



## **Datos de configuración de la cuenta**

Ver: 1.0

## Índice

<b>Sección</b>	<b>Página</b>
<b>I. Codificación de caracteres</b>	3
<b>II. Idiomas para envío</b>	3
<b>III. Configuración de remitentes e email</b>	4
A. Configuración del Remitente	4
B. Los rebotes	5
C. Configuración subdominios para links e imágenes	5
D. Gestión de bajas	6
<b>IV. Configuración de la Base de Datos</b>	6
A. Tipos de campos y diseño del registro	6
B. Sincronización	8
<b>V. Configuración de los accesos y formación</b>	9
A. Usuarios y niveles de acceso	9
B. Formación	9
<b>ANEXO A – Configuración subdominio remitentes</b>	10
<b>ANEXO B – Configuración subdominio imágenes y links</b>	11
<b>ANEXO C – Importancia de las entradas de SPF y DKIM</b>	12

## I. Codificación de caracteres

La codificación en la que desarrollaremos los HTML para los envíos y la codificación en la que se hallarán los datos en la Base de Datos y en la que importaremos y sincronizaremos esos datos. Existen dos opciones de codificación ISO y UTF-8.

Tanto al nivel de html como al nivel de base de datos la principal diferencia entre UTF-8 e ISO radica en que uno interpreta más caracteres que el otro. UTF-8 (8-bit Unicode Transformation Format) es una codificación de caracteres de longitud variable para Unicode. (Unicode alberga millones de caracteres de todo el mundo, por lo que la compatibilidad de caracteres resulta mucho más extensa que con ISO).

Con respeto a la codificación del html, la diferencia entre una y otra de las dos codificaciones consta en que ISO tiene codificados los caracteres con acentos y los símbolos con su correspondiente código HTML (Ejemplo: á = &acute; ; ñ = &ntilde;) en cambio el UTF-8 exceptuando japonés y demás idiomas idiogramáticos, será irrelevante el idioma en el que se escriba ya que lo cogerá tal cual, se podrán usar acentos y símbolos y siempre se verán correctamente.

Al nivel de ficheros de datos la correspondiente codificación para Windows para ISO será ANSI. Si el fichero lleva esta codificación los datos se importará correctamente. Lo más recomendado es que se use UTF-8 de esta manera será más fácil al nivel de gestionar los datos tanto al nivel de html como al nivel de base de datos.

Importación / sincronización	UTF-8 <input type="checkbox"/>	ISO <input type="checkbox"/>
Envío HTML	UTF-8 <input type="checkbox"/>	ISO <input type="checkbox"/>

## II. Idiomas para el envío

XCampaign dispone de un listado de idiomas que se puede añadir a una cuenta. Es decir el contenido de un email se puede crear en tantas idiomas que queremos. Eligiendo correctamente los idiomas que necesitamos facilitará muchísimo el trabajo al nivel de gestión del email tanto en las creaciones como en las estadísticas.

Idiomas



### III. Configuración de remitentes e email

#### A. Configuración del remitente (sender)

Vamos a utilizar la palabra “**sender**” (remitente) para describir al email que vamos a utilizar para realizar los envíos. El sender se compone de un **email** *ej:comunicacion@c.datacentric.es* y una **descripción** asociada al email "Boletines Datacentric" (Alias | Nombre).

La **descripción** (o el **alias** como se puede encontrar en XCampaign) aparecerá como el nombre del remitente cuando los usuarios reciban el correo (dependiendo del idioma variara el nombre del sender).

El sender o el email del remitente es una cuenta de correo normal y corriente. La única diferencia es que solo XCampaign se tiene que tener acceso a esa cuenta.

Una parte importante del sender es la parte que viene después del “@”, en el ejemplo de arriba será “c.datacentric.es”. Esto se conoce como el dominio, o subdominio en este caso, del sender. Esta parte es muy importante y siempre se recomienda que se crea un subdominio para los senders que se utilizan en los envíos de emails. La justificación está en una medida de precaución: si algo pasa con sus envíos y el **subdominio** (**c.dominioempresarial.com**) del sender se ve penalizado por los distintos ISPs que su **dominio** (**dominioempresarial.com** – sin el c.) empresarial no será afectado también.

