



# CÓDIGO ÉTICO DEL PROVEEDOR DE FUNDICIONES FUMBARRI-DURANGO, S.A.

## Contenido

<b>1. Introducción</b>	3
<b>2. Ética</b>	3
<b>2.1. Corrupción</b>	4
<b>2.2. Conflicto de intereses</b>	4
<b>3. Prácticas Laborales</b>	4
<b>3.1. Trabajo forzoso</b>	5
<b>3.2. Trabajo infantil</b>	5
<b>3.3. Derecho de asociación y negociación colectiva</b>	5
<b>3.4. Igualdad de oportunidades y no discriminación</b>	5
<b>3.5. Remuneración justa</b>	5
<b>4. Salud y Seguridad</b>	5
<b>4.1. Protección del trabajador</b>	6
<b>4.2. Potenciales situaciones de emergencia</b>	6
<b>4.3. Capacitación y competencia</b>	6
<b>5. Medio Ambiente</b>	6
<b>5.1. Aspectos ambientales</b>	6
<b>5.2. Desechos y emisiones</b>	6
<b>6. Calidad y Seguridad del Producto</b>	7
<b>6.1. Requisitos legales y del cliente</b>	7
<b>7. Seguridad de la Información</b>	7
<b>7.1. Directrices Generales</b>	7
<b>7.1.1. Confidencialidad de la información</b>	8



<b>7.1.2. Propiedad intelectual</b>	9
<b>7.1.3. Intercambio de información</b>	10
<b>7.1.4. Uso apropiado de los recursos</b>	11
<b>7.1.5. Responsabilidades de la persona usuaria</b>	12
<b>7.1.6. Equipo de persona usuaria</b>	15
<b>7.1.7. Gestión del equipamiento hardware</b>	16
<b>7.2. Directrices específicas</b>	17
<b>7.2.1. Ámbito de aplicación</b>	17
<b>7.2.2. Selección de personas</b>	19
<b>7.2.3. Auditoría de seguridad</b>	19
<b>7.2.4. Comunicación de incidencias</b>	20
<b>7.2.5. Seguridad física</b>	20
<b>7.2.6. Gestión de activos</b>	21
<b>7.2.7. Arquitectura de seguridad</b>	22
<b>7.2.8. Seguridad de sistemas</b>	22
<b>7.2.9. Seguridad de red</b>	24
<b>7.2.10. Trazabilidad de uso de los sistemas</b>	26
<b>7.2.11. Control y gestión de identidades y accesos</b>	26
<b>7.2.12. Gestión de cambios</b>	27
<b>7.2.13. Gestión técnica de cambios</b>	27
<b>7.2.14. Seguridad en desarrollo</b>	28
<b>7.2.15. Gestión de contingencias</b>	29
<b>7.3. Seguimiento y control</b>	29
<b>8. Implementación del Código y Auditorías</b>	29
<b>9. Comité de Ética y Canal de Denuncias</b>	30



## **1. Introducción**

El Código Ético del Proveedor de Fundiciones Fumbarri-Durango S.A. define los estándares mínimos de comportamiento ético y responsable que deben ser observados por los proveedores y fabricantes de productos que comercializa Fundiciones Fumbarri-Durango S.A. en el desarrollo de su actividad, de acuerdo con la cultura empresarial de Fundiciones Fumbarri-Durango S.A., firmemente asentada en el respeto de los derechos humanos y laborales.

Fundiciones Fumbarri-Durango S.A. se compromete a poner los medios necesarios para que los proveedores y fabricantes conozcan y comprendan el presente código y puedan asumir su cumplimiento.

El Código es de aplicación a todos los fabricantes y proveedores que intervienen en los procesos de compra, fabricación y acabado, y promueve y se asienta en los principios generales que definen el comportamiento ético de Fundiciones Fumbarri-Durango S.A.:

- Todas sus actividades se desarrollarán de manera ética y responsable.
- Toda persona que mantenga, directa o indirectamente, una relación laboral, económica, social o industrial con la empresa, recibirá un trato justo y respetuoso.
- Todas sus actividades se desarrollarán de manera respetuosa con el medioambiente.
- Toda persona seguirá el marco normativo en relación con la seguridad de la información que accedan a información, sistemas de información o recursos, con el fin de proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Todos sus proveedores y fabricantes se adherirán íntegramente a estos compromisos y promoverán su responsabilidad para asegurar que se cumplan los estándares contemplados en el presente Código.

## **2. Ética**

Desarrollar las relaciones comerciales atendiendo a principios de ética empresarial y gestión transparentes:



## **2.1. Corrupción**

La relación de Fundiciones Fumbarri-Durango S.A. con sus proveedores y fabricantes se basa en la legalidad, eficiencia y transparencia. Fundiciones Fumbarri-Durango S.A. no tolera, permite o se involucra en ningún tipo de corrupción, extorsión o soborno en el desempeño de su actividad, ni en el sector público ni en el privado. El comportamiento ético y responsable es uno de los pilares de la actuación de Fundiciones Fumbarri-Durango S.A., y sus proveedores deben cumplir con las políticas, normas y procedimientos de Fundiciones Fumbarri-Durango S.A. relativas a la corrupción, el soborno y la extorsión.

