POLÍTICA DE MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

I. OBJETIVO

El presente documento contiene la Política de Medidas de Seguridad de la Información que LAIKII S.A.C., identificada con RUC No. 20608995219, y con domicilio para estos efectos en Calle Joaquín Turina 152, distrito de San Borja, provincia y departamento de Lima, Perú, en adelante ("***Laikii***") pone a disposición de todos sus trabajadores. El objetivo es proteger la calidad y seguridad de la información. Para ello se detallan una serie de políticas y procedimientos sobre las medidas técnicas y organizativas que puedan garantizar la adecuada gestión de la información y protección de los recursos informáticos de Laikii, incluyendo los datos personales del banco de datos de titularidad de este.

II. RESPONSABLES

1. Es responsabilidad del jefe de cada área hacer cumplir la presente política.
2. Es responsabilidad del jefe dela Dirección de Tecnología vigilar, actualizar y divulgar la presente política.
3. Es responsabilidad de todos los trabajadores ejecutar los lineamientos descritos en la presente política.

III. POLÍTICAS Y PROCEDIMIENTOS

La Política de Medidas de Seguridad de la Información está compuesta por las siguientes políticas y procedimientos:

A. CONTROL DE REGISTROS Y ACCESOS. -

- Gestión de accesos: Para impedir accesos no autorizados a los recursos informáticos de Laikii se deben establecer procedimientos para asignar derechos de acceso con privilegios a los sistemas, los cuales han sido asignados en función del cargo que desempeñan. Para ello se debe tomar en consideración la condición de los trabajadores o prestadores de servicios que son usuarios de los sistemas en Laikii, desde su ingreso como trabajador o prestador de servicios y su cese, (en adelante, los "***Usuarios***") tomando especial consideración en los Usuarios que tienen accesos privilegiados. Los procedimientos deben considerar: (i) registro los usuarios de los sistemas de Laikii; (ii) gestión de accesos privilegiados y revisión periódica de los mismos; (iii) gestión de contraseñas; (iv) altas y bajas de las cuentas; (v) cancelación de accesos debido al cese de la relación laboral o de servicio con el Usuario; (vii) modificación de los perfiles de los Usuarios, toda modificación debe ser revisada por el jefe inmediato y validada por la Dirección de Tecnología; (viii) conformidad de los Usuarios activos, lo que ayudará a llevar un control de la vigencia de los Usuarios que están activos en Laikii de manera periódica.

- Responsabilidad de los Usuarios: Los Usuarios de los sistemas de Laikii deben ser informados de sus responsabilidades y de que el éxito de las medidas de seguridad depende de su cooperación. Se debe capacitar a los Usuarios en los siguientes temas: (i) uso de contraseñas; y (ii) equipos desatendidos.

- Control de acceso a los recursos informáticos: Para acceder a los recursos informáticos de Laikii y para que los Usuarios no comprometan la seguridad

de la información, se establecen mecanismos de identificación y autenticación.

- Control de acceso a los sistemas de Laikii: El acceso a los sistemas de Laikii debe ser controlado para evitar accesos no autorizados, incluyendo: (i) procedimientos de inicio de sesión seguros.

- Control de acceso a las aplicaciones: Se debe impedir el acceso a la información que se encuentre en aplicaciones y restringir el acceso a los Usuarios que no estén autorizados.

- Monitoreo de uso de los sistemas: Los sistemas deben ser monitoreados para detectar actividades no autorizadas y reportar cualquier incidente de seguridad.

- Computación móvil y teletrabajo: Evaluar las medidas de seguridad que proporcionen un nivel de seguridad acorde a la sensibilidad de la información y potenciales riesgos.

- Control de acceso lógico: Los recursos electrónicos deben contar con un control de acceso específico.

- Acceso lógico restringido: El acceso a todos los recursos está limitado a aquellos Usuarios y/o sistemas que cuenten con la autorización necesaria. El acceso de cualquier Usuario al sistema sin autorización, faculta a Laikii a tomar las acciones y sanciones pertinentes.

- Derecho de admisión acceso lógico: Se podrá denegar o bloquear el acceso a cualquier Usuario o sistema en casos justificados y de manera unilateral cuando Laikii lo considere necesario para salvaguardar la seguridad del sistema.

- Lista de acceso lógico autorizado: La Dirección de Tecnología pondrá a disposición de quienes requieran la información para su trabajo, las listas de colaboradores, sistemas con acceso autorizado y tipo de control de acceso.

B. REGISTROS DE INTERACCIONES. -

- Generación de registros: Cada vez que los Usuarios interactúen con los datos lógicos, se mantiene un registro de sus actividades para fines de trazabilidad.

- Registros: Se mantienen los registros de los Usuarios con acceso al sistema, horas de inicio, cierre de sesión y actividades más relevantes realizadas en el sistema.

