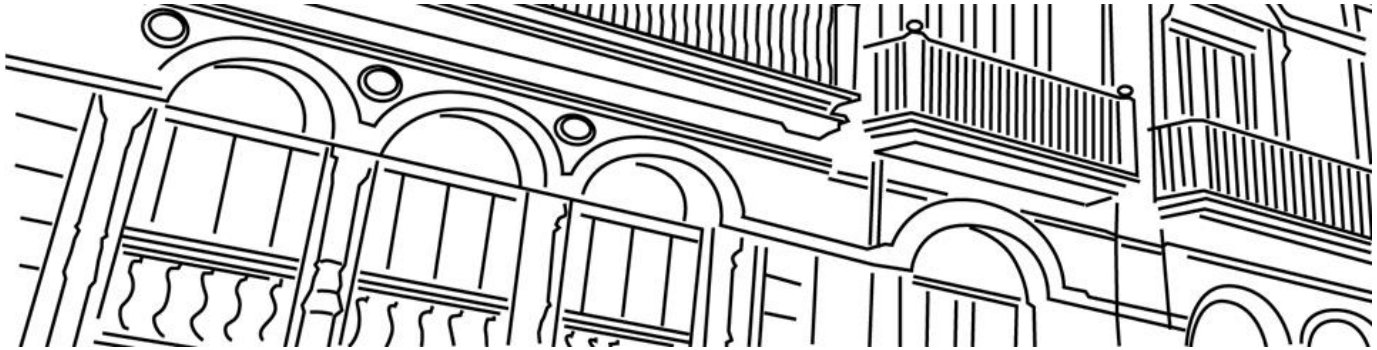

40 AÑOS BROSETA

Seminario Salud y Medios Digitales

Enero, 2017

FUNDACIÓN CEFi Centro de Estudios para el Fomento de la Investigación

ÍNDICE

1 CONSIDERACIONES GENERALES EN RELACIÓN CON LAS APPS.

1.1 CONTRATOS CON DESARROLLADORES.

1.2 T&C DE LAS APPS (CÓDIGOS DE CONDUCTA).

2 CONSIDERACIONES SECTORIALES EN RELACIÓN CON LAS APPS.

2.1 PATROCINIO-PUBLICIDAD.

2.2 ¿APPS PARA EL BIENESTAR O PRODUCTOS SANITARIOS? PRODUTOS FRONTERA.

3 CONSIDERACIONES SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN RELACIÓN CON LAS APPS.

3.1 DATO DE SALUD.

3.2 RÉGIMEN ACTUAL Y EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.

3.3 PRECEDENTES RELEVANTES EN RELACION CON LAS APPS.

3.4 PROPUESTA DE CÓDIGO DE CONDUCTA.

1 CONSIDERACIONES GENERALES EN RELACIÓN CON LAS APPS

1.1 CONTRATO CON DESARROLLADORES (i)

Contrato de obra *vs* Contrato de prestación de servicios. Obligación de resultado.

Cuerpo del contrato:

- Expositivo: voluntad de las partes y anexo descriptivo del proyecto.
- Objeto: diseño y desarrollo pero también integración, implementación y alojamiento/mantenimiento, en su caso + cesión derechos software (licencia uso).
- Cambios en el alcance: mecanismos de gestión. Seguimiento.
- Calendario de ejecución: recepción/aceptación parcial/es y definitiva/s. Entrega del código fuente.
- Calendario e hitos: penalizaciones y causa de terminación del contrato.
- Responsabilidades y garantías: autoría y originalidad, no infracción de derechos de terceros. Garantía de funcionamiento (distinto del mantenimiento correctivo).
- Condiciones económicas: conforme al calendario + incluye cesión derechos.
- Subcontratación: autorización previa.

1.1 CONTRATO CON DESARROLLADORES (ii)

- Protección de datos: servicios de mantenimiento (Art. 12 LOPD).
- Propiedad intelectual e industrial: principalmente, cesión de derechos de reproducción, distribución, comunicación pública y transformación. Derechos preexistentes.
- Finalización contractual: entrega materiales, código fuente.