Ningún proveedor o fabricante de Fundiciones Fumbarri-Durango S.A. deberá ofrecer o conceder a funcionarios públicos, a terceros o a cualquier empleado de Fundiciones Fumbarri-Durango S.A., en el contexto de la actividad empresarial desarrollada para o en nombre de este, directa o indirectamente, regalos, obsequios u otras ventajas no autorizadas, ya sean en metálico o en forma de prestaciones, con el objetivo de conseguir tratos de favor en la concesión o conservación de contratos o beneficios personales o para la empresa proveedora. Los actos de soborno, expresamente prohibidos, incluyen el ofrecimiento o promesa, directa o indirecta, de cualquier tipo de ventaja impropia, cualquier instrumento para su encubrimiento, así como el tráfico de influencias.

El proveedor cumplirá las normas más estrictas de conducta ética y moral, los convenios internacionales, respetando las leyes aplicables sobre esta materia, asegurando que se establecen los procedimientos adecuados que sean exigidos al efecto.

## **2.2. Conflicto de intereses**

El proveedor deberá mantener mecanismos que, en caso de potencial conflicto de intereses de alguno de sus empleados, garanticen la independencia del proveedor y su plena sujeción a la legislación aplicable.

## **3. Prácticas Laborales**

Respetar la protección de los derechos humanos y laborales fundamentales, reconocidos internacionalmente, dentro de su ámbito de influencia



### **3.1. Trabajo forzoso**

El proveedor deberá impulsar en sus acciones y adoptar las medidas necesarias en su organización para eliminar toda forma o modalidad de trabajo forzoso u obligatorio, entendido este como todo trabajo o servicio exigido a un individuo bajo la amenaza de una pena cualquiera.

### **3.2. Trabajo infantil**

El proveedor rechazará expresamente el empleo de mano de obra infantil en su organización, respetando las edades mínimas de contratación de conformidad con la legislación aplicable y contará con mecanismos adecuados y confiables para la verificación de la edad de sus empleados.

### **3.3. Derecho de asociación y negociación colectiva**

El proveedor respetará la libertad de asociación sindical y el derecho a la negociación colectiva de los trabajadores, con sujeción a las normas aplicables en cada caso.

### **3.4. Igualdad de oportunidades y no discriminación**

El proveedor deberá rechazar toda práctica discriminatoria en materia de empleo y ocupación, tratando a sus empleados de forma justa, con dignidad y respeto. A tal efecto, se calificará como discriminación cualquier distinción, exclusión o preferencia basada en motivos de raza, color, sexo, religión, opinión política, ascendencia nacional u origen social que tenga por efecto anular o alterar la igualdad de oportunidades o de trabajo en el empleo y la ocupación.

### **3.5. Remuneración justa**

El proveedor pagará a sus trabajadores de acuerdo con las leyes salariales aplicables, incluidos salarios mínimos, horas extras y beneficios sociales.

## **4. Salud y Seguridad**

Proporcionar un entorno laboral seguro, cumpliendo los requisitos establecidos en materia de prevención de riesgos laborales.



#### **4.1. Protección del trabajador**

El proveedor velará por la protección de sus trabajadores, protegiéndoles de la sobreexposición a peligros químicos, biológicos, físicos y de tareas que demanden sobreesfuerzo físico en el lugar de trabajo.

#### **4.2. Potenciales situaciones de emergencia**

El proveedor identificará y evaluará las potenciales situaciones de emergencia en el lugar de trabajo y minimizará el posible impacto mediante la implementación de planes de emergencia y procedimientos de respuesta ante emergencias.

#### **4.3. Capacitación y competencia**

El proveedor deberá dotar a su personal de la formación y los medios necesarios para realizar su trabajo conforme a lo contratado, y responder por cualquier daño o perjuicio cuya responsabilidad le sea imputable por acción u omisión, especialmente como consecuencia de no haber adoptado las medidas preventivas oportunas para evitarlo.

### **5. Medio Ambiente**

Mantener un enfoque preventivo que favorezca el medio ambiente, fomentado iniciativas que promuevan una mayor responsabilidad ambiental

#### **5.1. Aspectos ambientales**

El proveedor contará con una política medioambiental eficaz y que cumpla cuantas obligaciones le correspondan por la legislación aplicable.

#### **5.2. Desechos y emisiones**

El proveedor identificará y gestionará sustancias y otros materiales que representen un peligro al ser liberados al medio ambiente, a fin de garantizar su manipulación, traslado, almacenaje, reciclaje o reutilización y eliminación en condiciones seguras y cumpliendo con la normativa aplicable. Todos los desechos, aguas residuales o emisiones que tengan el potencial de afectar de manera desfavorable al entorno deberán ser administrados, controlados y tratados de manera apropiada.



## **6. Calidad y Seguridad del Producto**

Potenciar la mejora continua en la calidad de los productos y servicios suministrados

### **6.1. Requisitos legales y del cliente**

Todos los productos y servicios entregados por el proveedor deberán cumplir con los estándares y parámetros de calidad y seguridad requeridos por las leyes aplicables, prestando especial atención al cumplimiento de precios y plazos de entrega.

## **7. Seguridad de la Información**

### **7.1. Directrices Generales**

Cualquier tipo de intercambio de información que se produzca entre Fundiciones Fumbarri-Durango, S.A. y la organización proveedora se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada fuera de dicho marco ni para otros fines.

Sistemas centraliza los esfuerzos globales de protección de los activos de Fundiciones Fumbarri-Durango, S.A.

