Cláusulas de seguridad para proveedores

Cuando se redacta un contrato con un proveedor, es necesario definir cuáles de las siguientes cláusulas se incluirán en el contrato. (La terminología legal del acuerdo debe ser preparada por la persona responsable del área de jurídica):

1. Información sobre el servicio prestado, detallar la información que se pondrá a disposición para este objetivo y cómo se clasificará.
2. Si el proveedor tiene derecho a tomar subcontratistas; si puede hacerlo, debe obtener el consentimiento escrito de parte de la subsecretaría y un detalle de controles que deben cumplir los subcontratistas.
3. Una definición de información clasificada.
4. La duración del acuerdo y la obligación de mantener de forma confidencial y clasificada la información luego del vencimiento del contrato (al redactar este artículo, se debe tener en cuenta cómo se garantizará la continuidad del servicio en la subsecretaría).
5. El derecho de la subsecretaría a acceder a la información almacenada o procesada por el proveedor.
6. 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 del servicio en la subsecretaría.
7. Identificación y uso de controles clave para garantizar la protección de los activos de la subsecretaría; por ej., controles físicos, controles para protección contra códigos maliciosos, controles de protección física, controles para proteger 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.
8. Identificar al propietario de la información y cómo se reglamentan los derechos de propiedad intelectual.
9. Proceso para notificar a la otra parte del acuerdo sobre el acceso no autorizado a la información, violaciones a la confidencialidad o cualquier otro incidente.
10. Definir el tiempo de respuesta a los incidentes y establecer un proceso de escalamiento para la resolución de problemas e incidentes.
11. Acciones resultantes por incumplimiento de contrato, responsabilidad del proveedor por transacciones y demás actividades contratadas no ejecutadas o ejecutadas a destiempo o de forma incorrecta.
12. Conocimiento del proveedor sobre políticas y procedimientos clave de la subsecretaría.
13. Obligación de los proveedores de capacitar a los empleados para todas las actividades en las que están involucrados.
14. Comprobar que los proveedores serán conscientes de la necesidad de seguridad.
15. Prohibir que los funcionarios de la subsecretaría pasen a trabajar para los proveedores.
16. Nivel de servicio deseado y nivel de servicio no aceptable.
17. Definición de los criterios de presentación de servicio, control y emisión de informes.
18. Una definición exacta del sistema y formato de informes.
19. Un proceso de gestión de cambios claramente definido.
20. 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.
21. Una cláusula que especifique claramente que todos los derechos de acceso no autorizados implícitamente están prohibidos.

22. El derecho para supervisar y anular cualquier actividad relacionada con los activos de la subsecretaría.
23. Controles para garantizar la continuidad del negocio de acuerdo con las prioridades de la subsecretaría: qué servicios deben ser recuperados dentro de qué plazos.
24. Responsabilidad del proveedor para almacenar datos en conformidad con las regulaciones.
25. Condiciones para prórroga o término del contrato.
26. El idioma del contrato y de la comunicación futura entre la subsecretaría u los proveedores.

Creado por:

Ingeniero Proyectos T.I.C.
Daniel Coronado Rojo

Validado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DEPTO TECNOLOGIAS DE LA INFORMACION

Jefe Departamento T.I.C.
Rafael Reyes Cuevas

Aprobado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DIVISION ADMINISTRATIVA

Encargado de Seguridad de la Información
Jefe División Administrativa
Jorge Vega Saavedra