MANUAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA PROVEEDORES

De conformidad con lo establecido en la Resolución SBS N° 504-2021, que aprueba el Reglamento de Gestión de Seguridad de Información y Ciberseguridad y sus modificaciones (en adelante el "Reglamento de SI"), la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 ''Sistema de Gestión de Seguridad de la Información' (en adelante "Normativa Técnica"). **EL PROVEEDOR** es responsable de cumplir rigurosamente con cada una de las obligaciones que se detallan a continuación, relacionadas con la información de propiedad de **HERMES** y con la información que éste último comparta con **EL PROVEEDOR**:

1. **Controles de Seguridad**

   EL PROVEEDOR declara conocer de manera integral todos los alcances normativos contemplados en el Reglamento de SI; así como las medidas y/o sanciones por el incumplimiento del mismo.

   Siempre que, **EL PROVEEDOR** acceda, almacene o procese información de **HERMES**, mantendrá ("Controles") diseñados para resguardar la confidencialidad, integridad y disponibilidad de la información de **HERMES,** los cuales deberán cumplir con el Reglamento de SI, la Ley Nº 29733 "Ley de Protección de Datos Personales" y con la "Normativa Técnica", incluso lo siguiente:

   1.1 Controles de seguridad física

   EL PROVEEDOR mantendrá controles de acceso físico, destinados a resguardar la información de **HERMES,** durante el desarrollo del servicio contratado. **EL PROVEEDOR** deberá cumplir con todos y cada uno de los mecanismos de control señalados a continuación:

   - Puertas externas:
     Estar adecuadamente protegidas contra los accesos no autorizados a través de mecanismos de control, por ejemplo, barras, alarmas, cerraduras, tornos, cámaras de vigilancia etc.

   - Control de identificación:
     Implementar un control para la identificación del empleado o colaborador mediante el uso de tarjetas de identificación, tarjetas electrónicas, identificación biométrica, y otros, a fin de prevenir los accesos de personas no autorizadas.

   - Extintores:
     Deben estar en buen estado y disponibles para su uso.
   - Servidores On Premise:
     En caso la información de **HERMES** se almacene en servidores on-premise, estos deben estar ubicados en un área especialmente protegida, que cumplan como mínimo con las siguientes medidas de seguridad:

     - Contar con detectores de humo.
     - Falso techo, falso piso.

- Contar con UPS.
- Contar con cámaras de seguridad.
- Contar con una bitácora de accesos.
- Contar con personal que valide los ingresos o contar con controles de acceso de tipo tecnológico como: tarjetas electrónicas, uso de biometría, etc.
- El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.

1.2 Seguridad y Responsabilidad del Personal

EL PROVEEDOR establecerá políticas, lineamientos, procedimientos y estrategias relacionadas con la gestión de su personal que limiten el acceso a la información perteneciente a **HERMES**. Además, **EL PROVEEDOR** deberá suscribir acuerdos de confidencialidad por escrito con su personal, así como solicitar y verificar sus antecedentes penales, judiciales y policiales, según legislación vigente, especialmente en lo que respecta al personal que tenga acceso a la información de **HERMES** o que se encuentre a cargo de mantener, implementar o gestionar su programa de seguridad de la información y de los "Controles de Seguridad".

Todo personal de **EL PROVEEDOR** que tenga acceso a la información de **HERMES** es responsable de y por las actividades de las credenciales de acceso asignadas. Por tanto, toda persona debe proteger su usuario y contraseña o método de autenticación asociado a su identificador de usuario, asimismo, **EL PROVEEDOR** es responsable del actuar de su personal. El personal de **EL PROVEEDOR** no debe, ni puede utilizar el usuario de otra persona.

1.3 Protección contra Malware

EL PROVEEDOR debe instalar, configurar, activar y mantener actualizado un software antivirus, antiransomware EDR o XDR y anti espías (anti-spyware) de marcas confiables en el mercado, en todos los servidores, dispositivos, computadoras portátiles y estaciones de trabajo que procesen o almacenen información o cualquier otro dato de **HERMES.**

EL PROVEEDOR debe implementar controles, que no permitan a los usuarios realizar modificaciones o eliminar las configuraciones de seguridad en los softwares de seguridad instalados.