Incluir en el Anexo:

- ✓ Descripción detallada de las características, especificaciones y funcionalidades de la aplicación.
- ✓ Acuerdo de nivel de servicio (SLA).
- ✓ KPIs asociados al cumplimiento del SLA.

1.2 T&C DE LAS APPS (CÓDIGOS DE CONDUCTA)

Cláusulas más relevantes:

- Acceso a la aplicación: regulación del acceso a la aplicación, identificación inequívoca, asignación de nombre de usuario y contraseña.
- Régimen de responsabilidad: utilización bajo responsabilidad del usuario (toma decisiones). P.ej: app médica la información proporcionada por la aplicación no debe sustituir la opinión de un facultativo.
    - Otros: exclusión/limitación responsabilidades contenidos; *links*; mal funcionamiento por causas ajenas (vulnerabilidad internet).
- Propiedad intelectual e industrial: régimen aplicable a los contenidos incluidos en la aplicación (no cesión de derechos) así como los que puedan generar los usuarios (P.ej: foros, blogs).
- Protección de datos: deber de información del artículo 5 de la LOPD.

Códigos de autorregulación y éticos: Código Hon (*Health on the Net*).

2 CONSIDERACIONES SECTORIALES EN RELACIÓN CON LAS APPS

2.1 PATROCINIO-PUBLICIDAD (i)

Patrocinio: forma de promoción publicitaria según Autocontrol.

Diferencia entre información y publicidad: principal nota diferenciadora, el objetivo de la comunicación que se realiza (inteded purpose).

Algunos casos sometidos al Tribunal de Justicia de la Unión Europea:

- **Caso Damgaard:** finalidad del mensaje, la persona que emite la información y el marco en que se difunde.
- **Caso Novo Nordisk:** no se exige que todos los elementos de la publicidad sean idénticos al resumen oficial, aunque sí que se ajuste.

Principios generales aplicables a la publicidad de medicamentos al público:

- ✓ Autorizados + no prescripción + no financiados con fondos públicos + no sustancias psicotrópicas o estupefacientes.
- ✓ Todos los elementos de la publicidad han de ajustarse a las informaciones que figuren en la ficha técnica.
- ✓ Ha de favorecerse en cualquier caso su utilización racional, presentando el medicamento de forma objetiva y sin exagerar sus propiedades.
- ✓ La publicidad no debe ser engañosa.

2.1 PATROCINIO-PUBLICIDAD (ii)

- **Código de Buenas Prácticas de la Industria Farmacéutica** (Tit. I, Capítulo I, "Promoción de medicamentos de prescripción"; Cap. 8 "Entorno Digital"):
  - Difusión en un contexto técnico-científico y difusión entre profesionales (facultados para prescribir o dispensar medicamentos).
  - Los laboratorios son responsables de los contenidos que promuevan, controlen o financien.
  - Deben establecerse internamente guías de uso (normas de conducta y de control de contenidos) así como pautas de actuación responsables para su observancia por los empleados.
- **Marketing y Publicidad de medicamentos en la IF: Entorno Digital (Salud 2.0)- Fundación Salud 2000**
  - LSSI: no responsabilidad de los prestadores de un servicio de intermediación (información subidas a la app por terceros) salvo conocimiento efectivo.
  - Relación IF-pacientes (RRSS generalistas): centrado en patología y prohibición publicidad medicamentos de prescripción
  - Relación IF-profesional sanitario (RRSS especializadas): identificación profesionales; congresos médicos en *streaming*; visita médica (soporte)…

2.2 ¿APPS PARA EL BIENESTAR O PRODUCTOS SANITARIOS? PRODUTOS FRONTERA (i)

- Coexisten en el mercado:
  - Apps que son devices (o accesorios de devices) y están sujetos a la normativa.
  - Otras apps (*stand alone software* no incorporado en un *medical device*) que obtienen y tratan información para el diagnóstico o seguimiento de los pacientes. Por ejemplo: obtención de datos a través de medidores del *smartphone*:
    - Frecuencia cardiaca.
    - Podómetro.
    - Pulsómetro.

- Problemática de los "**Productos frontera**" ⇨ Finalidad prevista por el fabricante ("*intended purpose*").