Por tanto se puede tener tres opciones:

1. Se puede utilizar como sender un sender de XCampaign. Practica muy poco recomendada porque el mismo dominio de XCampaign puede ser utilizado por otros clientes (ej: [ejemplo@mailprofiler.com](mailto:ejemplo@mailprofiler.com)).
2. Se puede utilizar vuestro dominio corporativo de mail sin crear ningún subdominio, por ejemplo tenéis [www.mycompany.com](http://www.mycompany.com) y vuestro email corporativo es [myemail@mycompany.com](mailto:myemail@mycompany.com). En este caso decidís crear una nueva cuenta de correo cuyos datos (la dirección del servidor de email, cuenta y contraseña) nos váis a pasar, por ejemplo: [comunicaciones@mycompany.com](mailto:comunicaciones@mycompany.com). Nosotros vamos a configurar el sender con estos datos y la descripción pero se tiene la desventaja comentada arriba que vuestro dominio corporativo se puede ver influido por las consecuencias relacionadas con los envíos del email. Por tanto no recomendamos esta opción.
3. **Se crear un subdominio cuya configuración está descrita en el Anexo A.** Es la opción que recomendamos.

Idioma	La descripción del sender (alias)	Email del sender (remitente)	POP3	IMAP4
<i>Español</i>	<i>Comunicación Digital</i>	<i>comunicaciones@c.vuestroDom.es</i>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>

			<input type="checkbox"/>	<input type="checkbox"/>
--	--	--	--------------------------	--------------------------

## **B. Los rebotes (bounces)**

Un rebote (bounce) es un email que se envía al mismo remitente utilizado en enviar los emails. Puede ser un email automático que envía un sistema de correo al remitente (sender) informando que se ha producido un error de entrega o que no se ha procesado un correo, o puede ser un email enviado por el mismo usuario como por ejemplo cuando contestamos a una comunicación preguntando detalles.

Siempre todos los rebotes llegan en XCampaign. Algunos se filtran porque son identificados como respuestas automáticas sin relevancia alguna, el resto se queda en XCampaign. Para estos hay dos tipos de configuraciones:

- **Primera** que los reenviemos todos a una cuenta de correo.
- **Segunda** que se queden en XCampaign y se gestiona desde nuestra interfaz.

En los dos casos vamos a necesitar una dirección de email donde se envíen los rebotes: en primer caso todos, en el segundo solo los que se consideran importantes o que necesita una atención personalizada (normalmente alguien del departamento comercial).

<b>Sender(remitente)</b>	<b>Email para reenviar los rebotes</b>

## **C. Configuración de subdominios para links e imágenes**

Dentro de XCampaign existe una galería de imágenes, donde se almacenarán aquellas imágenes que sean comunes para todos los emails, más las específicas de cada email.

Para el control de los clics, apertura, etc... el sistema lo que hace es substituir los link que lleve el email por links internos, donde recibe toda la información que necesita para elaborar el informe, una vez que el usuario pincha, el sistema registra el clic, y reenvía el link original que aparecía en el email.

En el caso de las imágenes y en el de los clic, los enlaces que se utilizan son: content.xcampaign.es y www.xcampaign.es respectivamente. En principio esto es totalmente operativo, pero algunos ISP podrían pensar que este email podría ser phishing o spam, ya que el remitente (sender) que enviará el email, será algo así como comunicacion@c.vuestrosubdominio.com y las url's que hay internas corresponden a xcampaign.es con lo cual podría verse reducido el número de emails entregados o que directamente vayan a la bandeja de Spam.

Para evitar esto, lo que se hace es crear subdominios que apunten a xcampaign.es, de esta forma el sistema automáticamente substituye los dominios de xcampaign, por los subdominios que ha creado el cliente.

# Datacentric XCAMPAIGN™ : Máximas funcionalidades – Mínima complejidad

Con estos subdominios, en realidad lo que se está haciendo es creando un desvío de las peticiones de ese subdominio a los servidores de xcampaign. Para vosotros es totalmente transparente y nos aseguramos que haya una coherencia dentro del email para asegurar una mejor entrega de los emails.

Los nombres de los subdominios son ficticios. Nosotros utilizamos c para correo, l para los links e i para imágenes pero podría ser cualquier subdominio.

Para ver detalles sobre cómo se debe configurar los subdominios para imágenes y links por favor consulta el **Anexo B**.