1.4 Parches de Seguridad

EL PROVEEDOR implementará y mantendrá medidas de control y procedimientos orientados a garantizar que su infraestructura tecnológica, sistemas y dispositivos (incluyendo sistemas operativos y aplicaciones) que accedan, almacenen y/o procesen información de **HERMES** se encuentren en todo momento actualizados, lo que implica que **EL PROVEEDOR** implemente de manera inmediata todos los parches de seguridad cuando estos sean emitidos o sean solicitados para remediar fallos y vulnerabilidades de seguridad.

Con la finalidad de mitigar la amenaza, riesgo e impacto de las vulnerabilidades de la seguridad en el sistema o red, **El PROVEEDOR** deberá de:

- Desarrollar e implementar un proceso para investigar continuamente las fuentes fiables de advertencias sobre vulnerabilidades de seguridad emergentes;
- Identificar vulnerabilidades específicas que puedan impactar los ambientes operativos o plataformas utilizados por **EL PROVEEDOR**.
- Evaluar la criticidad de una vulnerabilidad en relación con las operaciones generales de **EL PROVEEDOR** y **HERMES**, a fin de determinar la conveniencia de instalar el correspondiente parche de seguridad;
- Probar e instalar oportunamente los parches de seguridad;
- Brindar los sustentos de pruebas de seguridad como Ethical Hacking, Pentesting, análisis y mitigación de vulnerabilidades de acuerdo a la característica del **SERVICIO**.

1.5 Gestión de la Cuenta del Usuario

EL PROVEEDOR implementará mecanismos de gestión que permitan la creación, modificación y eliminación segura de cuentas de usuario en las redes, sistemas y dispositivos a los que **EL PROVEEDOR** acceda para obtener información de HERMES. Estos mecanismos deberán permitir que **EL PROVEEDOR** tenga el control y el manejo de las cuentas privilegiadas y además garantizar que los titulares y responsables de la información de HERMES brinden la autorización respectiva a todas las solicitudes relacionadas con estas cuentas.

El PROVEEDOR tiene la obligación de resguardar y proteger las credenciales de acceso tales como nombres de usuario, contraseñas, credenciales físicos y tarjetas de acceso, así como cualquier otro que cumpla dicha finalidad, que le sean proporcionadas por **HERMES** para la realización de sus actividades. Estas credenciales brindan el acceso a los diversos sistemas informáticos y espacios físicos de **HERMES. El PROVEEDOR** reconoce y acepta que las credenciales de acceso son de uso exclusivo y personal, y bajo ningún concepto pueden ser divulgadas, transferidas o compartidas con terceros. Asimismo, **EL PROVEEDOR** asume plena responsabilidad por todas las acciones que se lleven a cabo mediante el uso de las credenciales de acceso asignadas en los sistemas de **HERMES**, así como por las repercusiones que puedan resultar del incumplimiento de estas obligaciones o de un uso indebido. En caso de que las credenciales asignadas a **EL PROVEEDOR** sean vulneradas, este deberá notificar de forma inmediata a **HERMES,** en un plazo no mayor de 24 horas de conocido el evento, a fin de que **HERMES** adopte las medidas de seguridad correspondientes. Este incumplimiento es causal de resolución del contrato, sin perjuicio de las acciones legales que **HERMES** adopte por los daños generados.

1.6 Autenticación de Usuario

El PROVEEDOR deberá asegurar de mantener una autentificación de usuarios que contenga el uso de un doble factor de autenticación y otros estándares de seguridad reconocidos como vigentes en el mercado, así como controles de acceso y la asignación de privilegios específicos relacionados con los sistemas operativos, aplicaciones, equipos, y demás recursos.

1.7 Registro y Control

El PROVEEDOR llevará el control, registro y monitoreo de todos los accesos a la información protegida en las redes, sistemas y dispositivos que este administre. Estos sistemas de control, registro y monitoreo deberán estar acordes con la "Normativa Técnica" aplicable, por lo que, **EL PROVEEDOR** se compromete a conservar todos los registros de acceso por un periodo mínimo de 90 días calendario.