Documentación europea relevante:

- "*Medical Devices: Guidance document Qualification and Classification of Stand Alone Software*" de la Dirección General de Salud y Seguridad Alimentaria de la Comisión Europea.
- "*Manual on borderline and classification in the Community. Regulatory framework for medical devices*" del Working Group on borderline and classification for consultation.

2.2 ¿APPS PARA EL BIENESTAR O PRODUCTOS SANITARIOS? PRODUTOS FRONTERA (ii)

Cuestiones relevantes:

- ✓ Calificación como software.
- ✓ Incorporación del software en un producto sanitario (es un PS o un accesorio).
- ✓ Realización por parte del software de acciones (distintas del archivo, almacenamiento o transferencia de la información) en relación con los datos de manera autónoma.
- ✓ En beneficio del usuario: a partir de los datos incluidos por el usuario u obtenidos a través de sensores (no lo sería un agregador de datos de población afectada).
- ✓ Generación de alarmas y avisos de manera automática (la propia aplicación diagnostica).
- ✓ Diferencia entre distintos módulos de la aplicación.
- ✓ Finalidad para la que se utiliza la aplicación (Intended purpose- medical purpose).

3 CONSIDERACIONES SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN RELACIÓN CON LAS APPS

3.1 DATO DE SALUD

- ✓ **Directiva 95/46/CE**: otorga al dato de salud la categoría de especial.
- ✓ **Consejo de Europa en la Memoria del Convenio 108**: "informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo, pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Igualmente comprenden las informaciones relativas al abuso del alcohol o al consumo de drogas".
- ✓ **Consejo de Europa en la Recomendación nº R (97) 5** en el punto 1 del Apéndice: "los datos médicos hacen referencia a todos los datos de carácter personal relativos a la salud de una persona, afectando a los datos manifiesta y estrechamente relacionados con la salud así como a las informaciones genéticas".
- ✓ **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal: no contiene definición.
- ✓ **Real Decreto 1720/2007**, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

3.2 RÉGIMEN ACTUAL. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (i)

"Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética".

- ✓ Datos especialmente protegidos.
- ✓ Consentimiento expreso, excepciones artículo 7.6 LOPD.
- ✓ Interés Legítimo: no aplica en caso de datos de salud.
- ✓ Excepciones a la transferencia internacional de datos.
- ✓ Infracción muy grave: tratar o ceder datos de salud.
- ✓ Nivel de seguridad aplicable: **ALTO**.

3.2 RÉGIMEN ACTUAL. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (ii)

- Definición:
  - Datos relativos a la salud física o mental del interesado que revelen información relativa al estado de salud física o mental pasado, presente o futuro del interesado independientemente de su fuente (e.j. médico, hospital, un dispositivo médico).
  - Incluyen expresamente los datos de carácter personal recopilados durante la inscripción de una persona física a efectos de la prestación de servicios sanitarios o durante la prestación de tales servicios (cualquier número, símbolo u otro dato que le identifique) que revelen información sobre su estado de salud.
- Se incluye referencia expresa a los datos genéticos y los datos biométricos.
- Prohibición general de tratamiento salvo excepciones.

3.2 RÉGIMEN ACTUAL. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (iii)

- Licitud, consentimiento, información…
- Principio de *Accountability*: medidas y técnicas apropiadas para demostrar cumplimento.
- Designación del *Data Protection Officer ;*
  - Tratamiento de datos personales sensibles a gran escala.
  - Prestadores de servicios médicos; seguros; compañías farmacéuticas y *biotech* y compañías tecnológicas.
- Portabilidad.
- *Privacy by* design/Privacy by default.
- *Privacy Impact Assesment* (PIA): en caso de alto riesgo para los derechos y libertades de las personas.
- Documentación: políticas sobre los tratamientos de datos; sustitución de la declaración de ficheros.
- *Data Breach*: medidas de seguridad "reforzadas" a partir del *risk approach*.

