ANEXO VI: PRIVACIDAD
NORMA MARCO DE PRIVACIDAD

El PSC deberá implementar las medidas necesarias para proteger la privacidad de los datos personales de los usuarios de sus servicios, incluyendo:

1) Designar a un Oficial de Privacidad, quien será el primer contacto frente a incidentes de privacidad;

2) Publicar en su página WEB la Política de Privacidad y el Plan de Privacidad y los datos de contacto del Responsable de Privacidad;

3) Implementar el Plan de privacidad de acuerdo a lo estipulado en el mismo documento, sujeto a las existentes obligaciones contractuales, licencias u otros arreglos de outsourcing;

4) Revisar y actualizar la Política de Privacidad y el Plan de Privacidad al menos una vez por año;

5) Elaborar y publicar en su página WEB una declaración de privacidad y seguridad;

Los documentos Política y Plan de Privacidad deben estar en concordancia con el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales y según los principios de privacidad descritos a continuación:

No	Tema	Principio
1	Prevenir el daño	Evaluar el riesgo al que la información personal se encuentra expuesta, e implementar medidas preventivas para reducir el impacto por el daño ocasionado, de manera proporcional a la probabilidad y severidad de los daños a los que se encuentra expuesta la información personal durante su recolección, uso o transferencia.

2	Notificación de prácticas	Los controladores de información personal deberían proveer declaraciones claras y accesibles sobre sus prácticas y políticas respecto de la información personal que debe incluir: - El hecho que la información personal es colectada. - Los propósitos por los cuales la información personal es colectada. - Los tipos de personas u organizaciones a los cuales la información personal puede ser revelada - La identidad y ubicación del controlador de la información personal, incluyendo información para contactarlo acerca de sus prácticas y manejos de la información personal. - Las opciones y medios que los controladores ofrecen a los individuos para limitar el uso y revelación, y el acceso correcto a su información personal.
		Todos los pasos que deben ser tomados para asegurar que la notificación ha sido provista antes o en el momento de la recolección de información personal.
		Puede no ser apropiado para los controladores de información personal notificar respecto de la recolección de información disponible públicamente.
3	Limitaciones de la recolección	La recolección de información personal debería estar limitado a información que es relevante para propósitos de recolección, mediante medios legales y confiables, si es apropiado, con notificaciones o consentimiento del individuo concerniente.
4	Uso de información personal	La información personal colectada debería ser usada sólo dentro de los propósitos de recolección y otros compatibles relacionados, excepto: - Aquellos que son recolectados con el consentimiento de los individuos propietarios de la información personal - Cuando sea necesario para proveer un servicio o producto solicitado por el individuo, o - Por autoridad de la Ley u otro instrumento legal, proclamaciones y pronunciamientos de efecto legal.

5	Selección de opciones	Si fuere apropiado, los individuos deberían ser provistos con mecanismos claros, comprensibles, prominentes, accesibles y asequibles para ejecutar selecciones en función de la recolección, uso y revelación de su información personal. Puede no ser apropiado para los controladores de información personal proveer estos mecanismos cuando se recolecte información públicamente disponible
6	Integridad de información personal	La información personal debería ser exacta, completa y actualizada para la extensión necesaria para el propósito de uso.
7	Salvaguardas de seguridad	Los controladores deberían proteger la información personal con controles contra riesgos, tales como pérdida o accesos no autorizados, o destrucción no autorizada, uso modificación o revelación u otros mal uso no autorizado. Tales salvaguardas deberían ser proporcionales a la probabilidad y severidad del daño, la sensibilidad de la información y el contexto en el cual es desarrollado, y debería ser sujeto a revisiones y evaluaciones periódicas.
8	Acceso y corrección	Los individuos deberían ser habilitados para: a) Obtener la confirmación si el controlador mantiene información personal del individuo b) Ha comunicado al individuo sobre su información personal, luego de haber reunido pruebas suficientes de su identidad: i) dentro de un tiempo razonable ii) bajo un cargo, si hubiera alguno, no excesivo iii) en una manera razonable iv) en una forma que es generalmente entendible; y, c) impugnar la exactitud de la información relacionada al individuo, y si fuera posible y apropiado, tener la información rectificada, completa, modificada o borrada.

		Tales accesos y oportunidades de corrección debería ser provista excepto si: i) la carga o gastos de hacerlo no sería razonable o sería desproporcional al riesgo para la privacidad del individuo en el caso en cuestión ii) la información no debería ser revelada debido a razones legales o seguridad o para proteger información comercial confidencial, o iii) la privacidad de la información de otras personas, diferentes al individuo, podrían ser violadas.
		Si una solicitud bajo (a) o (b) o una impugnación bajo (c) es denegada, el individuo debería ser provisto con razones sobre el porqué y tener la capacidad de impugnar tal denegación
9	Rendición de cuentas	El controlador debería ser sometido a una rendición de cuentas por el cumplimiento con las medidas que debe implementar para dar efecto a los principios estipulados en el presente documento. Cuando la información personal ha de ser transferida a otra persona u organización, sea de ámbito nacional o internacional, el controlador debería obtener el consentimiento del individuo o ejecutar la debida diligencia y tomar pasos razonables para asegurar que la persona u organización receptora protegerá la información de manera consistente con estos principios.