De forma genérica, los activos incluyen:

- La información protegida, es decir, aquella información que permite identificar a personas físicas y/o jurídicas, y aquella relativa a la configuración de los sistemas de información y las redes de comunicaciones.
- Los asociados para el tratamiento de la información protegida (software, hardware, redes de comunicaciones, soportes de información, equipamiento auxiliar e instalaciones).



### **7.1.1. Confidencialidad de la información**

Las personas externas que tengan acceso a información de Fundiciones Fumbarri-Durango, S.A. deberán considerar que dicha información, por defecto, tiene el carácter de protegida. Sólo se podrá considerar como información no protegida aquella información a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por Fundiciones Fumbarri-Durango, S.A.

Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en el que se encuentre.

Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior información protegida, salvo que esté debidamente autorizado.

Se minimizará el número de informes en formato papel que contengan información protegida y se mantendrán los mismos en lugar seguro y fuera del alcance de terceras personas.

En el caso de que, por motivos directamente relacionados con el puesto de trabajo, la persona empleada de la organización proveedora entre en posesión de información protegida contenida en cualquier tipo de soporte, deberá entender que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información. Asimismo, la persona empleada deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación con Fundiciones Fumbarri-Durango, S.A. de su empresa.

Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que las personas externas desarrollen para Fundiciones Fumbarri-Durango, S.A.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos.

Para garantizar la seguridad de los datos de carácter personal, las personas de la organización proveedora deberán observar las siguientes normas de actuación, además de las consideraciones ya mencionadas:



- Solo podrán crear ficheros cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán guardados en unidades locales de disco de los puestos PC de las personas usuarias y deberán ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
- No se albergarán datos de carácter personal en las unidades locales de disco de los puestos PC de persona usuaria.
- La salida de soportes y documentos (envío de e-mails incluido), fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por Fundiciones Fumbarri-Durango, S.A. y se realizará según el procedimiento definido.
- Los soportes y documentos deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido a las personas autorizadas.
- La transmisión de datos de carácter personal especialmente protegidos (p.ej. Salud), a través de redes de telecomunicaciones (p.ej. Correo electrónico) se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceras personas.

### **7.1.2. Propiedad intelectual**

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual.

Las personas usuarias únicamente podrán utilizar material autorizado por Fundiciones Fumbarri-Durango, S.A. para el desarrollo de sus funciones.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información de Fundiciones Fumbarri-Durango, S.A.

Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización por escrito.



Fundiciones Fumbarri-Durango, S.A. únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

### **7.1.3. Intercambio de información**

Ninguna persona deberá ocultar o manipular su identidad bajo ninguna circunstancia.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato. Fundiciones Fumbarri-Durango, S.A. se reserva, en función del riesgo identificado, la implantación de medidas de control, registro y auditoría sobre estos recursos de difusión.

En relación al intercambio de información dentro del marco del contrato de prestación de servicios, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por los derechos de autor infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de información protegida a terceras partes no autorizadas.
- Transmisión o recepción de aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.

Todas las actividades que puedan dañar la imagen y reputación de Fundiciones Fumbarri-Durango, S.A. están prohibidas en Internet y en cualquier otro lugar.



#### **7.1.4. Uso apropiado de los recursos**

Los recursos que Fundiciones Fumbarri-Durango, S.A. pone a disposición de las personas externas, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron proporcionados. Fundiciones Fumbarri-Durango, S.A. se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

Todos los equipos de la organización proveedora que se conecten a la red de producción se pondrán a disposición de Fundiciones Fumbarri-Durango, S.A. para que éste coordine la instalación del software y los configure apropiadamente.

Cualquier fichero introducido en la red de Fundiciones Fumbarri-Durango, S.A. o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal, y control de malware.

Se deberán restituir a Fundiciones Fumbarri-Durango, S.A. todos los activos, sin retraso injustificado, después de la finalización del contrato. Todos los ordenadores personales a los que Fundiciones Fumbarri-Durango, S.A. les haya instalado software se llevarán a Fundiciones Fumbarri-Durango, S.A. para que se formatee el disco duro a la finalización del servicio.

Se prohíbe expresamente:

- El uso de los recursos proporcionados por Fundiciones Fumbarri-Durango, S.A. para actividades no relacionadas con el propósito del servicio.
- La conexión a la red de producción de Fundiciones Fumbarri-Durango, S.A. de equipos y/o aplicaciones que no estén especificados como parte del software o de los estándares de los recursos informáticos propios.
- Introducir en los sistemas de información o la red corporativa de Fundiciones Fumbarri-Durango, S.A. contenidos obscenos, amenazadores, inmorales u ofensivos.



- Introducir voluntariamente en la red corporativa de Fundiciones Fumbarri-Durango, S.A. cualquier tipo de malware (virus, gusanos, troyanos, programas espía, ransomware, ...), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Todas las personas con acceso a la red de Fundiciones Fumbarri-Durango, S.A. tendrán la obligación de utilizar programas antimalware actualizados.
- Obtener sin autorización explícita otros derechos o accesos distintos a aquellos que Fundiciones Fumbarri-Durango, S.A. les haya asignado.
- Acceder sin autorización explícita a áreas restringidas de los sistemas de información de Fundiciones Fumbarri-Durango, S.A.
- Distorsionar o falsear los registros “log” de los sistemas de información de Fundiciones Fumbarri-Durango, S.A.
- Descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Fundiciones Fumbarri-Durango, S.A.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otras personas usuarias, ni dañar o alterar los recursos informáticos de Fundiciones Fumbarri-Durango, S.A.
- Destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos con información protegida (estos actos pueden constituir un delito).
- Albergar información protegida en las unidades locales de disco de los puestos PC de persona usuaria.