## D. Gestión de bajas

Vamos a elegir la modalidad de baja para los usuarios:

Se pondrá en el email un enlace, que cuando el cliente pulse se dará de baja directamente en XCampaign (sin confirmación) pero no en su CRM	<input type="checkbox"/>
Se pondrá un enlace en el email que vaya a una página, donde el cliente deberá confirmar la baja en XCampaign. Per no en su CRM.	<input type="checkbox"/>
Se pondrá un enlace que vaya a una página vuestra, donde el cliente podrá darse de baja pero luego se recomienda informar las bajas en XCampaign de alguna manera (webservice o importaciones)	<input type="checkbox"/>

## IV. Configuración de la Base de Datos

### A. Campos y diseño del registro

Los datos que se pueden almacenar en XCampaign son básicamente las que se puede almacenar en cualquier base de datos. La única diferencia es que son enfocados a segmentación de datos. Abajo es una clasificación de los tipos de campos que XCampaign dispone y sus códigos asociado que les ayuda rellenar el listado de campos de la siguiente página:

- **Campos de Texto (código TXT):** Este tipo de campos, almacenan cualquier valor.
- **Campos de selección con valores predefinidos (código SF o MSF):** Campo con múltiples valores (básicamente campos para numerar). Lo más importante de este campo es que tiene que ir con valores predefinidos. Estos campos son frecuentemente usados en la creación de selecciones. También es muy importante saber que un usuario puede tener uno o más de los valores predefinidas. En este caso se tiene que elegir el código **MSF**.
- **Intereses (código B):** Son campos binarios con valores "1" ó "0". Pueden tener una estructura jerárquica que les hace adecuados tanto para categorías como para sub categorías. Los intereses se asocian a los párrafos del email y cada vez que un usuario haga clic, ese interés quedará automáticamente asociado al él. Los intereses nos permiten obtener información sobre los gustos o preferencias de los clientes y posteriormente poder realizar segmentaciones más acordes a los distintos tipos de clientes que tenemos.
- **Fecha / Numérico (código F o N):** Campo que nos permite establecer rangos entre dos valores: numéricos o fechas. Cuando almacena campos numéricos: éstos son utilizados para crear selecciones del día a día, sin embargo el campo fecha podría estar utilizado para crear selecciones que serán utilizados en mailshot basados en eventos (comunicaciones transaccionales: el aniversario).

## Datacentric XCAMPAIGN™ : Máximas funcionalidades – Mínima complejidad

- **Campo Newsletter (código News):** Este tipo de campos sirven para asignar una Newsletter determinada a un usuario específico. Nos ayuda definir un listado de comunicaciones estándar de que disponemos y separar el comportamiento del usuario para cada una de ellas. En otras palabras, si un usuario se da de baja o alta a una comunicación no significa que se da de alta o baja a otra comunicación.
- **Selecciones externas (código SE):** Este tipo de campos son los que se utilizan para poder personalizar un correo electrónico con los datos de un fichero. Es decir la segmentación que queremos hacer se encuentra en un fichero externo. Pero aparte de los campos claves email o id, a lo mejor necesitamos que el email se personalice con el nombre. En este caso necesitamos crear estos tipos de campos y informarlos en el fichero que contiene la segmentación. **¡Muy importante!** Los registros tienen que existir ya en la base de datos cuando subamos el fichero, con este tipo de importaciones solo se realiza una segmentación no subida de registros.

En el listado de abajo puede rellenar los siguientes datos sobre los campos:

- **Nombre del campo:** la descripción con la que va a trabajar el usuario en XCampaign
- **Alias del campo:** que es el nombre de campo al nivel de bbdd. Este se va a utilizar para sincronizar la base de datos, por tanto tiene que respetar algunas normas: tiene que empezar con letra, no se permiten espacios, diacríticos, caracteres especiales. El único carácter permitido es el “\_”.
- **Tipo del campo:** es para elegir entre: **TXT, SF o MSF, F o N, SE** (para detalles mira la página anterior).
- **Si se sincroniza o no.** Es decir, si va incluido en el fichero de importación o exportación o en las llamadas al nuestro webservice.

Nr.	Nombre del campo	Alias del campo	Tipo	Se sincroniza?
1				<input checked="" type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>
11				<input type="checkbox"/>
12				<input type="checkbox"/>
13				<input type="checkbox"/>
14				<input type="checkbox"/>

## **B. Sincronización**

XCampaign tiene que estar al día con los datos de su CRM para que pueda aprovechar en la creación de las segmentaciones. Por tanto se dispone de varias modalidades de sincronización:

- **webservice:** muchas veces es necesario sincronizar información puntual que el usuario mismo lo cambia en vuestro CRM con XCampaign. Para estos tipos de sincronización, especialmente si del dato del usuario dependen algunos email transaccionales, se aconseja la sincronización via webservice.

