POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES

Elaborado por:	Revisado por:	Homologado por:	Aprobado por:
Julius K. Villavicencio Monti – **Oficial de Seguridad de la Información** **Subgerente de Planeamiento y Control de Gestión**	Teofilo Chambilla Aquino **Líder de Gobierno y Transformación Digital**	Julius K. Villavicencio Monti – **Subgerente de Planeamiento y Control de Gestión**	Jorge Herbozo Perez- Costa **Gerente General (e)**
Firma: Firmado digitalmente por: VILLAVICENCIO MONTI Julius Korel FAU 20425809882 hard Fecha: 26/09/2023 08:17:11	**Firma:** Firmado digitalmente por: CHAMBILLA AQUINO Teofilo FAU 20425809882 hard Fecha: 26/09/2023 09:37:28	**NO APLICA**	**Firma:** Firmado digitalmente por: HERBOZO PEREZ COSTA Jorge Luis Pelayo FAU 20425809882 hard Fecha: 26/09/2023 11:46:03

CONTROL DE CAMBIOS

Autor	Descripción del Cambio	Versión	Fecha
Oficial de Seguridad de la Información	• Elaboración inicial del documento	00	21/07/2023
Oficial de Seguridad de la Información	• Se modifica el nombre del formato del primer punto. • Se modifica el ítem 2 y 8.	01	Según firma digital

Elaborado por:	Revisado por:	Homologado por:	Aprobado por:
Julius K. Villavicencio Monti – **Oficial de Seguridad de la Información** **Subgerente de Planeamiento y Control de Gestión**	Teofilo Chambilla Aquino **Líder de Gobierno y Transformación Digital**	Julius K. Villavicencio Monti – **Subgerente de Planeamiento y Control de Gestión**	Jorge Herbozo Perez- Costa **Gerente General (e)**
Firma: Firmado digitalmente por: VILLAVICENCIO MONTI Julius Korel FAU 20425809882 hard Fecha: 26/09/2023 08:17:11	**Firma:** Firmado digitalmente por: CHAMBILLA AQUINO Teofilo FAU 20425809882 hard Fecha: 26/09/2023 09:37:28	**NO APLICA**	**Firma:** Firmado digitalmente por: HERBOZO PEREZ COSTA Jorge Luis Pelayo FAU 20425809882 hard Fecha: 26/09/2023 11:46:03

POLÍTICA DE SEGURIDAD DE INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

- El proveedor deberá firmar y entregar el Formato S4.1.1-FT25 constancia de recepción de la política para proveedores antes de iniciar el trabajo.
- Todo proveedor se asegurará que su personal que formará parte del servicio lea, entienda y cumpla la presente política.
- Todo proveedor proporcionará los datos completos de la persona de contacto, quien será el encargado de recibir todo tipo de documentación referente a la seguridad de la información.
- El proveedor deberá cumplir los siguientes puntos respecto a su personal:
  1) El proveedor deberá garantizar que los antecedentes profesionales, judiciales, penales y policiales del personal que forma parte del servicio, a fin de garantizar a la organización que no exista ningún tipo de sanción aplicado en la actualidad.
  2) Tomar Conciencia, educarse y capacitarse en temas relacionados a seguridad de la información, según sea relevante para las actividades relacionadas al servicio que brinda a Adinelsa.
  3) En el caso de que se realice cualquier cambio en el personal como baja, sustitución o cambio de funciones o responsabilidades el proveedor deberá informarla a la institución para que se tomen las medidas o se inicie el procedimiento correspondiente. Si el cambio es aprobado y se realiza, el proveedor se asegura que se cumpla con el punto 1 y 2.
  4) El proveedor se asegurará que solo se realicen las actividades que están mencionadas en el contrato y/o términos de referencia correspondiente al servicio prestado. Además, debe garantizar el cumplimiento del contrato y en algunos casos los acuerdos de niveles de servicio que formen parte del servicio prestado.
  5) Todo proveedor deberá velar que el personal que presta los servicios directamente a la ADINELSA cumpla con los lineamientos establecidos en la presente política. En caso de incumplimiento, la organización se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de la institución de resolver el contrato de prestación de servicios en los términos establecidos en el contrato o términos de referencia.
  6) El proveedor garantizará que todo intercambio de información entre el ADINELSA y el proveedor durante la ejecución del servicio tendrá **carácter confidencialidad** y no podrá ser utilizada ni manipulada fuera del marco establecido en el contrato de prestación de servicios.
  7) El proveedor deberá garantizar que todo su personal que realiza servicios para la institución cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondiente a la actividad asociada, como de manera transversal en materia de seguridad de la información.
  8) En el caso de que el proveedor conozca de cualquier pérdida, uso no autorizado, revelación de la información proporcionada o de propiedad de la institución o cualquier otro evento/debilidad/incidente o de la que se sospecha en cuanto a la seguridad de la información de los sistemas o servicios, deberá advertir y reportar inmediatamente a través de los canales de seguridad de la información proporcionados