2. Controles de Acceso

Durante el período en que **EL PROVEEDOR** tenga acceso, almacene o procese información perteneciente a **HERMES**, deberá implementar controles adecuados, tales como, la segregación de funciones, una matriz de permisos de acceso, registros de auditoría de acceso y monitoreo de acceso a los recursos utilizados para la protección de la información de **HERMES.** Los controles antes señalados tendrán como finalidad el garantizar únicamente el acceso a las personas que justifiquen una necesidad legítima del acceso a dicha información, relacionado a la ejecución del servicio acordado. El acceso a la información deberá cesar de manera inmediata una vez concluida la necesidad legítima que lo motivó. **EL PROVEEDOR** se compromete a registrar los detalles pertinentes relacionados con el acceso a la información en sus sistemas y equipos, manteniendo dichos registros durante un periodo mínimo de 90 días calendario. Además, **EL PROVEEDOR** será responsable de cualquier acceso no autorizado a la información protegida de **HERMES**. **EL PROVEEDOR** deberá notificar a **HERMES** de forma inmediata y dentro de un plazo de 24 horas en caso los accesos otorgados ya no sean requeridos y/o cuando el personal a cargo del servicio haya sido cesado.

2.1 **EL PROVEEDOR** se obliga a contar con una política y procedimientos de control de accesos que permitan gestionar de forma segura los accesos privilegiados a la infraestructura, ya sea on-premise o nube. Asimismo, **EL PROVEEDOR** garantiza el acceso exclusivo a personas autorizadas para la operación y soporte del servicio contratado por **HERMES**, incluyendo, además, la obligación de **EL PROVEEDOR** en la autenticación de usuarios y la monitorización de las actividades.

2.2 **EL PROVEEDOR** asume la responsabilidad total de cualquier daño derivado de un acceso o uso no autorizado de la información generada durante la vigencia del contrato o durante la ejecución del servicio para **HERMES**. Además, será responsable de cualquier violación o pérdida de información registrada, ya sea causada por **EL PROVEEDOR**, su personal o sus proveedores de servicio, durante cualquier fase de procesamiento, transmisión o almacenamiento de información de **HERMES.**

3. Requisitos de Cifrado

En cualquier circunstancia en la que **EL PROVEEDOR** acceda, almacene o procese información perteneciente a **HERMES**, estará obligado a mantener un estándar de cifrado que se encuentre vigente y no vulnerado en el mercado global. **EL PROVEEDOR** deberá cifrar toda la información de **HERMES** que sea almacenada en dispositivos portátiles o medios electrónicos transferibles, así como en medios lógicos que se mantengan fuera de las instalaciones de **HERMES**, exceptuando los

documentos impresos, o que sea transmitida a través de redes ajenas a la red interna de **HERMES**, que sea de propiedad o esté gestionada por **EL PROVEEDOR**.

4. **Capacitación y Supervisión**
   El PROVEEDOR llevará a cabo, de forma anual, la capacitación de sus directores, personal, proveedores y de cualquier individuo que intervenga en la prestación del servicio con **HERMES**, en materia de seguridad de la información, ciberseguridad y protección de datos personales. El cumplimiento de estas capacitaciones deberá ser informado anualmente al administrador correspondiente del servicio y ser remitido al correo electrónico seguridadinformacion@hermes.com.pe.

5. **Uso de las Redes, Sistemas o Dispositivos de HERMES.**
   El PROVEEDOR se obliga a adherirse a las políticas y procedimientos internos de **HERMES** en la medida de que este acceda a las redes, sistemas o dispositivos que sean de propiedad de **HERMES**, así como, aquellos dispositivos administrados por **EL PROVEEDOR**. Esta obligación incluye, pero no se limita a, el uso de programas de interfaz de aplicación (API), cuentas de correo electrónico, equipos y en aquellos supuestos donde **EL PROVEEDOR** deba hacer uso de las instalaciones de **HERMES** para la ejecución del servicio acordado.