### **7.1.5. Responsabilidades de la persona usuaria**

Las organizaciones proveedoras de servicios deberán asegurarse de que todas las personas que desarrollan labores para Fundiciones Fumbarri-Durango, S.A. respeten los siguientes principios básicos dentro de su actividad:



- Cada persona con acceso a información de Fundiciones Fumbarri-Durango, S.A. es responsable de la actividad desarrollada por su identificador de persona usuaria y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de persona usuaria, garantizando que la clave asociada sea únicamente conocida por la propia persona usuaria, no debiendo revelarse al resto de las personas bajo ningún concepto, ni mantenerla por escrito a la vista, ni al alcance de terceras personas.
- Las personas usuarias no deberán utilizar ningún identificador de otra persona usuaria, aunque dispongan de la autorización del propietario.
- Las personas usuarias conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
- Cualquier persona con acceso a la información protegida deberá seguir las siguientes directivas en relación a la gestión de las contraseñas:
  - La longitud mínima de la contraseña deberá ser de 6 caracteres y no deberá contener el nombre, apellidos ni el identificador de la persona usuaria en la misma. Deberá ser cambiada cada 3 meses y no repetir al menos las 24 contraseñas anteriores.
  - Igualmente, deberán tener complejidad y ser difícilmente adivinables, por lo que estarán constituidas por combinación al menos 3 de estas 4 opciones en los primeros 8 caracteres:
    - Mayúsculas
    - Minúsculas
    - Números
    - Caracteres especiales
  - Es recomendable utilizar las siguientes directrices para la selección de contraseñas:
    - No usar palabras conocidas, ni palabras que se puedan asociar con uno mismo, por ejemplo, el nombre.
    - La contraseña no deberá hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se deberá evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, ...



- La clave debería ser algo prácticamente imposible de adivinar. Pero al mismo tiempo debería ser fácilmente recordada por la persona usuaria. Un buen ejemplo es usar el acrónimo de alguna frase o expresión.
  - Pedir el cambio de la contraseña siempre que exista un posible indicio de conocimiento por parte de otras personas usuarias.
  - Cambiar las contraseñas como mínimo una vez cada 90 días y evitar la reutilización de antiguas contraseñas.
  - Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión (“login”).
  - Evitar incluir contraseñas en los procesos automatizados de inicio de sesión (p.ej. Aquellas almacenadas en navegadores).
  - Notificar cualquier incidencia de seguridad relacionada con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.

Cualquier persona con acceso a la información protegida deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.

Cualquier persona con acceso a información protegida deberá respetar al menos las siguientes normas de escritorio limpio, con el fin de proteger los documentos en papel, soportes informáticos y dispositivos portátiles de almacenamiento y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:

- Almacenar bajo llave los documentos en papel y los medios informáticos, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- Bloquear las sesiones de persona usuaria o apagar el PC al dejarlo desatendido.
- Proteger tanto los puntos de recepción y envío de información (correo postal, máquinas de scanner y fax) como los equipos de duplicado (fotocopiadora, fax y scanner). La reproducción o envío de información con este tipo de dispositivos quedará bajo la responsabilidad de la persona usuaria.
- Retirar, sin retraso injustificado, cualquier información protegida una vez impresa.
- Destruir la información protegida una vez no sea necesaria.



- Las personas con acceso a sistemas y/o información de Fundiciones Fumbarri-Durango, S.A. nunca deberán, sin autorización por escrito, realizar pruebas para detectar y/o explotar una supuesta debilidad o incidencia de seguridad.
- Ninguna persona con acceso a sistemas y/o información de Fundiciones Fumbarri-Durango, S.A. intentará sin autorización expresa y por escrito por ningún medio transgredir el sistema de seguridad y las autorizaciones. Se prohíbe la captura de tráfico de red por parte de las personas usuarias, salvo que se estén llevando a cabo tareas de auditoría autorizadas por escrito.

Todas las personas que accedan a la información protegida deberán seguir las siguientes normas de actuación:

- Proteger la información protegida de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
- Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
- Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o la información.

### **7.1.6. Equipo de persona usuaria**

Las organizaciones proveedoras de servicios deberán asegurarse de que todo el equipamiento informático de persona usuaria utilizado para acceder a información protegida cumple las siguientes normas:

- Ante la inactividad de la persona usuaria, el equipo deberá bloquearse automáticamente.
- Ningún equipo de persona usuaria dispondrá de herramientas que puedan transgredir los sistemas de seguridad y las autorizaciones.
- Los equipos de persona usuaria se mantendrán de acuerdo a las especificaciones del fabricante.
- Todos los equipos de persona usuaria estarán adecuadamente protegidos frente a malware:



- El software antimalware se deberá instalar y usar en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
- Se mantendrán al día con las últimas actualizaciones de seguridad disponibles.
- El software antimalware deberá estar siempre habilitado y actualizado.