Elaborado por:	**Revisado por:**	**Homologado por:**	**Aprobado por:**
Julius K. Villavicencio Monti – **Oficial de Seguridad de la Información Subgerente de Planeamiento y Control de Gestión**	Teofilo Chambilla Aquino **Líder de Gobierno y Transformación Digital**	Julius K. Villavicencio Monti – **Subgerente de Planeamiento y Control de Gestión**	Jorge Herbozo Perez- Costa **Gerente General (e)**
Firma: Firmado digitalmente por: VILLAVICENCIO MONTI Julius Korel FAU 20425809882 hard Fecha: 26/09/2023 08:17:11	**Firma:** Firmado digitalmente por: CHAMBILLA AQUINO Teofilo FAU 20425809882 hard Fecha: 26/09/2023 09:37:28	**NO APLICA**	**Firma:** Firmado digitalmente por: HERBOZO PEREZ COSTA Jorge Luis Pelayo FAU 20425809882 hard Fecha: 26/09/2023 11:46:03

y/o al correo segurinfo@adinelsa.com.pe; en caso que fuera necesario, debiendo adoptar todos los pasos necesarios para ayudar a la entidad a remediar tal uso no autorizado o revelación de la información.

9) El proveedor deberá garantizar que todos los recursos que la institución le proporcione sean utilizados únicamente para cumplir con las actividades del servicio prestado.
10) El proveedor que cuente con equipos de cómputo propios, el cual utilicen para cumplir sus actividades de servicio dentro de la organización, deberán cumplir con los controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.
11) Todo proveedor deberá de tener en cuenta que la información de la organización no debe ser utilizada para beneficio propio o de terceros y solo deberá ser utilizada para los fines establecidos en el contrato de prestación de servicios.
12) Todo proveedor es responsable de transmitir y hacer cumplir la presente política a terceros subcontratados, autorizados debidamente por la organización.
13) El proveedor deberá garantizar que toda información que fue recibida durante la ejecución del servicio prestado deberá ser eliminada de su poder al finalizar el servicio.
14) Todo proveedor se asegurará de cumplir todas las obligaciones de confidencialidad aún culminado el contratado de prestación de servicios por cualquier motivo.
15) Los terceros deberán registrar al momento de su entrada, en el control de ingreso, el ingreso de equipos de cómputo, y herramientas que no sean propiedad de ADINELSA.
16) El servicio entregado por terceros según su criticidad e impacto en la continuidad del negocio, deberán incluir parámetros de seguridad de información dentro del contrato establecido con ADINELSA o del acuerdo de nivel de servicio (SLA – service level agreement), de ser el caso y contemplar penalidades ante el incumplimiento.
17) El nivel de servicio de los terceros respecto a temas de tecnología debe ser evaluado y aceptado por la oficina de tecnologías de la información y comunicaciones, con opinión previa de seguridad de información (de corresponder).
18) En el caso que el servicio incluya la creación de una cuenta de correo electrónico de la institución, está debe ser usada para el desempeño de las funciones asignadas dentro de la institución.
19) Los administradores de servidores, bases de datos y demás roles que manejen información clasificada como confidencial, deben garantizar la confidencialidad de la información y el uso de credenciales de administración (usuario y contraseña), sin excepción.
20) El servicio de acceso remoto deberá permitir el acceso a la red de datos a aquellos usuarios externos expresamente autorizados por el usuario del servicio y que lo haya solicitarlo mediante el Formato S3.1.3-FT01 Alta, Baja o Modificación de Usuario, el cual debe estar sujeto a autenticación con un nivel adecuado de protección y obedecer a necesidades justificadas.
21) No se debe proveer información sobre la ubicación del centro de procesamiento de datos o de los lugares críticos, como mecanismo de seguridad.
22) El proveedor deberá garantizar que el servicio prestado puede ser periódicamente monitoreado para verificar su cumplimiento.

Elaborado por:	Revisado por:	Homologado por:	Aprobado por:
Julius K. Villavicencio Monti – **Oficial de Seguridad de la Información Subgerente de Planeamiento y Control de Gestión**	Teofilo Chambilla Aquino **Líder de Gobierno y Transformación Digital**	Julius K. Villavicencio Monti – **Subgerente de Planeamiento y Control de Gestión**	Jorge Herbozo Perez- Costa **Gerente General (e)**
Firma: Firmado digitalmente por: VILLAVICENCIO MONTI Julius Korel FAU 20425809882 hard Fecha: 26/09/2023 08:17:11	**Firma:** Firmado digitalmente por: CHAMBILLA AQUINO Teofilo FAU 20425809882 hard Fecha: 26/09/2023 09:37:28	**NO APLICA**	**Firma:** Firmado digitalmente por: HERBOZO PEREZ COSTA Jorge Luis Pelayo FAU 20425809882 hard Fecha: 26/09/2023 11:46:03