3.2 RÉGIMEN ACTUAL. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (iv)

- Medidas de seguridad:
  - Aplicable a Responsables y Encargados del Tratamiento.
  - Medidas técnicas y organizativas "apropiadas" para garantizar un nivel de seguridad adecuado al riesgo ("*risk approach*") teniendo en consideración:
    - ✓ Estado de la técnica y costes de la aplicación.
    - ✓ Naturaleza, alcance, contexto y fines del tratamiento.
    - ✓ Riesgos para los derechos y libertades de las personas.
  - Sin embargo, no establece un listado estructurado de medidas ni prevé desarrollo o especificación ulterior.
  - La adhesión a un código de conducta o mecanismo de certificación como elemento para demostrar el cumplimiento (principio *accountability*).

3.3 PRECEDENTES RELEVANTES EN RELACION CON LAS APPS (i)

Health data in apps and devices – Article 29 Data Protection Working Party (Febrero, 2015)

Régimen estricto para el tratamiento de datos de salud (art. 8 directiva): prohibición general, salvo excepciones: el mal uso de estos datos puede tener consecuencias serias para los derechos del individuo.

✓Concepto dato de salud:

- ❑más amplio que los datos médicos: rotura de una pierna (caso Linquist) o llevar gafas, hábitos de alcohol o tabaco o alergias.
- ❑no tienen porque relacionarse necesariamente con padecer una enfermedad, de hecho, pueden referirse a la propensión a padecer una enfermedad (hábitos de vida, hábitos de dietas…).
- ❑reconoce la existencia de *grey areas:* hay muchos datos que por sí solos no serían datos de salud (peso, presión de la sangre o ritmo cardíaco o hábitos de sueño) pero combinados con otros, permiten alcanzar conclusiones sobre la salud del individuo.

✓En todo caso, sin perjuicio de los supuestos de habilitación legal para su tratamiento, deberá obtenerse el consentimiento expreso.

3.3 PRECEDENTES RELEVANTES EN RELACION CON LAS APPS (ii)

✓ Incide en tres aspectos capitales a considerar en el tratamiento de los datos:

- ❑ Transparencia: es consustancial al consentimiento. Si este no es informado, el consentimiento no es válido.
- ❑ Limitación del uso: cualquier uso distinto al médico (realizado por profesionales sanitarios) está estrictamente limitado. Deben definirse claramente los usos y finalidades, analizar si son compatibles y, en todo caso, obtener consentimientos.
- ❑ Seguridad: las técnicas de anonimización o pseudoanonimización y otras medidas de seguridad basadas en el *privacy by design* y *privacy by default* deben ser implementadas.

3.3 PRECEDENTES RELEVANTES EN RELACION CON LAS APPS (iii)

Opinion 1/2015, Mobile Health- European Data Protection Supervisor (Mayo, 2015)

- ✓ Reitera el régimen de especial protección a los que están sometidos los datos de salud.
- ✓ Los datos disociados (reversiblemente) o datos pseudoanimizados son datos de carácter personal.
- ✓ ¿Todo dato procesado en el ámbito del m – Health es dato sensible?:
  - ❑ Los datos sobre *lifestyle* o *wellbeing*, deben ser considerados datos sobre salud cuando: son tratados en un contexto médico y,
  - ❑ cuando de la información obtenida se puede inferir razonablemente información sobre salud, en particular, cuando la finalidad pretendida es monitorizar la salud o bienestar del individuo, independientemente de que se trate la información en el contexto médico o no.
- ✓ Análisis caso por caso: en caso de duda, el concepto de datos de salud debe ser interpretado de forma amplia.
- ✓ Dificultad de asignar responsabilidades a los distintos *players* (desarrolladores, sistemas operativos; fabricantes, *app stores* o terceros (*advertisers*)).
- ✓ Advierte del impacto del Big Data (*Internet of Things*; *wearable, computer devices*…) y la amplísima información que puede obtenerse a partir de muchas *apps* y *devices* contectados, revelando información sobre salud, comportamientos, hábitos, etc…

3.3 PRECEDENTES RELEVANTES EN RELACION CON LAS APPS (iv)

✓ Formula las siguientes reflexiones:

- ❑ Seguridad: garantizar la confidencialidad, integridad y disponibilidad de la información, conforme a la normativa sobre protección de datos; estándares internacionales o *best practices* (por ejemplo: Smartphone Secure *Development Guidelines* de ENISA).