- Procedimiento de disposición: Los registros serán almacenados por noventa (90) días para finalidades de seguridad de la información y una vez que estos ya no sean útiles para tal fin, se efectuará la destrucción de estos.

C. REGISTRO DE INCIDENCIAS. -

- Incidente de seguridad informática: Es todo evento adverso vinculado a la seguridad de los sistemas y recursos informáticos.

- Clasificaciones del incidente: Los incidentes se pueden clasificar en: (i) fallas en aplicativos o servicios críticos; (ii) código malicioso; (iii) accesos no autorizados o mal uso de los recursos informáticos; (iv) violación de la presente Política de Medidas de Seguridad de la Información.

- Prevención de incidentes: La Dirección de Tecnología toma las medidas técnicas necesarias para prevenir que ocurran incidentes. Sin perjuicio de ello, es obligación de todos los trabajadores, prestadores de servicios u otros proveedores de Laikii acatar las medidas de seguridad aquí descritas para evitar la ocurrencia de incidentes.

- Detección y reporte del incidente: Una vez detectado el incidente o la existencia de un potencial incidente se debe informar del incidente o la potencial existencia de un incidente de manera inmediata a la Dirección de Tecnología para que tomen las medidas adecuadas para la mitigación del riesgo.

- Análisis del incidente: Una vez ocurrido el incidente de seguridad informática, se debe analizar la gravedad y qué información ha sido comprometida a efectos de determinar las posibles respuestas o soluciones. Adicionalmente, se evaluará dar aviso a los titulares de la información, en caso corresponda.

- Respuesta del incidente o medida adoptada: La Dirección de Tecnología es la encargada de tomar las acciones o medidas pertinentes para dar respuesta inmediata al incidente de seguridad de la información, así como de tomar las medidas necesarias para mitigar los riesgos en caso tengan la duda razonable de un potencial incidente.

- Registro del incidente: Cualquier incidente que ocurra debe ser registrado en el registro de incidentes que administrará la Dirección de Tecnología. Se deberán registrar los incidentes de seguridad relacionados con los bancos de datos personales de Laikii, este registro deberá contener como mínimo la siguiente información:

  A. Fecha y hora del incidente.
  B. Nombre de la persona que lo reporta.
  C. Naturaleza del incidente.
  D. Datos personales comprometidos.
  E. Nombres de las personas involucradas en la resolución del incidente.
  F. Consecuencias del incidente.
  G. Medidas correctivas implementadas.
  H. Recuperación de datos, en este caso se debe colocar además (i) Nombre de la persona que realizó la recuperación y (ii) Descripción y fecha de los datos restaurados.

- Prevención de nuevos incidentes: La Dirección de Tecnología dictará las medidas de prevención necesarias para evitar la ocurrencia de nuevos incidentes.

D. COPIAS O REPRODUCCIONES. -

- Generación de copias: La generación de copias o la reproducción de documentos que contengan datos personales, datos confidenciales o sensibles de Laikii, únicamente podrán ser realizadas bajo el control del personal autorizado. Para lo cual deberán enviar una solicitud al encargado

de la Dirección de Tecnología, en la cual se debe indicar expresamente el nombre del solicitante y la finalidad de las copias o reproducción de documentos.

- Destrucción de copias: En caso de ser necesario, Laikii como titular de banco de datos personales deberá designar a personas autorizadas a generar y/o eliminar las copias o reproducciones de los datos personales. Las cuáles serán eliminadas y destruidas cuando ya no sean útiles para la finalidad que se generaron. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

E. GESTIÓN Y USO DE CONTRASEÑAS. -

- Bloqueo de Pantalla (Protector de Pantalla): El Usuario es responsable de proteger su información debidamente, teniendo que activar el protector de pantalla del equipo asignado siempre que deje su posición de trabajo.

- Contraseña de equipo de cómputo: El Usuario es responsable de mantener su contraseña vigente y de no compartirla con ningún otro Usuario como medida de seguridad; si el Usuario comparte su contraseña, la responsabilidad recae completamente sobre él. La Dirección de Tecnología ha planificado que cada cierto tiempo se solicite el cambio de la contraseña (entre 30 a 90 días) para todos los colaboradores y en caso no realicen el cambio de contraseña se le bloquearan los accesos al sistema. La contraseña debe contener al menos 8 dígitos, ser alfanumérica (mayúsculas, minúsculas y números) e incluir un carácter especial.

- Contraseña de equipo de comunicaciones (Celulares): En los equipos de comunicaciones donde se tenga información de Laikii, necesariamente se deberá activar una contraseña para restringir el acceso al equipo, por consiguiente, bajo ninguna circunstancia se puede desactivar la contraseña y en caso ello suceda recae la responsabilidad completamente sobre dicho Usuario.

F. SEGURIDAD DE LOS EQUIPOS. -

- Seguridad física de equipos de cómputo (Laptops): Todos los Usuarios son responsables de mantener la seguridad del equipo en el puesto de trabajo asignado. En caso de requerir desplazar el equipo por algún motivo, se deberá informar previamente al jefe del área correspondiente.