6. **Auditorías, Certificaciones y Evaluaciones**
   Las ejecuciones de las prestaciones acordadas en el contrato a cargo de **EL PROVEEDOR** podrán ser objeto de revisión, supervisión continua o evaluación por parte del personal de **HERMES,** incluido su Unidad de Auditoría Interna y su Sociedad Auditora Externa, así como por el funcionario que la Superintendencia de Banca, Seguros y AFP designe para tal fin y en la oportunidad en que lo estime conveniente. Estas revisiones estarán orientadas a validar que **EL PROVEEDOR** cuente con los controles de seguridad necesarios para proteger la información de **HERMES** de acuerdo con las obligaciones contractuales establecidas.

   6.1 **EL PROVEEDOR** permitirá a **HERMES** realizar de forma coordinada y en las ocasiones que sea requerido, cualquier evaluación que tenga como finalidad la verificación de los controles de seguridad de la información de **EL PROVEEDOR**, para ello**, EL PROVEEDOR** deberá brindar las facilidades para la interacción con su personal responsable, así como el acceso a la documentación, infraestructura, oficinas, y lugares y software de aplicación que tengan acceso a la información de **HERMES. HERMES** deberá enviar esta solicitud con un mínimo de diez (10) días calendario de anticipación a la realización de la auditoría. **HERMES** tratará la información que **EL PROVEEDOR** proporcione en las evaluaciones como información de carácter confidencial del **PROVEEDOR**.

   6.2 Si por la naturaleza del servicio contratado, **EL PROVEEDOR** almacena información confidencial de **HERMES** dentro de sus sistemas, aplicaciones, en la nube, en sus instalaciones, y/o cualquier otro sistema de almacenamiento, de manera constante y permanente durante toda la ejecución del servicio, **EL PROVEEDOR** deberá presentar a **HERMES** la Certificación de Seguridad de la Información y Ciberseguridad ISO 27001, que acredita el cumplimiento de los estándares de seguridad de la información requeridos. Asimismo, **EL PROVEEDOR** pondrá a disposición de **HERMES** el informe de prueba de penetración más reciente o el último

informe de auditoría o el reporte SOC2 tipo 2, u otros informes de evaluación de ciberseguridad que dejen constancia del cumplimiento de las obligaciones señalados en la presente cláusula.

6.3 Si **EL PROVEEDOR** accede, almacena o procesa información de **HERMES** o tiene acceso a recursos tecnológicos de **HERMES** desde sus sistemas o sus sistemas se conectan a la red o a los sistemas internos de **HERMES**, en ese caso, **HERMES** podrá solicitar a **EL PROVEEDOR** un informe técnico pruebas de vulnerabilidad que incluyan las evidencias correspondientes, para el desarrollo del informe se incluirá la ejecución de pruebas automatizadas y manuales por parte de personal especializado, sobre los sistemas e infraestructura tecnológica que **EL PROVEEDOR** emplee para el desarrollo del servicio contratado. Así mismo, **HERMES** podrá solicitar a **EL PROVEEDOR** que se le proporcione las acciones de mitigación o remediación que se han tomado sobre las vulnerabilidades detectadas y relacionadas con los recursos tecnológicos que se utilizan para proporcionar el servicio **HERMES**.

6.4 **EL PROVEEDOR** controlará de manera continua los riesgos identificados y asociados con la información de **HERMES** para asegurar que las “Medidas de Protección” sean diseñadas y se mantengan acordes a los lineamientos indicado por **HERMES** durante la vigencia del contrato y/o durante la ejecución del servicio, a fin de impedir el acceso no autorizado, modificaciones no autorizadas o pérdidas de información de **HERMES. EL PROVEEDOR** periódicamente (pero no menos de una vez por año) evaluará y documentará la efectividad de sus controles de seguridad en sus redes, sistemas y dispositivos (lo que incluye infraestructura, las aplicaciones y los servicios) usados para acceder, almacenar o procesar la información de **HERMES**. **EL PROVEEDOR** deberá proporcionar a **HERMES** los resultados de las pruebas de vulnerabilidad realizada y el estado de las medidas correctivas que se dispongan en las conclusiones a las que se arribe, **HERMES** tratará estos resultados como información de carácter confidencial del **PROVEEDOR**.