- ❑ Transparencia; información completa y consentimiento libre para determinados tratamientos. Buenas prácticas:

  - ❖ Que el usuario pueda elegir que la información permanezca en el propio *device vs* servidor en remoto.

  - ❖ Que el usuario pueda elegir libremente la posibilidad de compartir con terceros la información.

- ❑ Diseño: es crucial que los diseñadores y fabricantes, faciliten al usuario políticas de privacidad *friendly* y *settings options* que les permitan el control sobre sus datos, con la información adecuada (*Privacy by desing*)

3.3 PRECEDENTES RELEVANTES EN RELACION CON LAS APPS (v)

Best Practices for Consumer Wearables & Wellness Apps & Devices (Future of Privacy Forum - USA) August, 2016

Aplicable a datos sobre *wellness, lifestyle* o *fitness*, fuera del contexto médico y por tanto de su utilización con fines médicos. Reconoce la dificultad de diferenciar estos datos sobre los datos de salud

Parámetros a considerar para concluir sobre dato de salud: (i) contexto y finalidades para los que se recogen; **(ii)** naturaleza de los datos **(iii)** accesibles a los médicos; **(iv)** si existe un clara conexión con la salud del individuo; **(v)** si son utilizados para medir o predecir riesgos relacionados con la salud o para facilitar la monitorización médica o si se pueden obtener conclusiones sobre el estado de salud del individuo.

Cita el criterio contenido en la Opinion 1/2015 del WP 29 pero también el emitido por este mismo grupo de trabajo en su *Letter- health data in apps and devices*, cuando señala que los datos que obtienen y tratan estos datos no siempre deben ser considerados datos de salud, refiriéndose como tales a los *raw* o *low impact personal data*.

3.3 PRECEDENTES RELEVANTES EN RELACION CON LAS APPS (vi)

Recomendaciones:

- ✓ Políticas claras y transparentes cuando se **informa**: qué datos, usos y finalidades, disociación, cesiones, periodo de conservación etc.
- ✓ Políticas sobre el **consentimiento** de los usuarios: consentimiento expreso para cualquier uso "material" o distinto al original o para su cesión a terceros, inclusive en caso de utilización posterior para finalidades de investigación científica.
- ✓ Finalidades **publicitarias o de marketing**: se desaconseja la venta o cesión a plataformas o brokers, exigiéndose un consentimiento, cuanto menos tácito (opt -out) para la publicidad en la app.
- ✓ **Limitación de uso**: prohibición absoluta para un uso relacionado en procesos de selección; riesgos crediticios o de seguros.
- ✓ Política para la **conservación** de la información en las apps.
- ✓ Programa de **seguridad**: medidas como pseudoanonimización; encriptación; revisión sobre su efectividad de forma recurrente.

3.4 PROPUESTA DE CÓDIGO DE CONDUCTA (i)

- ✓ Remitido por la Comisión Europea al Grupo del Artículo 29. Precedente: *Green paper on mobile Health (Abril, 2014)*.
- ✓ Cómo debe ser aplicada la normativa sobre protección de datos en relación con las mHealth apps.
- ✓ Focalizada en los desarrolladores (toman decisiones sobre la obtención y tratamiento de los datos).
- ✓ Concepto Dato de Salud:
  - ❑ Información sobre la situación física o mental.
  - ❑ Información de otro tipo (P.ej: servicios sanitarios o hábitos de vida o comportamientos) que revela el status de salud.
- ✓ Consentimiento: debe obtenerse;
  - ❑ Antes de iniciar el tratamiento de los datos.
  - ❑ De forma libre, específica e informada.
  - ❑ Granular (buena práctica).
  - ❑ Revocabilidad.

3.4 PROPUESTA DE CÓDIGO DE CONDUCTA (ii)

✓ Limitación del uso:

- ❑ Claramente definida.
- ❑ Se permiten otros usos, que sean "compatibles". Para determinar qué son compatibles, es necesario considerar:
  - ❖ Relación entre el uso inicial y el que se pretende.
  - ❖ El contexto en el que se obtienen y la expectativa del usuario.
  - ❖ La sensibilidad de la información y el impacto sobre su privacidad.
  - ❖ Garantías implementas para evitar un impacto indebido sobre la privacidad.
    - ❖ E.j.: nivel de concentración de azúcar en diabéticos- comercialización de los datos a laboratorios.

