1. OBJETO

Los proveedores y contratistas resultan vitales para el crecimiento y la competitividad de las organizaciones, pero, **si no se cuenta con herramientas de protección adecuadas, dejan de ser un factor de crecimiento para convertirse en un elemento generador de riesgo.**

En el momento en que una organización considera compartir una parte de su proceso productivo con otra, también acepta compartir información vital y confidencial que, eventualmente, puede poner en riesgo la operación en caso de ser divulgada.

Antes de suscribir un acuerdo o firmar un contrato, conviene asegurarse de que la organización que actuará como proveedor hace uso de las mejores prácticas en cuanto a gestión de la calidad y de la seguridad de la información, basada en normas como ISO 9001 e ISO 27001.

La tercerización siempre implicará un riesgo. Eso es algo que debemos tener claro antes de subcontratar un proceso o establecer un acuerdo con algún proveedor. La Gestión de Proveedores en ISO 270001 considera las cláusulas de seguridad en los contratos como una herramienta para mitigar el riesgo, mas no para evitarlo.

2. DESCRIPCIÓN

Siempre que sea necesario por el tipo de relación que se tenga con el proveedor, habrá que incluir una serie de cláusulas en el contrato, presupuesto, acuerdo de colaboración, contrato de UTE… que regule nuestra relación y que nos garanticen la trazabilidad de la seguridad de la información.

Inclusión de **cláusulas** en los contratos con los proveedores:

- **Derechos a auditoría:** garantiza a la organización contratante, el derecho a evaluar y auditar los controles de seguridad implementados por el proveedor, en forma periódica o cuando se presenten cambios significativos en los controles o en la relación contractual entre ambas partes.
- **Notificaciones sobre infracciones en la seguridad**: esta cláusula obliga al proveedor a informar a la organización contratante sobre cualquier violación a la seguridad de la información que afecte sus operaciones o sus negocios.
- **Aceptación de las prácticas de seguridad**: con esta cláusula el proveedor declara que conoce y acepta sin restricciones las prácticas de seguridad de la información propuestas por el contratante, y que comunicará en forma oportuna, su imposibilidad de adherirse a alguna, algunas o todas ellas en un momento determinado.

- **Tiempo de respuesta ante una violación**: el proveedor debe comunicar al contratante los planes de tratamiento que contempla ante posibles violaciones de la seguridad, y los tiempos en que tendrán efecto esas acciones.
- **Demostración de cumplimiento**: el proveedor debe demostrar con evidencia irrefutable, que los controles que ha implementado y las acciones correctivas que ha diseñado cumplen con los requisitos contractuales. Es probable que esta demostración de cumplimiento requiera una auditoría o una verificación de algún tercero.
- **Control sobre la cadena de suministro**: el proveedor puede tener la necesidad de aplicar a otras organizaciones con las que suscriba acuerdos, las mismas políticas y condiciones que a él le ha impuesto la organización contratante, en la medida en la que se conforme una cadena de suministro.
- **Comunicación sobre cambios**: el proveedor debe informar a la organización contratante, todos los cambios en su entorno que afecten el negocio o la operación de su cliente, en forma oportuna.