Cámara de Comercio de Bogotá

Lineamientos de Protección de Datos Personales para contratistas CCB

2023

Los puntos descritos a continuación especifican unos lineamientos mínimos a tener en cuenta.

Las condiciones para el tratamiento de datos pueden variar según el servicio que presten los contratistas, por lo que es posible que se requiera incluir lineamientos adicionales de acuerdo con el alcance de dicho servicio.

Lineamientos generales de PDP para proveedores

1. Tanto los lineamientos de seguridad y de protección de datos personales de la CCB como los requerimientos de seguridad de la información y de protección de datos establecidos para el servicio contratado deben ser conocidos y acogidos por el contratista, sus empleados y terceros que tengan relación con el desarrollo del contrato establecido con la CCB.

2. Los activos, accesos e información proporcionados por la CCB y/o los datos recopilados en el desarrollo del contrato, son únicamente para el desarrollo de las actividades objeto del contrato.

3. Al finalizar el contrato, el contratista debe certificar la devolución de los activos proporcionados, así como la entrega de la información, de las evidencias de autorización de tratamiento de datos obtenidas, y certificar su posterior eliminación, conforme a lo establecido en el contrato.

4. Los usuarios y las contraseñas asignadas para el acceso a los sistemas de la CCB son de uso individual para la persona a quien se le entregaron. Cada usuario es responsable de su adecuado manejo y protección y en caso de tener algún evento/incidente deberá reportarlo inmediatamente al supervisor del contrato.

Lineamientos generales de PDP para proveedores

5. Es responsabilidad del contratista usar en sus equipos software licenciado, tanto en los equipos propios como en los asignados por la CCB. En caso de que el equipo de cómputo sea asignado por la CCB, el software instalado debe ser el autorizado por la Vicepresidencia de Tecnología de acuerdo con los lineamientos y prácticas de la CCB.

6. Los equipos de cómputo y servidores (físicos o virtualizados) deben contar con soluciones de protección contra código malicioso, como por ejemplo antimalware, antivirus, antispam, XDR, entre otros.

7. Los datos personales privados, semiprivados o sensibles de clientes, proveedores, usuarios y colaboradores CCB son de carácter confidencial y están sujetos a los mecanismos de control definidos en los lineamientos y prácticas de Seguridad de la Información y el Manual para el tratamiento de los Datos Personales de la CCB.

8. En el caso de recopilar datos personales mediante mecanismos tales como: formularios de registro, listas de asistencia, contactos telefónicos en los que se soliciten datos, entre otros; la Oficina de Gestión de Riesgos de la CCB debe validar el mecanismo utilizado para la obtención de las autorizaciones de tratamiento de datos, así como el almacenamiento de la evidencia de dichas autorizaciones.

Lineamientos generales de PDP para proveedores

9. Debe establecerse contraseñas para los documentos o bases de datos que sean compartidos con la CCB o terceros autorizados que contengan información personal o confidencial. La contraseña debe ser entregada por un canal alterno o en un momento diferente a la información compartida. El uso de mecanismos alternos que protejan los datos al ser compartidos debe ser validado y aprobado por la CCB.

10. Para el envío de correos a múltiples destinatarios, se debe procurar utilizar los servicios de CRM establecidos por la Gerencia de Relacionamiento con el Cliente. Se debe evitar la divulgación de los correos, por lo que la información de los destinatarios NO debe ser visible para los receptores de las comunicaciones.

11. Está prohibida la creación y/o administración de grupos en plataformas de mensajería instantánea, como por ejemplo WhatsApp, Messenger, Telegram, entre otros; para el manejo de información de la CCB o de sus empresarios, sin la validación y aprobación del supervisor del contrato y de la Oficina de Gestión de Riesgos de la CCB.

Lineamientos generales de PDP para proveedores

12. El acceso a la red de la CCB desde redes externas por parte del contratista, deberá ser avalada por la vicepresidencia de tecnología y esta se realiza a través de la VPN y el mecanismo de autenticación que la CCB establezca. Los equipos de los contratistas que requieren conexión desde la red interna o externa deben cumplir como mínimo con: Sistema operativo:

    - Licenciado y actualizado Windows 8 en adelante.
    - Software detección de malware: instalado y con firmas actualizadas en los últimos 7 días.
    - Tener habilitado la actualización de parches del sistema operativo.

13. Se debe evitar el uso de redes wifi públicas para el desarrollo de las funciones del contratista en relación con la ejecución del contrato establecido con la CCB.

14. Los contratistas deben reportar a la CCB los incidentes de seguridad de la información, inmediatamente tengan conocimiento de los mismos, a través del correo electrónico incidentesdeseguridad@ccb.org.co y/o al supervisor del contrato.

15. Los contratistas deben reportar, independientemente de la gestión realizada, cualquier solicitud de clientes o terceros en relación con sus datos personales o incidentes que incluyan datos personales al correo protecciondedatos@ccb.org.co y/o al supervisor del contrato.

Lineamientos generales de PDP para proveedores

En caso de que el contratista provea y/o participe de la implementación de software:

1. Tanto la implementación de un nuevo software como la actualización de uno existente debe estar planeada, administrada, y formalmente documentada asegurando que durante su ciclo de vida los riesgos de seguridad de la información y protección de datos personales asociados sean mitigados, teniendo en cuenta la privacidad por diseño y en los casos que sea necesario desarrollando, desde la CCB, un Análisis de Impacto en la Privacidad (PIA).

2. En el desarrollo de sitios web o aplicaciones donde se requiera capturar, almacenar y realizar análisis de las cookies, se debe incluir la autorización para el uso de las mismas, de manera que:

    1. Solamente las cookies de servicio se mantengan activadas por defecto y se exponga al usuario la opción de aceptar o no cualquier otro tipo de cookies, estando por defecto deshabilitadas.

    2. La actualización para la aceptación de uso de cookies se realice máximo cada 6 meses o cuando se presentan cambios en los usos o las cookies utilizadas en la CCB.

Lineamientos generales de PDP para proveedores

En caso de que el contratista provea y/o participe de la implementación de software:

3. El sitio web o la aplicación debe contar con protocolos seguros de transferencia de información.
4. En el caso de cargar y mostrar información personal sin que exista una contraseña de acceso, la información correspondiente a datos personales de naturaleza sensible, privada o semiprivada debe ser enmascarada.

En caso de contratistas que cuenten con plataformas que incluyen la creación de usuario y contraseña para los clientes:

Se deben configurar políticas mínimas para crear contraseñas fuertes, así como establecer un mecanismo de olvido de contraseñas. La generación y entrega de los mecanismos de autenticación a los usuarios deben contar con condiciones de seguridad, evitando en todo momento enviar por correo o mensajes, usuarios y/o contraseñas de acceso en claro.