SYNLAB

CÓDIGO BUENAS PRÁCTICAS PROVEEDORES

Elaboración:	Revisión:	Aprobación:
Nombre. COMITÉ COMPLIANCE	**Nombre.** NINO STANIC	**Nombre.** ALBERTO SUMMA
Cargo. RAFAEL FONT HEAD OF INNOVATION	**Cargo.** JUNIOR REVISOR THERAPEUTICS	**Cargo.** CEO
Firma.	**Firma.**	**Firma.**
Fecha:01-06-2017	**Fecha: 29-01-2018**	**Fecha: 30-01-2018**

Versión	Fecha	Afecta	Breve descripción del cambio
1ª	29-1-2018	Creación	

1. Objeto

El Código de Buenas Prácticas de Proveedores de SYNLAB HOLDING IBERIA (en adelante SYNLAB) define los requisitos mínimos no negociables que solicitamos a nuestros proveedores y sus proveedores subcontratados respeten y cumplan a la hora de hacer negocios con Synlab.

2. Cumplimiento

SYNLAB espera que el Proveedor respete todas las leyes y normativas aplicables y, en particular, las relativas a los puntos que se detallan en el presente documento y que se esfuerce por cumplir los estándares internacionales y del sector, así como las buenas prácticas.

3. Aplicación

La aceptación del Código de Buenas Prácticas de Proveedores es un requisito previo en todos los contratos de SYNLAB para sus proveedores. Al aceptar la Orden de pedido, que hace referencia al Código, el Proveedor se compromete a que todas sus actividades estarán sujetas a las disposiciones incluidas en el presente Código.

4. Contenido

A continuación, se definen los principios que deben regir mi actuación profesional como PROVEEDOR de *SYNLAB*:

1. Estoy obligado a desarrollar mi actividad siguiendo los más elevados estándares éticos, siendo honesto e inspirando confianza, con un comportamiento coherente e inquebrantable, velando en todo momento por la buena reputación de SYNLAB.

2 Inspiraré todas mis actuaciones de manera que persigan el interés de SYNLAB sobre mi interés propio, evitando cualquier clase de **conflicto de interés** que pueda surgir en la actividad que realizo en nombre y por cuenta de la entidad.

3 Me obligo a desempeñar mis funciones **conforme a la legalidad**, a prohibir en mi actividad cualquier comportamiento ilícito o constitutivo de delito y a velar por la existencia de controles para la no comisión de los mismos.

4 Me obligo a guardar absoluta **reserva y confidencialidad de la información** de SYNLAB de la que dispongo, así como de la información de terceros a la que he tenido acceso ejerciendo alguna actividad para o en nombre de SYNLAB. Trataré toda la información conforme a la legislación vigente y, entre ésta, conforme a la legislación en materia de protección de datos personales.

5 Debo adoptar cuantas medidas sean necesarias para evitar cualquier situación de cohecho o corrupción entre particulares, consistentes en la aceptación de dádivas y regalos injustificados para lograr la contratación de productos o servicios.
Asimismo, no tengo permitido realizar conductas que sean constitutivas de cohecho o tráfico de influencias con autoridad o funcionario público.

6 Gestionaré todas mis conductas dentro de los estándares de **transparencia y buenas prácticas empresariales**, con el fin de incorporar una cultura de prevención de acciones fraudulentas.

7 Tengo prohibido llevar a cabo cualquier **conducta irregular o fraude**, pues abarca riesgos que pueden menoscabar la confianza del público y dañar la reputación de la integridad de SYNLAB. Dentro de estos riesgos, se destacan:

a. Entregar información financiera fraudulenta.

b. Lograr ingresos o activos obtenidos mediante acciones fraudulentas o ilícitas.

c. Corrupción: ofrecer, solicitar, entregar o recibir, bienes en dinero o en especie, a cambio de acciones, decisiones u omisiones que puedan beneficiar a la entidad; ya sea a particular o a funcionario público.

d. Aceptar dádivas, para sí o para un tercero, que consistan en dinero o sustancias prohibidas.

e. Publicidad engañosa

f. Falsedades: creación, eliminación, modificación, alteración o divulgación de cualquier tipo de información tendente a distorsionar la realidad.

g. Otras conductas irregulares: conflicto de interés, abuso de información privilegiada, discriminación, vulneración de secretos empresariales, infracciones medioambientales etc.

8 Me comprometo a cumplir todas las **leyes antimonopolio y de protección de la competencia** que corresponda y que prohíban acuerdos o acciones que restrinjan sin motivo fundado el comercio, que sean **engañosos** o que induzcan a error, o bien que limiten injustificadamente la acción de la competencia sin proporcionar efectos beneficiosos para los consumidores. Se consideran prácticas contrarias a la libre competencia.

