Cláusulas de seguridad para proveedores y socios

Cuando se redacta un contrato con un proveedor o socio, es necesario definir cuáles de las siguientes cláusulas se incluirán en el contrato (a terminología legal del acuerdo debe ser preparada por la persona responsable de asuntos legales):

1. Información sobre el servicio prestado, detallar la información que se pondrá a disposición para este objetivo y cómo se clasificará, incluyendo el mapeo de esquemas cuando la organización y el proveedor usan diferentes esquemas de clasificación.
2. Si el proveedor tiene derecho a tomar subcontratistas; si puede hacerlo, debe obtener el consentimiento escrito de parte de la organización con un detalle de controles que deben cumplir los subcontratistas.
3. Una definición de información clasificada y cómo ser regula el secreto comercial.
4. La duración del acuerdo y la obligación de mantener de forma confidencial y clasificada la información y/o los secretos comerciales luego del vencimiento del contrato (al redactar este artículo, se debe tener en cuenta cómo se garantizará la continuidad de negocio en la organización).
5. El derecho de la organización a acceder a información almacenada o procesada por el proveedor o socio.
6. El derecho de auditar o supervisar el uso de información confidencial y de supervisar la ejecución del contrato en las instalaciones del proveedor o socio, o si las auditorías pueden ser realizadas por terceros. Especificar los derechos de los auditores.
7. Las acciones requeridas luego del vencimiento del contrato (devolución, destrucción o borrado de información confidencial, devolución de equipos, etc.) para garantizar la protección de información confidencial y para asegurar la continuidad de negocio en la organización.
8. Identificación y uso de controles clave para garantizar la protección de los activos de la organización, por ej., controles físicos, controles para protección contra código malicioso, controles de protección física, controles para protege la integridad, disponibilidad y confidencialidad de la información, controles para asegurar la devolución o destrucción de activos de información después de ser utilizados, controles para evitar la copia y distribución de información, controles para la adquisición, desarrollo y mantenimiento seguros de sistemas de información y sistemas de seguridad de la información.
9. Garantizar el acceso a informes financieros, a informes de auditoría internos y externos y a otros informes relacionados con las actividades de negocio de los proveedores o socios que puedan ser importantes para la organización.
10. Responsabilidades y acciones de las partes para evitar que personas no autorizadas accedan a la información (por ej., solamente personas que necesitan el conocimiento pueden tener derechos de acceso a la información, etc.).
11. Identificar al propietario de la información y cómo se reglamentan los derechos de propiedad intelectual.
12. Uso permitido de información clasificada y activos relacionados; es decir, el método establecido para manejar ese tipo de información y activos.
13. Proceso para notificar a la otra parte del acuerdo sobre amenazas y vulnerabilidades de seguridad, así como el acceso no autorizado a la información, violaciones a la confidencialidad o cualquier otro incidente o incumplimiento contractual.
14. Definir el tiempo de respuesta a los incidentes y establecer un proceso de escalamiento para la resolución de problemas e incidentes.

Commented [AES1]: Para aprender a seleccionar cláusulas de seguridad, lea estos artículos:

[illegible]

15. Acciones resultantes por incumplimiento de contrato, responsabilidad del proveedor o socio por transacciones y demás actividades contratadas no ejecutadas o ejecutadas a destiempo o de forma incorrecta.
16. Conocimiento del proveedor o socio sobre políticas y procedimientos clave de la organización.
17. Obligación de los proveedores o socios de capacitar a los empleados para todas las actividades en las que están involucrados.
18. Comprobar que los proveedores o socios sean conscientes de la necesidad de seguridad.
19. Prohibir que los empleados de la organización pasen a los proveedores o socios cualquier activo de información sin la debida autorización del propietario del activo.
20. Nivel de servicio deseado y nivel de servicio no aceptable.
21. Definición de los criterios de medición de servicio, incluyendo el mantenimiento de los controles, y control y emisión de informes.
22. Una definición exacta del sistema y formatos de informes.
23. Un proceso de gestión de cambios claramente definido.
24. Sistema de control de acceso: definir los motivos para los derechos de acceso de terceros, procesos permitidos de inicio de sesión y claves, proceso de autorización para acceso y asignación de privilegios a usuarios determinados, obligación de llevar un registro de todos los usuarios y sus derechos de acceso, procesos para eliminar derechos de acceso.
25. Una cláusula que especifique claramente que todos los derechos de acceso no autorizados explícitamente están prohibidos.
26. El derecho para supervisar y anular cualquier actividad relacionada con los activos de la organización.
27. Controles para garantizar la continuidad de negocio de acuerdo con las prioridades de la organización: qué servicios deben ser recuperados dentro de qué plazos.
28. Responsabilidad por daño en caso de incumplimiento de relaciones contractuales, incluyendo responsabilidad patrimonial en caso de violación de confidencialidad de la información o en caso de no prestación de servicio.
29. Responsabilidad del proveedor o socio para almacenar datos en conformidad con las regulaciones.
30. Condiciones para prórroga o cancelación del contrato.
31. El idioma del contrato y de la comunicación futura entre la organización y los proveedores o socios.
32. Detalles sobre los requisitos legales, estatutarios, reglamentarios y contractuales que debe cumplir el proveedor, ya que se derivan de los requisitos que debe cumplir la organización.
33. Nivel de seguridad objetivo y nivel de seguridad inaceptable.
34. Requisitos de formación y concienciación para actividades de seguridad críticas específicas.
35. Contactos relevantes con respecto a asuntos comerciales y de seguridad de la información.
36. Requisitos de selección, cuando sea legalmente posible, para el personal del proveedor.
37. Proceso de resolución de conflictos.
38. Modificación de los contratos de trabajo de los empleados de los proveedores para incluir cláusulas de seguridad de la información que deben ser cumplidas por los mismos.
39. Roles y responsabilidades de seguridad de la información para la organización y el proveedor.
40. Controles gestionados por la organización y los gestionados por el proveedor de servicios en la nube.