6.5 Si alguna de las partes identifica que las “Medidas de protección" de **EL PROVEEDOR** contiene alguna vulnerabilidad, observación o hallazgo, como resultado de las auditorías realizadas por **HERMES** o una sociedad auditora externa autorizada por el mismo o evaluación y/o investigación, **EL PROVEEDOR** corregirá o mitigará inmediatamente a su propio costo, cualquier vulnerabilidad, observación o hallazgo, dentro del plazo establecido de acuerdo a su criticidad contados desde su identificación. Para vulnerabilidades, observaciones y/o hallazgos catalogados como críticos, un plazo no mayor a siete (7) días calendario. Para vulnerabilidades, observaciones y/o hallazgos catalogados como altas, un plazo de veinte (20) días calendario. Para vulnerabilidades, observaciones y/o hallazgos catalogados como medias y bajos, un plazo de noventa (90) días calendario. En todos los casos, **EL PROVEEDOR** deberá entregar las respectivas evidencias de cierre de dichas vulnerabilidades, observaciones y/o hallazgos a **HERMES**.

Si **HERMES** identificara alguna vulnerabilidad, observación y/o hallazgo, **EL PROVEEDOR** deberá proporcionar las evidencias y sustentos que acrediten que las correcciones efectuadas en virtud del párrafo anterior, cumplen con los requisitos de la presente cláusula. Si **EL PROVEEDOR** no puede corregir o mitigar dichas vulnerabilidades, observaciones y/o hallazgos dentro del periodo de tiempo especificado, deberá notificar inmediatamente a **HERMES** y proponer otros plazos y sustentos razonables.

7. Respuesta a incidentes de Seguridad

Las Partes acuerdan que, para manejar adecuadamente cualquier evento que afecte negativamente la seguridad de la información confidencial y restringida proporcionada por **HERMES**, información generada por la ejecución del servicio, así como el acceso a cualquier recurso provisto por **HERMES** para la gestión del servicio, tales como el acceso a las redes, los sistemas o los dispositivos de propiedad de **HERMES**, así como los dispositivos gestionados por este último**,** incluidos los programas de aplicación de interfaz, cuentas de correo electrónico, equipamiento y cuando **EL PROVEEDOR** haga uso de las instalaciones de **HERMES** (en adelante, ""incidente""), **EL PROVEEDOR** deberá de contar con:

i. Mantener un programa de respuesta a incidentes de ciberseguridad, basado en las mejores prácticas vigentes del mercado.
ii. Mecanismos para monitorear y detectar posibles "incidentes".
iii. Plan de respuesta ante "incidentes" que le permita analizar y responder oportunamente a cualquier tipo de "incidente" de seguridad.
iv. Procedimientos para evaluar los "incidentes" y realizar el escalamiento correspondiente a instancias superiores, según sea el caso.

7.1 En caso de que **EL PROVEEDOR** identifique algún "incidente" que afecte o pueda afectar la información confidencial y restringida de **HERMES**, en el acceso, almacenamiento y/o procesamiento de la información en instancias on-premise y/o servicios en la nube contratados, **EL PROVEEDOR** inmediatamente deberá:

- Adoptar las medidas inmediatas para mitigar los efectos de dicha vulneración (daño o potencial daño)
- Asegurar la información proporcionada por **HERMES,** mediante mecanismos de seguridad implementados.
- Notificar a **HERMES**, en un plazo no mayor a las 24 horas después de identificar el "incidente" de Seguridad, mediante el envío de un correo electrónico al área de Seguridad de la información de **HERMES** seguridadinformacion@hermes.com.pe. con la información descrita en el siguiente párrafo; así como las medidas y procedimientos llevados a cabo, en virtud de las leyes aplicables, a efectos de mitigar los efectos del "incidente".
- Proporcionar la información que sea relevante acerca del "incidente" de Seguridad, lo que incluye: una descripción de la información protegida sujeta al "incidente" de Seguridad (lo que incluye las categorías y cantidad de registros de datos y sujetos relacionados a los datos comprendidos); la fecha y hora del incidente de seguridad; una descripción de las probables consecuencias del incidente de seguridad; una descripción de las circunstancias que dieron lugar al ""incidente"" de seguridad (por ej.