Se velará especialmente por la seguridad de todos los equipos móviles de persona usuaria que contengan información protegida o permitan acceder a ella de algún modo:

- Verificando que no incluyen más información que la que sea estrictamente necesaria.
- Garantizando que se aplican controles de acceso a dicha información.
- Minimizando los accesos a dicha información en presencia de personas ajenas al servicio prestado.
- Transportando los equipos en fundas, maletines o equipamiento similar que incorpore la apropiada protección frente a agentes ambientales.

### **7.1.7. Gestión del equipamiento hardware**

Las organizaciones proveedoras de servicios deberán asegurarse de que todos los equipos proporcionados por Fundiciones Fumbarri-Durango, S.A. para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Para ello deberán cumplir las siguientes normas:

- La organización proveedora deberá mantener una relación actualizada de equipos proporcionados por Fundiciones Fumbarri-Durango, S.A. y personas usuarias de dichos activos, o personas responsables asociadas en caso de que los activos no sean de uso unipersonal. Dicha relación podrá ser requerida por Fundiciones Fumbarri-Durango, S.A.
- Siempre que una organización proveedora quiera reasignar algún equipo de Fundiciones Fumbarri-Durango, S.A. que haya contenido información protegida deberá devolverlo temporalmente para que se puedan llevar a cabo los procedimientos de borrado seguro necesarios de forma previa a su reasignación.



- En caso de que una organización proveedora quiera proceder a dar de baja de la relación de equipos de Fundiciones Fumbarri-Durango, S.A. recibidos alguno de ellos, siempre deberá devolverlos, para que Fundiciones Fumbarri-Durango, S.A. pueda tratar dicha baja de forma apropiada.
- En caso de que una organización proveedora cese en la prestación del servicio, deberá devolver a Fundiciones Fumbarri-Durango, S.A. toda la relación de equipos recibidos, tal y como establecen los correspondientes contratos de prestación de servicios. Sólo en el caso de documentos en papel y soportes informáticos la organización proveedora podrá proceder a su eliminación segura, en cuyo caso deberá notificar a Fundiciones Fumbarri-Durango, S.A. dicha eliminación.

## **7.2. Directrices específicas**

### **7.2.1. Ámbito de aplicación**

Todas las organizaciones proveedoras deberán cumplir, además de las normas generales, las específicas recogidas en el presente apartado que les correspondan en cada caso, en función de las características del servicio prestado a Fundiciones Fumbarri-Durango, S.A.

Las tipologías de servicio que se contemplan son las que se indican a continuación.

- Lugar de ejecución del servicio: En función del lugar principal en el que se desarrollen los servicios se distinguen dos casos:
  - Fundiciones Fumbarri-Durango, S.A.: La organización proveedora presta el servicio principalmente desde la propia sede de Fundiciones Fumbarri-Durango, S.A.
  - Remoto: La organización proveedora presta el servicio principalmente desde sus propias dependencias, pese a que se puedan llevar a cabo actividades puntuales en la sede de Fundiciones Fumbarri-Durango, S.A.
- Propiedad de las infraestructuras TIC utilizadas: En función de quién sea el propietario de las principales infraestructuras TIC (comunicaciones, equipos de persona usuaria, software) utilizadas para prestar el servicio se distinguen dos casos:
  - Fundiciones Fumbarri-Durango, S.A.



- Organización proveedora.
- Nivel de acceso a los sistemas de Fundiciones Fumbarri-Durango, S.A.: En función del nivel de acceso a los sistemas de información de Fundiciones Fumbarri-Durango, S.A. se distinguen tres casos:
  - Con acceso privilegiado: El servicio prestado requiere del acceso privilegiado a los sistemas de información de Fundiciones Fumbarri-Durango, S.A., con capacidad para administrar dichos sistemas y/o los datos de producción que procesan.
  - Con acceso de nivel de persona usuaria: El servicio prestado requiere de la utilización de los sistemas de información de Fundiciones Fumbarri-Durango, S.A., de modo que las personas que prestan el servicio disponen de cuentas de persona usuaria que les permiten acceder a alguno de dichos sistemas con privilegios habituales.
  - Sin acceso: El servicio prestado no requiere de la utilización de los sistemas de información de Fundiciones Fumbarri-Durango, S.A., de modo que las personas que prestan el servicio no disponen de cuentas de persona usuaria en dichos sistemas.

En función de cada una de las tres categorías en las que se encuadre cada servicio, la organización proveedora deberá cumplir, adicionalmente a las normas generales de seguridad, las específicas recogidas en los apartados que se indican en la siguiente tabla:

	LUGAR		INFRAESTRUCTURA		ACCESO		
	Fumbarri	Remoto	Fumbarri	Organización proveedora	Privilegiado	Normal	Sin acceso
Selección de personas	NO	NO	NO	NO	SÍ	NO	NO
Auditoría de seguridad	NO	NO	NO	NO	SÍ	NO	NO
Comunicación de incidencias	SÍ	SÍ	SÍ	NO	SÍ	SÍ	NO
Seguridad física	NO	SÍ	NO	NO	NO	NO	NO
Gestión de activos	NO	NO	NO	SÍ	NO	NO	NO
Arquitectura seguridad	NO	NO	NO	SÍ	SÍ	SÍ	NO
Seguridad sistemas	NO	NO	NO	SÍ	NO	NO	NO