9 Para evitar vulneraciones en **materia de propiedad intelectual**, me comprometo a cumplir con la legislación vigente en esta materia.

10 Debo actuar en mis relaciones con los clientes, conforme a **criterios de consideración, respeto y dignidad,** teniendo en cuenta la diferente sensibilidad cultural de cada persona y no llevando a cabo actuaciones que pudieran ser discriminatoria en el trato por razón de raza, religión, edad, nacionalidad, género o cualquier otra condición personal o social prohibida por la ley, con especial consideración hacia la atención de las personas con discapacidad o minusvalías.

11 SYNLAB apoya plenamente la **Convención Marco y las Directrices sobre comercio y derechos humanos de las Naciones Unidas** y espera que el proveedor respete todos los derechos humanos, incluidos los derechos laborales, en todas sus actividades económicas.

12 SYNLAB espera que los sistemas de gestión y operación, así como los empleados, del Proveedor trabajen para prevenir las enfermedades y lesiones laborales.

13 SYNLAB solicita a sus Proveedores que cumplan con todos los requisitos legales aplicables sobre medio ambiente y que demuestra una mejora continua de su actuación medioambiental.

14 Conozco que tengo a mi disposición un **canal de denuncias: http://asesoriapenalcorporativa.es/canal-denuncias/synlab/**

SYNLAB

POLÍTICA DE ADOPCIÓN DE DECISIONES FISCALES

Elaboración:	Revisión:	Aprobación:
Nombre. OCi **Cargo.** **Firma.** **Fecha:01-06-2017**	**Nombre.** OCi **Cargo.** **Firma.** **Fecha: 29-01-2018**	**Nombre.** **Cargo.** O. ADM. **Firma.** **Fecha: 30-01-2018**

Versión	Fecha	Afecta	Breve descripción del cambio
1ª	29-1-2018	Creación	

El departamento financiero de SYNLAB HOLDING IBERIA S.A. (en adelante SYLANB), que ejerce funciones fiscales, tiene atribuida la función de formular la estrategia fiscal de la compañía, de acuerdo a las directrices del grupo marcadas por el órgano de administración de SYLANB en el marco de la exigencia de transparencia fiscal.

El departamento fiscal del grupo (de la matriz) envía las directrices por comunicaciones formales vía correo electrónico.

Además, corresponde a los Administradores aprobar las inversiones u operaciones que por su elevada cuantía o características tengan especial relevancia fiscal así como todas aquellas operaciones fiscales.

Las inversiones de adquisiciones de compañías se tratan directamente con el órgano de administración y es éste quien junto con el departamento de adquisiciones toma las decisiones. Estas operaciones con impacto fiscal son asesoradas en materia fiscal por personal interno de la empresa y expertos externos.

Las operaciones fiscales y riesgos fiscales que puedan ser detectados son planteadas ante los administradores y son éstos quienes toman la decisión última.

En el ejercicio de estas funciones, los Administradores aprueban este Protocolo Fiscal, que recoge la estrategia fiscal de SYNLAB y su compromiso con la aplicación de buenas prácticas tributarias.

La estrategia fiscal de SYNLAB consiste básicamente en asegurar el cumplimiento de la normativa tributaria aplicable y en procurar una adecuada coordinación de la política fiscal en el marco de la consecución del interés social y del apoyo a la estrategia empresarial a largo plazo evitando riesgos e ineficiencias fiscales en la ejecución de las decisiones de negocio.

El cumplimiento por SYNLAB de sus obligaciones fiscales y sus relaciones con las Administraciones Tributarias se rige por los siguientes principios:

I. El **cumplimiento de las normas tributarias**, satisfaciendo los tributos que resulten exigibles de acuerdo con el ordenamiento jurídico.

II. La **adopción de decisiones** en materia tributaria sobre la base de una interpretación razonable de la normativa aplicable y en estrecha vinculación con la actividad de la empresa. La toma de decisiones en el ámbito fiscal se somete a la aprobación de órganos colegiados, con especial incidencia en las áreas susceptibles de hacer incurrir a la empresa en responsabilidad tributaria, sancionadora o penal.

III. **Sistema de reporting** de la información contable y fiscal, a través de la implementación de organigramas detallados, manuales, políticas internas e instrucciones, en la cual se establezcan las pautas y responsabilidades específicas de cada proceso: planificación, gestión, control y supervisión y ajustes por cambios, delimitando los responsables y funciones.