pérdida, robo, copiado); una descripción de las medidas recomendadas para mitigar cualquier efecto adverso del ""incidente"" de seguridad; una descripción de las medidas que **EL PROVEEDOR** propone para abordar el "incidente" de seguridad; y personas de contacto relevantes que estarán "razonablemente disponibles" hasta que las partes acuerden mutuamente que se resolvió el incidente de seguridad. Para los "incidentes" de seguridad que impliquen información de **HERMES**, "razonablemente disponible" significa 24 horas por día, 7 días a la semana.

- Elaborar un plan de acción para la recuperación de la información, así como protocolos para evitar la repetición de "incidentes" similares.
- En caso de ser un servicio significativo de procesamiento de datos, deberá gestionar los "incidentes" de seguridad de la información y desarrollar las actividades planificadas previstas en el artículo 13 del Reglamento de SI.
- Indemnizar a **HERMES** por todos los daños y gatos generados, multas o sanciones impuestas y cualquier otra responsabilidad derivada del "incidente".

7.2 **EL PROVEEDOR** tomará las medidas adecuadas para corregir inmediatamente el origen de la/las causa(s) de cualquier incidente de seguridad, y cooperará en forma razonable con **HERMES** respecto a la investigación y medidas correctivas que se llevarán a cabo en relación con el "incidente". Asimismo, inmediatamente proporcionará a **HERMES** los resultados de la investigación y cualquier medida correctiva que se haya implementado. Bajo solicitud de **HERMES**, **EL PROVEEDOR** deberá proporcionar un análisis forense, el cual será asumido y realizado por **EL PROVEEDOR** con la empresa que **HERMES** designe.

7.3 **EL PROVEEDOR** deberá reportar "incidentes" de seguridad de la información o eventos potenciales de riesgo de seguridad de la información a **HERMES** dentro de las 24 horas de conocido el hecho, así como cumplir con la gestión de "incidentes" de ciberseguridad y con el reporte "incidentes" de ciberseguridad significativos a que se hacen referencia en los artículos 12 y 15 del Reglamento SI.

7.4 Excepto en caso de que las leyes aplicables lo dispongan de otro modo, **EL PROVEEDOR** no realizará (ni permitirá que ningún tercero realice) ninguna declaración con relación al incidente de seguridad que directa o indirectamente haga referencia a **HERMES**, a menos que **HERMES** brinde una autorización expresa por escrito.

8. Uso Aceptable de la Información, Equipos y Servicios Informáticos

8.1 **El PROVEEDOR**, durante todo el tiempo acceda, procese y/o almacene información de **HERMES**, así como utilice recursos tecnológicos de **HERMES**, estará obligado a llevar a cabo un uso diligente y responsable relacionado con las actividades del servicio. Adicionalmente, **EL PROVEEDOR** deberá notificar a **HERMES** sobre cualquier incidente que pudiera poner en riesgo los recursos informáticos y la información que dichos recursos albergan.

8.2 **EL PROVEEDOR,** siempre que acceda a la red de **HERMES** utilizando sus propios dispositivos, **EL PROVEEDOR** estará obligado a asegurar y demostrar que posee mecanismos de protección a nivel de puntos finales (estaciones de trabajo, computadoras y/o laptops), tales como, un

software antivirus actualizado, antiransomware EDR o XDR, actualizaciones de seguridad del sistema operativo y de aplicaciones, restricción de permisos administrativos, prevención de pérdida de datos (DLP), cifrado de discos duros y cualquier otra medida que **HERMES** considere pertinente.

8.3 En caso de que se requiera llevar a cabo el intercambio de información como parte del servicio, **EL PROVEEDOR** y **HERMES** se comprometen a coordinar la entrega o intercambio de dicha información a través de canales seguros, que aseguren la integridad y la confidencialidad de la misma.

9. Seguridad para la Adquisición, Desarrollo y Mantenimiento

9.1 EL PROVEEDOR deberá alinearse y asegurar que el personal que brinda el servicio a **HERMES** aplique estándares de desarrollo seguro en concordancia con los que cuenta **HERMES** para la configuración, desarrollo y mantenimiento de los sistemas y aplicaciones requeridas.