- **Importaciones/exportaciones:** la sincronización masiva de datos es recomendable hacerse vía importaciones de datos desde ficheros. También desde XCampaign se puede exportar datos con tareas programadas a cierta hora para dejar ficheros en un sitio ajeno de XCampaign como por ejemplo un **sftp**. Nosotros podemos poner a su disposición este sftp en caso que no dispone de uno. **En estos ficheros siempre se tiene que incluir los “alias de los campos” como se han definido en la página anterior. Se pueden sincronizar altas como bajas igual.**

Si elige realizar la sincronización utilizando importaciones/exportaciones de ficheros por favor rellene el siguiente listado:

Nr.	Nombre de fichero	Tipo de subida (Manual o SFTP)	Tipo (XML o CSV)	Hora (para tareas automaticas)
1				
2				
3				
4				
5				
6				

Si elige realizar una sincronización (online) vamos a necesitar un listado de IPs de donde se conecta para poder habilitarlo en nuestro sistema. También es necesario que les pasamos unos datos para que se puede conectar.

Nr.	IP
1	
2	
3	
4	

## V. Configuración de los accesos y formación

### A. Usuarios y niveles de acceso

Necesitaremos la información de los usuarios que tendrán acceso con privilegios dentro de la herramienta (administradores, creadores de contenido, etc...).

En XCampaign tenemos distintos roles que se pueden asignar a un usuario:

- **Manager:** acceso a todas las secciones
- **Reportes:** acceso a los reportes
- **Marketing:** creación de campañas, lanzamiento de campañas y acceso a reportes
- **Segmentaciones:** acceso solo a segmentaciones
- **A su medida:** en este caso se tiene que especificar que derechos se necesita para que creamos un role a medida.

Nombre	Apellido	Email	Derechos
Usu1	Ape1	<u>Usu1@dominio.com</u>	Uno de los valores de arriba

### B. Formación

Se debe fijar una fecha para poder daros la formación de uso de la herramienta. La fecha que nos propongáis inicialmente podrá sufrir variaciones en función de de disponibilidad de nuestro equipo técnico, que serán los encargados de realizar la formación.

\_\_\_\_\_ De \_\_\_\_\_ Del \_\_\_\_\_

## **ANEXO A – Configuración subdominio remitentes**

Para configurar correctamente el dominio del remitente se necesitan varias entradas en el DNS asociadas al este subdominio.

Este subdominio requiere la creación de una entrada tipo **A**<sup>1</sup> apuntando a 95.168.208.136. La elección de la letra “c.” es nuestra pero se podría utilizar cualquier nombre de subdominio que os viene mejor.

```
name = c.vuestrodominio.com, address = 95.168.208.136
```

Además este subdominio también debe llevar una entrada tipo **MX**<sup>2</sup> apuntando a [bounce.xprofiler.es](https://bounce.xprofiler.es)

```
name = c.vuestrodominio.com, exchange = bounce.xprofiler.es
```

Además debemos crear dos entradas de tipo **TXT**<sup>3</sup>, para activar SPF y DKIM (para autenticación de los remites y evitar que nos paren por posible phishing<sup>4</sup>). Para la importancia de estas entradas se puede leer el **Anexo C**.

### **Entrada TXT – SPF.**

Valor entrada TXT:

```
c.vuestrodominio.com IN TXT v=spf1 mx include:_spf4.xcampaign.es  
include:_spf6.xcampaign.es ~all
```

### **Entrada TXT - DKIM.**

Para el DKIM se necesita crear un subdominio con el nombre:

**xprofiler.\_domainkey.c.vuestrodominio.com** y a este subdominio asociamos una entrada **TXT** con el valor (el valor va solo en una línea).