3.4 PROPUESTA DE CÓDIGO DE CONDUCTA (iii)

- ✓ Principio de **minimización** de datos (e.j.: edad concreta *vs* edad aproximada)
- ✓ **Transparencia**: información completa e inteligible.
- ✓ ***Privacy by Desing*** y ***Privacy by Default****:*
  - ❑ Diseño e implementación de la app observando la normativa (e.j.: proceso de elección del usuario sobre el tratamiento de sus datos y seguridad)
  - ❑ Por defecto o ante la inactividad del usuario, la app aplica la opción que implica menor injerencia de la intimidad.
- ✓ **Derechos** del individuo: acceso, rectificación, supresión, portabilidad…. Necesidad de que la app facilite el ejercicio efectivo de los derechos.
- ✓ **Como y cuando informar**: información por capas (la info + relevante antes de instalar, con posibilidad de fácil acceso al resto de la política de privacidad).
- ✓ **Conservación de los datos**: principio de calidad de los datos (necesidad). Buena práctica su eliminación (o anonimización) "de oficio" ante la inacción del usuario.

3.4 PROPUESTA DE CÓDIGO DE CONDUCTA (iv)

- ✓ **Medidas de seguridad**:
  - ❑ *Risk approach* a partir de la naturaleza de los datos y su impacto en la privacidad. Guías ENISA.
  - ❑ Necesidad de realizar un Privacy Impact Assessment (se contiene una guía).
  - ❑ Existencia de procesos para la gestión de riesgo y evaluación continua.
- ✓ **Publicidad en las apps**: permisible bajo ciertas condiciones.
  - ❑ Debe ser autorizada por el usuario
  - ❑ Si se trata de publicidad contextual (e.j.: sin acceso a datos ni *profiling*) se puede dar la opción del **opt-out**.
  - ❑ Si se trata de publicidad dirigida, **opt-in**.

3.4 PROPUESTA DE CÓDIGO DE CONDUCTA (v)

- ✓ Utilización de datos para **otros usos**:
  - ❑ Deben ser compatibles: investigación científica, histórica o estudios estadísticos lo son.
  - ❑ Recomienda la pseudoanonimización o anonimización de los datos.
  - ❑ Cualquier otro uso, necesitará con carácter general el consentimiento previo.
- ✓ **Cesión de datos**: las recomendaciones siguen el régimen existente y al previsto en el Reglamento General, tanto para la cesión como para el acceso (consentimiento, uso del tercero "compatible" con el originalmente, consentido, contrato vinculante con el tercero y responsabilidad "*in eligendo*" e "*in vigilando*".
- ✓ **Transferencia internacional**: las recomendaciones siguen el régimen actual y futuro. Especial incidencia en caso de *cloud computing*.

3.4 PROPUESTA DE CÓDIGO DE CONDUCTA (vi)

- ✓ ***Data breach***: procedimiento a seguir (además de actuar rápidamente para minimizar los daños):
  - ❑ Análisis sobre si afecta a datos personales.
  - ❑ Análisis de la conveniencia de informar a la autoridad y a los afectados.
- ✓ **Menores**:
  - ❑ La edad de referencia son los 16 años (Reglamento General), si bien en España parece que se mantendrá en 14 años.
  - ❑ Restringir al máximo la toma de datos y la posibilidad de que se recojan datos de sus familiares o amigos.
  - ❑ Verificar la obtención del consentimiento parental.

Madrid

Goya, 29 - 28001
Tel. + 34 91 432 31 44

Valencia

Pascual y Genís, 5 - 46002
Tel. + 34 96 392 10 06

Zúrich (Suiza)

Schützengasse, 4 - 8001
Tel. + 41 445 208 103

Santiago de Chile (Chile)

Apoquindo 3600 - Las Condes
Tel. +56 227 162 587

www.broseta.com | info@broseta.com