	LUGAR		INFRAESTRUCTURA		ACCESO		
	<i>Fumbarri</i>	<i>Remoto</i>	<i>Fumbarri</i>	<i>Organización proveedora</i>	<i>Privilegiado</i>	<i>Normal</i>	<i>Sin acceso</i>
Seguridad red	NO	NO	NO	SÍ	NO	NO	NO
Trazabilidad de uso de los sistemas	NO	NO	NO	SÍ	SÍ	NO	NO
Control y gestión de identidades y accesos	NO	NO	NO	SÍ	NO	NO	NO
Gestión cambios	NO	NO	NO	SÍ	SÍ	SÍ	NO
Gestión técnica de cambios	NO	NO	NO	NO	SÍ	NO	NO
Seguridad en desarrollo	NO	NO	NO	NO	SÍ	SÍ	NO
Gestión contingencias	NO	NO	NO	SÍ	NO	NO	NO

### **7.2.2. Selección de personas**

La organización proveedora deberá verificar los antecedentes profesionales de las personas asignadas al servicio, garantizando a Fundiciones Fumbarri-Durango, S.A. que en el pasado no ha sido sancionado por mala praxis profesional ni se ha visto envuelto en incidencias relacionadas con la confidencialidad de la información tratada que le hayan supuesto algún tipo de sanción.

La organización proveedora deberá garantizar a Fundiciones Fumbarri-Durango, S.A. la posibilidad de baja inmediata de las personas asignadas al servicio de cualquier persona en relación con la cual Fundiciones Fumbarri-Durango, S.A. desee ejercer el derecho de veto.

### **7.2.3. Auditoría de seguridad**

La organización proveedora deberá permitir que Fundiciones Fumbarri-Durango, S.A. lleve a cabo las auditorías de seguridad solicitadas, colaborando con el equipo auditor y facilitando todas las evidencias y registros le sean requeridos.



El alcance y profundidad de cada auditoría será establecido expresamente por Fundiciones Fumbarri-Durango, S.A. en cada caso. Las auditorías se llevarán a cabo siguiendo la planificación que se acuerde en cada caso con la organización proveedora del servicio.

Fundiciones Fumbarri-Durango, S.A. se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den causas específicas que lo justifiquen.

#### **7.2.4. Comunicación de incidencias**

Cuando detecte cualquier incidencia de seguridad de la información deberá notificarlo inmediatamente a [calidad@fumbarri.com](mailto:calidad@fumbarri.com).

Cualquier persona usuaria podrá trasladar a través del citado buzón aquellos eventos, sugerencias, vulnerabilidades, ... que puedan tener relación con la seguridad de la información y las directrices contempladas en las presentes normas de las que tenga conocimiento.

Se deberá notificar a través del citado buzón cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal (p.ej. Pérdida de listados y/o soportes informáticos, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos de copias de seguridad, ...).

El citado buzón centraliza la recogida, análisis y gestión de las incidencias recibidas.

Si no se tuviera acceso al buzón, se deberán utilizar los cauces de comunicación establecidos dentro del propio servicio, de modo que sea el interlocutor de Fundiciones Fumbarri-Durango, S.A. quien comunique la incidencia de seguridad.

#### **7.2.5. Seguridad física**

La sede deberá estar cerrada y deberá contar con algún sistema de control de acceso.

Existirá algún tipo de control de las visitas, al menos en áreas de acceso público y/o de carga y descarga.



La sede deberá contar, al menos, con sistemas adecuados de detección y extinción de incendios, y deberá estar construida de modo que ofrezca una suficiente resistencia frente a inundaciones.

Si se mantiene algún tipo de copia de seguridad, los sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida, que incluya al menos las siguientes medidas de seguridad:

- El área especialmente protegida deberá tener un sistema de control de acceso independiente al de la sede.
- Se limitará el acceso a las personas externas a las áreas especialmente protegidas. Este acceso se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personas autorizadas.
- Se mantendrá un registro de todos los accesos de personas ajenas.
- Las personas externas no podrán permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
- El consumo de alimentos o bebidas en estas áreas especialmente protegidas estará prohibido.
- Los sistemas ubicados en estas áreas deberán contar con algún tipo de protección frente a fallos de alimentación.

### **7.2.6. Gestión de activos**

La organización proveedora deberá contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.

Todos los activos utilizados para la prestación del servicio deberán tener una persona responsable, que se deberá asegurar de que dichos activos incorporan las medidas de seguridad mínimas establecidas por la organización proveedora, y que al menos deben ser las especificadas en la presente normativa.

Siempre que un activo haya contenido información protegida, la organización proveedora deberá llevar a cabo las bajas de activos garantizando la eliminación segura de dicha información, aplicando funciones de borrado seguro o destruyendo físicamente el activo, para que la información que haya contenido no pueda ser recuperable.



### **7.2.7. Arquitectura de seguridad**

Siempre que la organización proveedora de servicios realice trabajos de desarrollo y/o pruebas de aplicaciones para Fundiciones Fumbarri-Durango, S.A. o con información protegida, los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción en los que se albergue o procese información protegida.

Todos los accesos a los sistemas de información que alberguen o procesen información protegida deberán estar protegidos, al menos, por un cortafuegos, que limite la capacidad de conexión a ellos.

Los sistemas de información que alberguen o procesen información especialmente sensible deberán estar aislados del resto.