Valor entrada TXT →

```
xprofiler._domainkey.<c.vuestrodominio.com> IN TXT "v=DKIM1; g=*; k=rsa;  
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC9XhDuRmab2n+Sex8ENkSXR8BjiW6TExy81Qwg0wZPW  
aRZy5Ug0PhgfaoyUpHEbVONrz4QpUXsH1L1vVgibJDFk+87pJ+ng8Gi+Oj42wna26aYqqtYtUmvPfeqcVTs  
3ZxPa/E6MapQK6Ap1wNLJsD2cE3q+gmBXFu0Z7nptESIkwIDAQAB"
```

<sup>1</sup> **A** (Dirección) Este registro se usa para traducir nombres de servidores de alojamiento a direcciones IPv4

<sup>2</sup> **MX** (Registro de Intercambio de Correo) Tipo de Registro DNS. Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

<sup>3</sup> **TXT** (Información textual) Permite a los dominios identificarse de modos arbitrarios

<sup>4</sup> **Phishing** o suplantación de identidad se basa en intentar adquirir información confidencial de forma fraudulenta.

## **ANEXO B – Configuración subdominio imágenes y links(enlaces)**

### **Subdominio links:**

Un registro DNS de tipo **CNAME**<sup>5</sup> apuntando a [www.xcampaign.es](http://www.xcampaign.es) (este subdominio lo utilizaremos para traquear los link y poder generar los informes)

```
name = 1.vuestrodominio.com, cname = www.xcampaign.es
```

### **Subdominio imágenes:**

Un segundo registro DNS de tipo **CNAME** apuntando a [content.xcampaign.es](http://content.xcampaign.es) (este subdominio lo utilizaremos para almacenar las imágenes de las plantillas)

```
name = i.vuestrodominio.com, cname = content.xcampaign.es
```

---

<sup>5</sup> **CNAME** (Nombre Canónico) Tipo de registro DNS. Se usa para crear nombres de servidores de alojamiento adicionales, o alias.

## **ANEXO C- Importancia de SPF y DKIM**

**SPF** (Convenio de Remitentes, del inglés **Sender Policy Framework**) es una protección contra la falsificación de direcciones en el envío de correo electrónico identifica, a través de los registros de nombres de dominio (DNS), a los servidores de correo SMTP autorizados para el transporte de los mensajes. Este convenio puede significar el fin de abusos como el spam y otros males del correo electrónico. Para la entrada que hemos proporcionado antes:

```
“v=spf1 mx include:_spf4.xcampaign.es include:_spf6.xcampaign.es ~all”
```

**v=** define la versión usada de SPF (versión 1).

**mx** autoriza a las máquinas con la IP de los registros MX.

**~all** sugiere desautorización a las máquinas que no encajen en lo autorizado explícitamente.

El proceso de verificación SPF en el servidor de correo del destinatario consiste en comprobar los registros DNS del dominio del remitente. Si la dirección IP del servidor que ha conectado encaja en la especificación de direcciones permitidas en el registro SPF entonces se añade una cabecera de título Received-SPF indicando el resultado positivo de la comprobación.

Los programas lectores de correo harán uso de SPF para clasificar el correo justo al contrario del criterio de la carpeta de spam, llevando a la carpeta de entrada el correo verificado por el servidor del destinatario. Examinando las cabeceras de un mensaje verificado por SPF podría observarse la cabecera Received-SPF:

**DKIM** (Correo de Claves de Dominio Identificadas, del inglés **DomainKeys Identified Mail**) es un mecanismo de autenticación de correo electrónico que permite a una organización responsabilizarse del envío de un mensaje, de manera que éste pueda ser validado por un destinatario.

Dicha organización puede ser una fuente directa del mensaje, como el autor, el servidor encargado de gestionar el correo de ese dominio, o un servidor intermedio situado en el tránsito que recorre dicho correo, como por ejemplo un servicio independiente que provee recursos de correo al servidor que gestiona el dominio principal. La necesidad de este tipo de autenticación surge por la falsificación de contenidos de las que hace uso el spam.

La principal ventaja de este sistema para los receptores de e-mail es que permite firmar el dominio de manera que se puede identificar de manera fiable el flujo de correo legítimo, lo que permite que la utilización de listas blancas o negras basadas en dominio sean mucho más efectivas.

DKIM también protege contra la manipulación de correo electrónico, proporcionando integridad de extremo a extremo, desde un módulo firmante a un módulo validador. En la mayoría de los casos el módulo firmante actúa en nombre de la organización originaria insertando una firma DKIM en las cabeceras del mensaje, y el módulo de comprobación en nombre de la organización del receptor, validando la firma obteniendo la clave pública del firmante a través del DNS