- Antivirus: La Dirección de Tecnología es responsable de mantener actualizado y vigente el software antivirus instalado en todos los equipos de cómputo. De existir sospechas de mal funcionamiento a causa de virus, los Usuarios deben comunicarse de inmediato con la Dirección de Tecnología de Laikii encargada de dichas tareas.

- Dispositivos de almacenamiento externo o medios informáticos removibles: El uso de este tipo de medios de almacenamiento externo (cintas de respaldo, memorias USB, disco duro externo, entre otros) serán controlados a través de un sistema de control de accesos. debe de ser autorizado por el jefe del área del Usuario que desea hacer su uso.

- Eliminación de la Información de los medios informáticos removibles: Cuando se requiera eliminar información en un medio informático removible se deben utilizar mecanismos seguros de eliminación que garanticen la destrucción total de la información.

G. CONSERVACIÓN, RESPALDO Y RECUPERACIÓN DE DATOS. -

- Ambientes donde se conservan recursos informáticos: Los ambientes donde se conservan recursos informáticos cuentan con las medidas de seguridad apropiadas.

- Respaldos: Se han implementado mecanismos de respaldo de seguridad, los cuales permiten verificar la integridad de los datos personales almacenados en el respaldo, los cuales se hacen con una periodicidad diaria y almacenada durante 7 días.

- Recuperación: Ante una interrupción o daño se ha previsto la recuperación de los datos personales, garantizando el retorno al estado en el que se encontraban al momento en que se produjo la interrupción o daño.

H. ALMACENAMIENTO Y TRASLADO DE DOCUMENTACIÓN NO AUTOMATIZADA.

- Almacenamiento de datos no automatizados: Los archivadores u otros elementos donde se almacene información no automatizada con datos personales, se encontrarán resguardados bajo llave y solo el encargado del área tendrá acceso a ésta. Los archivadores permanecerán cerrados mientras no se estén utilizando los documentos que contienen los datos personales. En caso que, un colaborador requiera dichos documentos deberá solicitar permiso al encargado del área para lo cual deberá expresar por escrito el uso que le dará a dicha información.

- Traslado físico dentro de Laikii: Cuando se traslade documentación física que contenga datos personales dentro de Laikii, se tomarán medidas que impidan el acceso o manipulación de dicha información. Por tanto, cuando se proceda a trasladar un documento que contenga datos personales, se deberá llevar un registro de la persona encargada del traslado, el solicitante, la finalidad del uso de dicha información y la firma del encargado del área que autorizó el traslado en señal de conformidad.

- Traslado físico fuera de Laikii: Cuando se traslade documentación física que contenga datos personales fuera de Laikii, esto sólo se podrá hacer con la autorización del jefe del área que maneje dicha información y se hará utilizando los medios de transporte y medidas necesarias que eviten su acceso no autorizado, pérdida o manipulación durante el tránsito hacia su destino. En ese sentido, se deberá llenar un registro de la persona encargada del traslado, el solicitante, la finalidad del uso de dicha información y la firma del encargado del área que autorizó el traslado en señal de conformidad.

I. USO DE CORREOS ELECTRÓNICOS. -

- Retención de correos electrónicos: Todos los Usuarios tienen una cuenta de correo electrónico asignada para realizar sus labores, la cual tiene un límite en su capacidad de almacenamiento, esta medida se toma para no bajar el

rendimiento en el envío y recepción de los correos para todos los trabajadores.

- Uso de correos electrónicos: Todos los Usuarios deben tener conocimiento del uso debido de los correos electrónicos corporativos. Tener en cuenta los siguientes puntos: (i) Los Usuarios no podrán utilizar el correo electrónico de Laikii para distribuir información de Laikii sin autorización del jefe del área donde laboran; (ii) El Usuario debe tener el debido cuidado para que los correos electrónicos personales corporativos no se entiendan como comunicados oficiales de Laikii; (iii) Los Usuarios no pueden utilizar el correo electrónico de Laikii para transmitir "cadenas de mensajes"; (iv) Ningún correo electrónico debe ser enviado con la intención de ocultar o modificar el nombre del emisor; (v) Se proveerá una cuenta de correo electrónico a los contratistas mediante una solicitud de seguridad aprobada; (vi) Los Usuarios son responsables de todo correo electrónico procedente de su cuenta; (vii) Cuando se envíen documentos con información sensible o confidencial a través de un correo electrónico, los Usuarios deberán enviar el documento protegido con una contraseña o clave de seguridad.

IV. INCUMPLIMIENTO

Es responsabilidad de todo Usuario hacer cumplir las disposiciones indicadas en la presente política. En caso sucediera un incumplimiento, el responsable del proceso debe informar al área correspondiente, a fin de que esta evalúe el tipo de medida disciplinaria a aplicar.