### **7.2.8. Seguridad de sistemas**

Los sistemas de información que alberguen o traten información protegida deberán registrar los eventos más significativos en torno a su funcionamiento. Estos registros de actividad estarán contemplados dentro de la normativa de copias de seguridad de la organización proveedora.

Los relojes de los sistemas de la organización proveedora que procesen o alberguen información protegida estarán sincronizados entre sí y con la hora oficial.

La organización proveedora del servicio garantizará que la capacidad de los sistemas de información que guarden o traten información protegida se gestiona adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.

Los sistemas de información que alberguen o procesen información protegida estarán adecuadamente protegidos frente a software malicioso, aplicando las siguientes precauciones:

- Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de desarrollo, prueba y producción.



- El software antimalware se deberá instalar y usar en todos los servidores y ordenadores personales para reducir el riesgo asociado con el software malicioso.
- El software antimalware deberá estar siempre habilitado y actualizado.

La organización proveedora establecerá una normativa de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado, con una periodicidad diaria.

Siempre que se utilice el correo electrónico en relación al servicio prestado, la organización proveedora deberá respetar las siguientes premisas:

- No se permitirá la transmisión vía correo electrónico de información protegida salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.
- Siempre que para la prestación del servicio se haga uso del correo electrónico de Fundiciones Fumbarri-Durango, S.A. se deberán respetar, al menos, los siguientes principios:
  - Se considerará al correo electrónico como una herramienta más de trabajo proporcionada con el fin exclusivo del servicio contratado. Esta consideración facultará a Fundiciones Fumbarri-Durango, S.A. a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad de las personas y su derecho a la intimidad.
  - El sistema de correo electrónico de Fundiciones Fumbarri-Durango, S.A. no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
  - Las personas usuarias no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples personas usuarias).

El acceso a los sistemas de información que alberguen o procesen información protegida deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador de persona y una contraseña asociada.



Los sistemas de información que alberguen o procesen información protegida deberán contar con sistemas de control de acceso que limiten el acceso a dicha información exclusivamente a las personas del servicio.

Las sesiones de acceso a los sistemas de información que alberguen o procesen información protegida deberán bloquearse automáticamente tras un cierto tiempo de inactividad de las personas usuarias.

Siempre que se haga uso de software facilitado por Fundiciones Fumbarri-Durango, S.A. se deberán atender las siguientes normas:

- Todas las personas que accedan a los sistemas de información de Fundiciones Fumbarri-Durango, S.A. deberán utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.
- Todas las personas tienen prohibido instalar copias ilegales de cualquier software.
- Se prohíbe el uso de software no validado por Fundiciones Fumbarri-Durango, S.A.
- También está prohibido desinstalar cualquiera de los programas instalados por Fundiciones Fumbarri-Durango, S.A.

### **7.2.9. Seguridad de red**

Las redes a través de las que circule la información protegida deberán estar adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados por la organización proveedora.

Los servicios disponibles en las redes a través de las que circule la información protegida deberán limitarse en la medida de lo posible.

Las redes que permitan el acceso a la infraestructura TIC de Fundiciones Fumbarri-Durango, S.A. deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:



- El acceso de personas usuarias remotos a la red de Fundiciones Fumbarri-Durango, S.A. estará sujeto al cumplimiento de procedimientos de identificación y autenticación previa, y validación del acceso.
- Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.
- En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas.

El acceso a las redes a través de las que circule la información protegida deberá estar limitado.

Todos los equipos conectados a las redes a través de las que circule la información protegida deberán estar apropiadamente identificados, de modo que los tráficos de red puedan ser identificables.

El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regula mediante la aplicación de la siguiente normativa:

- No se permite la utilización de equipamiento no controlado por Fundiciones Fumbarri-Durango, S.A. para las actividades de teletrabajo.
- Se establecerán criterios de autorización del teletrabajo en base a las necesidades del puesto de trabajo.
- Se establecerán las medidas necesarias para la conexión segura a la red corporativa.
- Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.
- Se controlará la revocación de derechos de acceso y devolución de equipamiento tras la finalización del periodo de necesidad del mismo.

Siempre que se haga uso del acceso a Internet proporcionado por Fundiciones Fumbarri-Durango, S.A. se deberán respetar, adicionalmente, la siguiente normativa:



- Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Las personas usuarias no deben buscar o visitar sitios que no sirvan como soporte al objetivo de negocio de Fundiciones Fumbarri-Durango, S.A. o al cumplimiento de su trabajo diario.
- El acceso a Internet desde la red corporativa se restringirá por medio de dispositivos de control incorporados en la misma. La utilización de otros medios de conexión deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de Internet.
- Las personas usuarias no deberán usar el nombre, símbolo, logotipo o símbolos similares al de Fundiciones Fumbarri-Durango, S.A. en ningún elemento de Internet (correo electrónico, páginas Web, etc.) no justificado por actividades estrictamente laborales.
- Únicamente se permitirá la transferencia de datos de o hacia Internet cuando estén relacionadas con actividades del negocio. La transferencia de ficheros no relativa a estas actividades (p.ej. La descarga de programas, ficheros multimedia, ...) estará prohibida.

### **7.2.10. Trazabilidad de uso de los sistemas**

Se registrarán los accesos privilegiados conservándose dichos registros de acuerdo a la normativa de copias de seguridad de la Organización.

Se registrará la actividad de los sistemas utilizados para llevar a cabo dicho acceso privilegiado, conservándose dichos registros de acuerdo a la normativa de copias de seguridad de la Organización.

