LEGAL ARMY

COVID-19 Checklist

Medidas que puedes adoptar en tu empresa para controlar el riesgo provocado por el coronavirus.

Contractual.

- [ ] Revisa todos tus contratos, tanto si eres proveedor como cliente, para ver si existen cláusulas de fuerza mayor o acontecimientos fuera de tu control que puedan conllevar implicaciones para el cumplimiento de las obligaciones del contrato, como retrasos en la prestación del servicio, terminación anticipada sin penalizaciones, retraso en los pagos, etc.

- [ ] En caso de contar con clientes finales (personas físicas), analiza cómo puede afectar el cierre o la suspensión temporal de tu negocio a la relación contractual, y si existen previsiones legales que permitan ese cese temporal en la prestación de productos o servicios sin necesidad de penalización para tu empresa o de devolver las cantidades abonadas por el cliente por servicios no disfrutados argumentando causas de fuerza mayor (por ejemplo, en caso de suscripciones mensuales que no hayan podido ser utilizadas por cierre de los establecimientos).

- [ ] Valora, a través de los contratos firmados con proveedores, si existen cláusulas que les obliguen a tener un plan de continuidad de negocio, incluso en casos de fuerza mayor, para continuar con la prestación de sus servicios, aunque sea a través de servicios mínimos. A la inversa, valora también si como proveedor de servicios a tus clientes estás obligado a contar con planes de continuidad de negocio y de qué manera.

- [ ] Comprueba si tu empresa cuenta con los seguros necesarios para posibles pérdidas en caso de pandemias, así como si has exigido en tus contratos con proveedores que éstos cuenten con dichos seguros que cubran las posibles responsabilidades por suspensión temporal/terminación de los servicios, la imposibilidad de hacer frente a los pagos, etc.

Protección de datos y Seguridad de la información.

- [ ] Revisa las medidas, políticas y procedimientos de seguridad implantados en tu empresa para ver si cumplen con un nivel de seguridad adecuado para que los empleados puedan desarrollar sus funciones desde casa (teletrabajo) con total seguridad: comunicaciones seguras, bases de datos protegidas, controles de accesos adecuados, copias de seguridad actualizadas, etc.

- [ ] Revisa que todo el personal ha firmado las políticas de protección de datos internas: políticas de privacidad y protección de datos, código de conducta, confidencialidad, uso de dispositivos electrónicos, seguridad de la información, etc. Así mismo, verifica que dichas políticas incluyen menciones específicas al teletrabajo y a las obligaciones concretas del empleado en caso de llevarlo a cabo.

- [ ] Comprueba que todos los empleados pueden acceder a la información que necesitan para trabajar de forma segura a través de los medios habilitados para ello. Recuerda que el uso de medios de almacenamiento extraíbles (pendrives, discos duros externos) está totalmente desaconsejado.

- [ ] Comprueba que cuentas con políticas de continuidad de negocio, que permitan seguir con el desarrollo de la actividad de la compañía en casos de fuerza mayor, pandemias o desastres naturales, y que incluyan entre otras cuestiones los métodos implementados para mantener la seguridad y continuidad de la información en estos casos.

- [ ] Comprueba si tu empresa cuenta con un procedimiento relativo a la notificación de brechas de seguridad, y que todos los empleados están familiarizados con él y con lo que supone una brecha de seguridad, para que, en caso de que ocurra una violación de seguridad, sepáis cómo llevar a cabo dicha gestión.

Otras medidas.

- [ ] Revisa todas las políticas de privacidad de la compañía frente a terceros, tanto online como offline, avisos legales y políticas de cookies para tener actualizados todos los tratamientos de datos personales que se realizan en la compañía.

- [ ] Asegúrate de que el protocolo para la atención de derechos de los interesados funciona correctamente: se cuenta con un responsable para atender estas solicitudes, tiempo de contestación a las mismas, etc.

- [ ] Comprueba los distintos plazos aplicables a la conservación y destrucción de los datos.

- [ ] Responsabilidad proactiva y gestión de riesgos: revisa, evalúa y mejora las medidas de seguridad y organizativas en función del riesgo que conllevan los diferentes tratamientos de datos de carácter personal.