales.

b. Analizar cómo la percepción de la privacidad ha evolucionado con la tecnología, desde el uso de redes sociales hasta la economía colaborativa y su relación con los Derechos Humanos.

c. Económico: Explicar cómo los datos personales se han convertido en un recurso estratégico para las empresas, impulsando modelos de negocio basados en *big data* y personalización.

BLOQUE 2: METODOLÓGICO – IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

NORMA OBLIGATORIA: Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales de la Superintendencia de Protección de Datos Personales.

1. Aproximación a las normas de mejores prácticas (Ej. *ISO/IEC* 27701, *ISO/IEC* 27001, 27002, 27005, 42001, *COBIT* 19, *OWASP ASVS*, *OWASP Top Ten*, *PCI-DSS*, *FAIR MODEL*, y entre otras).

2. Inicio de la implementación un sistema de gestión de protección de datos personales

a. Iniciación

b. Análisis de controles existentes

c. Alcance

d. Aprobación y coordinación del plan

3. Etapas

a. Definición y establecimiento

i. Políticas de protección de datos personales

ii. Gestión de riesgos para la protección de derechos y libertades

1. Establecimiento del contexto
2. Identificación de riesgos
3. Análisis de riesgos
4. Evaluación de riesgos
5. Tratamiento de riesgos

iii. Evaluación de impacto de tratamiento de datos personales

iv. Declaración de aplicabilidad (Justificar medidas de seguridad)

b. Implementación

i. Gestión de documental

ii. Selección de medidas de seguridad, organizacionales y técnicas

iii. Implementación

iv. Capacitación y comunicación

c. Monitoreo y revisión

i. Análisis y evaluación del rendimiento del sistema

ii. Auditorías internas y/o externas

d. Mantenimiento y mejora continua

i. Tratamiento de no conformidades

ii. Mejora continua e innovación

e. Optativo: Actividades prácticas sobre el contenido de los puntos detallados en el punto 3.

BLOQUE 3: TÉCNICO – CALIBRACIÓN DE RIESGOS Y SEGURIDAD DE DATOS

NORMA OBLIGATORIA: Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales de la Superintendencia de Protección de Datos Personales.

1. Establecimiento del Contexto

a. Obtención de datos de entrada, elaboración de métricas, diseño de modelos de riesgo

b. Comprensión de los conceptos fundamentales de una gestión de riesgos para la protección de los derechos y libertades de los titulares de los datos

c. Elaboración de criterios de evaluación para la protección de derechos y libertades

d. Determinación de la tolerancia y/o de la capacidad al riesgo.

2. Implementación de la identificación de riesgos

a. Perfilamiento de amenazas

b. Escaneo de vulnerabilidades técnicas y dependencias de software

c. Tipos de ciberataques (Ej. denegación de servicio, malware, entre otras)

d. Respuesta a incidentes

3. Análisis cuantitativo de riesgos; ***(escoger cuantitativo y/o cualitativo)***

Se podrá considerar al menos uno de los siguientes métodos recomendados:

a. Probabilidad de ocurrencia

b. Métodos frecuentistas, métodos Bayesianos u otros aplicables

c. Distribuciones de probabilidades (continuas y discretas)

d. Modelos de riesgo (Ej: Modelo *FAIR*)

e. Valor al riesgo en ciberseguridad y en protección de datos

f. Análisis de Monte Carlo y/o Modelos de aprendizaje automático (analítica predictiva aplicada)

g. Métodos de calibración (Ej. *Conformal prediction* u otros aplicables)

4. Análisis cualitativo de riesgos ***(escoger cuantitativo y/o cualitativo)***

Se podrán considerar al menos uno de los siguientes métodos recomendados:

a. Métodos de calibración de opiniones (Ej. *Delphi*, *Lens*, etc.)

b. Técnicas para la elaboración de cuestionarios

c. Análisis argumental

d. Reducción de sesgos y ruido

e. Matrices de riesgos

f. *Rationales* (Justificar los valores de entrada y etiquetas en las matrices de riesgos)

5. Priorización de riesgos

a. Estrategias

b. Ponderación

6. Implementación de medidas de seguridad en protección datos personales

a. Medidas para la prevención de vulneraciones a la seguridad de datos personales

b. Medidas para la detección de vulneraciones a la seguridad de datos personales

c. Medidas para la respuesta a vulneraciones a la seguridad de datos personales

d. Interdependencias entre los controles de riesgos

e. Evaluación del rendimiento de las medidas de seguridad en el tiempo

f. Taxonomías de controles de riesgos (Ej: *ISO/IEC* 27001, *CIS Controls*, entre otras)

g. Recuperación de desastres y continuidad de actividades (*business continuity management*)

Actividad Práctica optativa: Ejercicios donde los delegados respondan a incidentes simulados como *ransomware* o brechas en sistemas en la nube, u otros

BLOQUE 4: BLOQUE DE CONTENIDOS SUGERIDOS NO OBLIGATORIOS

1. Relación de la tecnología con la protección de datos personales:

Se podrán considerar al menos uno de los siguientes métodos recomendados:

a. *Big Data*,

b. *Analytics*,

c. *Machine Learning*,

d. Entre otras tecnologías

2. Talleres de con herramientas y/o metodologías para gestión de riesgos en protección de datos.

3. Protección de Datos y Estrategia Empresarial:

a. Importancia de los datos personales del consumidor/usuario: Análisis del valor estratégico de los datos en la toma de decisiones empresariales y su relación con Derecho Humanos.

b. Tratamiento de datos en análisis de mercado y elaboración de perfiles: Estudio de casos internacionales que muestren cómo las empresas implementan estrategias de personalización respetando la privacidad de los usuarios.

c. Impacto reputacional y económico del cumplimiento normativo: Talleres para evaluar cómo la transparencia y la ética en el manejo de datos pueden convertirse en ventajas competitivas.

ESTIMACIÓN DE HORAS: mínimo 80.