Los errores y fallos registrados en la actividad de los sistemas se analizarán, adoptándose las medidas necesarias para su subsanación.

### **7.2.11. Control y gestión de identidades y accesos**

Todas las personas usuarias con acceso a un sistema de información dispondrán de una única autorización de acceso compuesta de identificador de persona usuaria y contraseña.



La organización proveedora deberá garantizar que periódicamente se constata que sólo tienen acceso a la información protegida las personas debidamente autorizadas para ello.

En aquellos casos en los que además se acceda a los sistemas de información de Fundiciones Fumbarri-Durango, S.A. se deberán considerar, además, la siguiente normativa:

- Ninguna persona usuaria recibirá un identificador de acceso a los sistemas de Fundiciones Fumbarri-Durango, S.A. hasta que no acepte por escrito la normativa de seguridad vigente.
- Las personas usuarias tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- En relación a datos de carácter personal, exclusivamente las personas autorizadas para ello podrán conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por la persona responsable del fichero.

### **7.2.12. Gestión de cambios**

Todos los cambios en la infraestructura TIC deberán estar controlados y autorizados, garantizándose que no forma parte de ella componentes no controlados.

Se deberá verificar que todos los nuevos componentes introducidos en la infraestructura TIC de la organización proveedora utilizada para la prestación del servicio funcionan adecuadamente y cumplen los propósitos para los que fueron incorporados.

### **7.2.13. Gestión técnica de cambios**

Todos los cambios que se lleven a cabo se deberán realizar siguiendo un procedimiento formalmente establecido y documentado, que garantice que se siguen los pasos apropiados para realizar el cambio.

El procedimiento de gestión de cambios deberá garantizar que se minimizan los cambios sobre la infraestructura TIC, limitándose a los estrictamente imprescindibles.



Se deberán probar todos los cambios antes de su despliegue en el entorno de producción, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento y seguridad de la infraestructura TIC.

Las organizaciones proveedoras deberán escanear y mitigar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando a Fundiciones Fumbarri-Durango, S.A. de todas aquellas asociadas a los componentes críticos.

### **7.2.14. Seguridad en desarrollo**

Todo el proceso de desarrollo de software externalizado será controlado y supervisado por Fundiciones Fumbarri-Durango, S.A.

Se incorporarán mecanismos de identificación, autenticación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implantación y operación del software.

Las especificaciones del software deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.

El software que se desarrolle deberá incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.

Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.

Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.

Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.

El acceso al código fuente de los aplicativos deberá estar limitado a las personas del servicio.



En el entorno de pruebas sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.

Durante las pruebas de los aplicativos se verificará que no existen brechas de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.

Sólo se transferirá al entorno de producción aquel software que haya sido expresamente aprobado.

En relación a los servicios Web se considerará la gestión del Top 10 de Owasp.

### **7.2.15. Gestión de contingencias**

El servicio deberá contar con un plan que permite su prestación aun en caso de contingencias.

El plan anterior deberá ser desarrollado en función de los eventos capaces de causar interrupciones en el servicio y su probabilidad de ocurrencia.

La organización proveedora deberá poder demostrar la viabilidad del plan de contingencias existente.

### **7.3. Seguimiento y control**

Con el fin de velar por el correcto uso de los mencionados recursos, a través de los mecanismos formales y técnicos que se considere oportunos, Fundiciones Fumbarri-Durango, S.A. comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente.

## **8. Implementación del Código y Auditorías**

Los fabricantes y proveedores implementarán y aplicarán programas para poner en práctica este Código. Deberán designar un representante de la Dirección que será responsable de la aplicación y cumplimiento de este Código.



Los fabricantes y proveedores deberán dar a conocer este Código a todos sus empleados.

Fundiciones Fumbarri-Durango S.A. se reserva el derecho de verificar que los proveedores y fabricantes cumplan con lo establecido en el Código. En caso de tener conocimiento de alguna acción o condiciones de no cumplimiento de lo establecido en el Código, Fundiciones Fumbarri-Durango S.A. se reserva el derecho de demandar la realización de medidas correctivas al proveedor.

Fundiciones Fumbarri-Durango S.A. también se reserva el derecho de dar por terminado cualquier contrato o convenio comercial de cualquier proveedor y fabricante que no cumpla el Código.

## **9. Comité de Ética y Canal de Denuncias**

El presente Código se alinea con los principios y valores que recoge el Código de Conducta Empresarial de Fundiciones Fumbarri-Durango S.A., el cual regula un Comité de Ética y un Canal de Denuncias, a fin de asegurar su cumplimiento.

En este sentido, y para asegurar el cumplimiento del presente Código de Conducta de Proveedores, el Comité de Ética de Fundiciones Fumbarri-Durango S.A. podrá actuar por propia iniciativa o a instancias de un fabricante, proveedor o de un tercero con relación directa e interés comercial o profesional legítimo, mediante denuncia realizada de buena fe.

A tal fin, las comunicaciones realizadas al amparo del presente Código, ya contengan denuncias de incumplimiento o consultas relativas a su interpretación o aplicación, podrán hacerse llegar a la sociedad a través de los siguientes medios:

- Correo ordinario a la dirección: San Roke, 22 48200 Durango (Bizkaia), a la atención del Comité de Ética
- Correo electrónico a la dirección: