POLÍTICA DE SEGURIDAD DE PROVEEDORES

El Centro de Arbitraje Latinoamericano e Investigaciones Jurídicas – CEAR LATINOAMERICANO – establece esta política con el propósito de garantizar la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso proveedores críticos, es decir, aquellas terceras partes o entidades externas cuya intervención pueda afectar de manera significativa la confidencialidad, integridad o disponibilidad de la información de la organización, o la continuidad de sus servicios.

Antes de iniciar la ejecución de contratos con *proveedores críticos*, se deben suscribir los respectivos acuerdos de confidencialidad, los cuales deben incluir:

1. Cláusulas de confidencialidad, asegurando la protección de la información.
2. Compromisos en materia de seguridad de la información, aplicables durante y después de la vigencia del contrato.

Asimismo, se deben establecer mecanismos de control en las relaciones contractuales con *proveedores críticos* para garantizar que:

1. La información a la que tengan acceso los proveedores cumpla con las políticas de seguridad y privacidad de la información de la organización.
2. Los servicios provistos por los proveedores cumplan con los estándares de seguridad establecidos.

Las políticas de seguridad de la organización deben ser difundidas por los funcionarios responsables de la elaboración y/o firma de contratos o convenios con *proveedores críticos*.
Por otro lado, los contratos o acuerdos con los proveedores deben incluir una cláusula de terminación en caso de incumplimiento de las políticas de seguridad y privacidad de la información.
En este sentido, la organización ha definido las siguientes cláusulas:

I. ACUERDO DE CONFIDENCIALIDAD

a. El acuerdo de confidencialidad debe ser firmado, sin excepción, por cualquier proveedor crítico con el que se establezca un intercambio de información.
b. Este acuerdo debe estipular que el acceso a los datos vinculados al servicio prestado a la organización solo podrá ser realizado por personas y/o entidades formalmente autorizadas.
c. Debe incluir penalizaciones basadas en los daños potenciales derivados de la violación de la confidencialidad de la información.

Av. Faustino Sánchez Carrión N° 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
(01) 397 8586 / (51) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

II. REQUERIMIENTOS DE SEGURIDAD DE APLICACIONES Y/O SERVICIOS

a. Si el proveedor es responsable de aplicaciones o servicios informáticos, estos deben cumplir con los requerimientos de protección de la confidencialidad, integridad y disponibilidad, definidos por la organización. Dichos requerimientos deberán ser demostrados en función del activo que será gestionado, mediante uno o más de los siguientes controles:

   1. **Monitoreo:** El proveedor debe contar con mecanismos que permitan detectar incidentes de seguridad de la información en la aplicación utilizada para la prestación del servicio. El nivel de detección debe ajustarse a los requerimientos del activo involucrado.
   2. **Control de acceso:** Se deben presentar mecanismos de control de acceso a los servicios y datos manejados, en cumplimiento de la **PO-13 Política de Gestión de Acceso**. El acceso a la información de la organización por parte de proveedores debe limitarse estrictamente a lo necesario para cumplir con el servicio asignado.
   3. **Gestión de incidentes:** El proveedor debe notificar inmediatamente a la organización sobre cualquier incidente de seguridad de la información o ciberseguridad que pueda afectar los activos tecnológicos de la organización y/o sus clientes, ya sea directa o indirectamente.
   4. **Licenciamiento:** Todas las aplicaciones y servicios prestados por el proveedor deben contar con licencias vigentes, en conformidad con el marco legal y regulaciones aplicables.
   5. **Cumplimiento de políticas:** Las personas que actúan como proveedores de la organización deben seguir las Políticas de Seguridad y Privacidad de la Información. Como excepción, en caso de incumplimiento, el proceso disciplinario se gestionará bajo la figura de incumplimiento de contrato.

b. Las obligaciones de confidencialidad continuarán vigentes incluso después de la finalización del contrato por cualquier causa.
c. La organización se reserva el derecho de realizar auditorías extraordinarias, siempre que existan causas justificadas.
d. El proveedor debe comunicar oportunamente a la unidad orgánica usuaria del servicio cualquier cambio en el personal asignado a la prestación del servicio.

III. PROHIBICIONES DEL PROVEEDOR(A)

a. Usar los recursos proporcionados por la organización para actividades no relacionadas con el propósito del servicio.

Av. Faustino Sánchez Carrión N° 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
(01) 397 8586 / (51) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

b. Intentar y/u obtener, sin autorización explícita, otros derechos o accesos distintos a los que la organización haya asignado.
c. Intentar y/o acceder, sin autorización explícita, a áreas restringidas de la organización.
d. Revelar, modificar, destruir o dar mal uso a la información a la que tenga acceso.
e. Utilizar la información de la organización para beneficio propio o de terceros.
f. Realizar copias no autorizadas de software, en cumplimiento de la Ley sobre el Derecho de Autor.

IV. SEGUIMIENTO, REVISIÓN Y GESTIÓN DE CAMBIOS

a. CEAR LATINOAMERICANO realizará el seguimiento anual de los proveedores críticos que tengan acceso a información, servicios, plataformas, sistemas o recursos tecnológicos de la organización.
b. El seguimiento tendrá como finalidad verificar el cumplimiento de las obligaciones de seguridad de la información, confidencialidad, privacidad y continuidad del servicio establecidas en la presente política y en los acuerdos contractuales correspondientes.
c. La revisión de los proveedores críticos podrá considerar, según corresponda, el cumplimiento de cláusulas de confidencialidad, controles de acceso, licenciamiento, reporte de incidentes, protección de la información, uso adecuado de recursos tecnológicos y aplicación de las políticas internas de seguridad y privacidad de la información.
d. La revisión podrá realizarse de manera anual o cuando exista un cambio relevante en el servicio, en el personal asignado, en los accesos otorgados, en la tecnología utilizada o ante la ocurrencia de un incidente de seguridad.
e. Todo cambio relacionado con los servicios prestados por proveedores críticos deberá ser comunicado oportunamente a CEAR LATINOAMERICANO.
f. La comunicación de cambios deberá realizarse especialmente cuando exista modificación de personal asignado, cambio de herramientas tecnológicas, variación en los accesos, transferencia de información, subcontratación, actualización de aplicaciones o modificación del alcance del servicio.
g. Los cambios comunicados deberán ser evaluados por el área responsable antes de su implementación, con la finalidad de identificar posibles riesgos para la confidencialidad, integridad o disponibilidad de la información.
h. Cuando se identifiquen incumplimientos, desviaciones o riesgos asociados al proveedor crítico, CEAR LATINOAMERICANO podrá solicitar acciones correctivas, restringir accesos, actualizar acuerdos, reforzar controles, suspender temporalmente el servicio o aplicar las medidas contractuales correspondientes.

Av. Faustino Sánchez Carrión N° 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
(01) 397 8586 / (51) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe

i. La presente política será revisada y actualizada cuando existan cambios normativos, tecnológicos, contractuales, organizacionales o de seguridad que puedan afectar la relación con proveedores críticos.

Firmado Por Erika Mancilla Tamara

Organo de Gobierno

CEAR LATINOAMERICANO

Av. Faustino Sánchez Carrión N° 615
Edif. Vértice 22 Oficina 306 - Jesús María - Lima
(01) 397 8586 / (51) 957 540 053
arbitraje@cearlatinoamericano.pe
Web: www.cearlatinoamericano.pe