9.2 EL PROVEEDOR debe incorporar el análisis estático y dinámico de los códigos de seguridad en el ciclo de vida del desarrollo del software. Asimismo, **EL PROVEEDOR** deberá mitigar los problemas de seguridad identificados durante el análisis estático y dinámico de los códigos antes de pasarlos al entorno de producción.

9.3 Como parte del ciclo de vida del desarrollo, **EL PROVEEDOR** debe realizar un análisis seguridad a la aplicación (análisis de vulnerabilidades o Ethical Hacking) antes de pasarlos al entorno de producción y sea publicada con la finalidad de identificar vulnerabilidades y estas sean subsanadas en los plazos especificados en la sección 6.5 de Auditorías, Certificaciones y Evaluaciones

9.4 EL PROVEEDOR debe garantizar que se informe de forma periódica sobre las actualizaciones o correcciones que se realicen al sistema o aplicación. Además de proporcionar la asesoría y acompañamiento debido.

9.5 El PROVEEDOR en coordinación con **HERMES** debe poner a disposición canales seguros para el intercambio de información que garanticen su integridad y confidencialidad.

10. Cumplimiento

El PROVEEDOR debe de cumplir con los requisitos indicados por **HERMES**, así como también con los controles solicitados en las normativas y regulaciones que aplican a **HERMES** como la Ley 29733 - Ley de Protección de Datos Personales y su reglamento, Circular G140 SBS, Resolución SBS N° 504-2021 que aprueba el reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

11. Borrado seguro de la información

11.1 En caso de desvinculación laboral del personal de **EL PROVEEDOR** asignado a la ejecución del servicio, **EL PROVEEDOR** se encargará de:

- Que dicho personal realice la devolución de la información generada, procesada o almacenada de **HERMES**, así como a llevar a cabo un borrado seguro de información de **HERMES** almacenada, procesada o generada en los equipos utilizados por su personal para el desarrollo del servicio.

11.2 En el caso de finalización de la vigencia del Contrato o servicios o ante una solicitud efectuada por **HERMES**, ya sea en entornos on-premise o en modalidades de nube (SaaS, PaaS, entre otros), **EL PROVEEDOR** asegura que se cumplirán las siguientes condiciones:

- **EL PROVEEDOR** cesará el uso de la información confidencial debiendo devolver a **HERMES** toda la información recibida, generada, procesada y/o almacenada.
- Realizar el borrado seguro de la información generada, procesada y/o almacenada en la infraestructura y/o repositorios físicos o en nube y destruir toda copia que se haya realizado.
- Además, **EL PROVEEDOR** está obligado a proporcionar una confirmación por escrito en un plazo no mayor a 15 días calendario de resuelto el contrato y evidenciar los mecanismos utilizados para el borrado seguro y su implementación, con el fin de eliminar de manera permanente e irrecuperable la información de **HERMES.** Esta evidencia deberá ser enviada de manera formal al área de Seguridad de la Información de **HERMES** a través del buzón de correo electrónico seguridadinformacion@hermes.com.pe. **HERMES** se reserva el derecho de realizar verificaciones según considere necesario.

12. Subcontratación por parte del Proveedor

En todo momento que **EL PROVEEDOR** realice la subcontratación del personal o del servicio contratado, deberá garantizar que el subcontratista cumpla los puntos expuestos en la presente cláusula. Además, el subcontratista deberá contar con acuerdos de confidencialidad y protección de datos personales sobre la información de **HERMES**.

12.1 Es responsabilidad de **EL PROVEEDOR** informar en un plazo no mayor a quince (15) días calendario cualquier modificación con el subcontratista para el desarrollo del servicio adquirido por **HERMES**. En caso de que **EL PROVEEDOR** requiera realizar una subcontratación para el desarrollo de la totalidad del servicio, deberá de contar con la autorización expresa de **HERMES**.

Fecha de entrada en vigor: 18.02.2026.

Última actualización: 18.02.2026.