IV. La **prevención y reducción de los riesgos fiscales significativos**, velando por que la tributación guarde una relación adecuada con la estructura y ubicación de las actividades, los medios humanos y materiales y los riesgos empresariales de la empresa.

V. La potenciación de una **relación con las autoridades** en materia tributaria basada en el respeto a la ley, la lealtad, la confianza, la profesionalidad, la colaboración, la reciprocidad y la buena fe, sin perjuicio de las legítimas controversias que, respetando los principios anteriores y en defensa del interés social, puedan generarse con dichas autoridades en torno a la interpretación de las normas aplicables.

VI. La **información a los Administradores mancomunados** sobre las principales implicaciones fiscales de las operaciones o asuntos que se sometan a su aprobación, cuando constituyan un factor relevante para formar su voluntad.

VII. Sometimiento a **auditorías fiscales periódicas**. Consultas periódicas a los asesores fiscales sobre dudas acerca de la estrategia fiscal y sobre posibles requerimientos fiscales, con objeto de trasladar al grupo una visión detallada a partir de una opinión experta.

VIII. Creación de un sistema de **comunicaciones internas** destinado a involucrar a todos los integrantes de la empresa en el cumplimiento de una cultura de cumplimiento de las obligaciones fiscales.

Buenas prácticas tributarias

En aplicación de los principios anteriores, la empresa asume las siguientes buenas prácticas tributarias:

1. No utilizar estructuras de carácter artificioso ajenas a las actividades propias de la misma y con la única finalidad de reducir su carga tributaria ni, en particular, realizar transacciones con entidades vinculadas por motivaciones exclusivamente de erosión de las bases imponibles o de traslado de beneficios a territorios de baja tributación.

2. Evitar las estructuras de carácter opaco con finalidades tributarias, entendiéndose por tales aquellas destinadas a impedir el conocimiento por parte de las Administraciones Tributarias competentes del responsable final de las actividades o del titular último de los bienes o derechos implicados.

3. No constituir ni adquirir sociedades residentes en paraísos fiscales, con la sola excepción de los supuestos en que viniera obligada a ello por tratarse de una adquisición indirecta.

4. Colaborar con las Administraciones Tributarias competentes en la detección y búsqueda de soluciones respecto de las prácticas fiscales

fraudulentas de las que la empresa tenga conocimiento.

5. Facilitar la información y documentación con trascendencia fiscal que soliciten las Administraciones Tributarias competentes, en el menor plazo posible y con el alcance debido.

6. Dar a conocer y discutir adecuadamente con el órgano que corresponda de la Administración Tributaria competente todas las cuestiones de hecho relevantes de las que tenga conocimiento para instruir, en su caso, los expedientes de que se trate y potenciar, en la medida de lo razonablemente posible y sin menoscabo de una buena gestión empresarial, los acuerdos y conformidades en el curso de los procedimientos inspectores.

7. Adoptar los mecanismos de control necesarios para asegurar, dentro de una adecuada gestión empresarial, el cumplimiento de la normativa tributaria.

8. Igualmente, dedicará a tales fines los recursos humanos y materiales adecuados y suficientemente cualificados.

9. Administradores mancomunados, a través de su presidente y consejero delegado y de sus altos directivos, impulsará el seguimiento de los principios y buenas prácticas tributarias que se contienen en esta Política fiscal corporativa cuyas actividades tengan una trascendencia significativa en el ámbito tributario.

SYNLAB

POLÍTICA DE COMPLIANCE

Elaboración:	Revisión:	Aprobación:
Nombre. OCi Cargo. Firma. Fecha: 28-1-2018	Nombre. OCi Cargo. Firma. Fecha: 29-1-2018	Nombre. Cargo. O AOM. Firma. Fecha: 29-1-2018

Versión	Fecha	Afecta	Breve descripción de la modificación
1ª	29/01/18	Creación	

SYNLAB HOLDING IBERIA, S.A., (en adelante "SYNLAB"), realiza su actividad y operaciones en cumplimiento de todas las leyes y reglamentos pertinentes e implementa directrices, políticas y procedimientos internos que garantizan que dichas leyes y reglamentos se siguen cumpliendo.

SYNLAB identifica, gestiona y comunica al Órgano de Gobierno (Órgano de administración) y a la Dirección de la entidad, el riesgo de incumplimiento penal que debe ser prevenido.

El comportamiento inadecuado de un sólo directivo, empleado o personal que realice funciones para la entidad puede potencialmente dañar nuestra imagen y reputación en un espacio temporal muy corto. Por ello, debemos prevenir y evitar de forma activa esta posibilidad. Para ello, se requiere que todos los miembros de SYNLAB tanto los accionistas, consejeros, directivos como empleados (en adelante, el "Personal"), llevemos a cabo nuestras actividades con el firme compromiso de cumplir con la legislación y regulación vigentes, nuestros principios éticos, nuestros protocolos y nuestras políticas internas, así como con los procedimientos y controles establecidos en la entidad.

La finalidad de la presente Política es poner en conocimiento del Personal de SYNLAB, así como de los terceros que se relacionen con la entidad, un mensaje rotundo de oposición a la comisión de cualquier acto ilícito, penal o de cualquier otra índole. En ningún caso está justificada la comisión de un delito por parte del personal, ni aun cuando tal actuación produjese, aparentemente, un beneficio de cualquier clase para la entidad. Asimismo, SYNLAB está dispuesta a combatir estos actos y a prevenir un eventual deterioro de su imagen y su valor reputacional.

Esta Política de Compliance constituye el marco de referencia del Modelo de Prevención de Delitos existente en SYNLAB, que es conocido por todo el Personal e impulsado por el Órgano de gobierno.

1.- ¿Por qué un Sistema de Gestión de Compliance?

Las principales razones para implementar un Sistema de Gestión de Compliance efectivo y eficaz se destacan a continuación:

a) **Cultura de ética empresarial sólida:** orientación con respecto al comportamiento adecuado y correcto para los directivos y los empleados.
b) **Responsabilidad y multas**: para evitar responsabilidades penales/civiles y la imposición de sanciones y multas a la entidad.
c) **Reclamaciones legales**: para evitar las reclamaciones de terceros contra la entidad.
d) **Riesgo reputacional:** para evitar que la reputación de la entidad resulte perjudicada, garantizando el valor de la misma.
e) **Gestión de la cadena de suministro:** para garantizar la reducción del riesgo de la cadena de suministro asegurando la aplicación de prácticas empresariales responsables y éticas en las cadenas de suministro globales.

Por tanto, un Sistema de Gestión de Compliance contribuye a garantizar y aumentar el valor de SYNLAB y a proteger a la entidad frente a reclamaciones relacionadas con riesgos penales.

2.- Sistema de Gestión de Compliance Penal

SYNLAB cuenta con un Sistema de Gestión de Compliance que cumple los requisitos mínimos, expuestos a lo largo de este documento, y es congruente con los fines de la entidad.

Para establecer un Sistema de Gestión efectivo, SYNLAB tiene en cuenta los siguientes pasos:

- Identifica y evalúa los riesgos;
- Desarrolla medidas preventivas;
- Implanta;
- Detecta, responde y sigue la efectividad;
- Realiza informes;
- Mejora continua de su Sistema de Gestión.

El Compliance Penal es el resultado de que SYNLAB cumpla con sus objetivos a través del cumplimiento de los requisitos que a continuación se exponen:

I. Compromiso

El cumplimiento empieza por la cúpula de la entidad.

El Órgano de administración de SYNLAB ha asumido el compromiso de crear en la entidad un entorno de cumplimiento, basado tanto en el respeto de la normativa vigente (legislación general y sectorial, así como normas y procedimientos internos), como en la exigencia de comportamientos éticos, responsables y diligentes a todos los integrantes de la entidad (administradores, directivos, empleados y profesionales) y de los terceros con los que se relaciona (colaboradores, proveedores y clientes).

Este entorno y cultura de cumplimiento incluye, pero no se limita, a la prevención de delitos, abarcando al mismo tiempo, objetivos éticos y de gestión diligente y responsable.

Asimismo, el Órgano de Administración es responsable de desarrollar e implementar un Sistema de Gestión de Compliance basado en la aplicación de

políticas y procedimientos adecuados que garantizan el cumplimiento de todas las leyes y reglamentos aplicables.

El nombramiento de un Órgano de Control Interno (OCI) no exime al Órgano de administración de su responsabilidad última de establecer un Sistema de Compliance penal efectivo.

El Órgano de Administración de SYNLAB comunica su compromiso claro con el cumplimiento normativo penal ("mayor jerarquía mayor exigencia") y cumple con los requisitos de esta política de compliance y del Sistema de gestión de compliance penal implantado.

SYNLAB está comprometida con la mejora continua del Sistema de gestión de compliance penal.

Asimismo, el Órgano de Administración ha asumido la obligación de prevención, control y gestión en materia de cumplimiento normativo y responsabilidad penal de la empresa, como camino hacia la implantación de una verdadera cultura ética, bajo el principio de proporcionalidad y en consonancia con la situación económica actual.

A tal efecto, el Órgano de Administración de la entidad asume a obligación y responsabilidad:

- ✓ Establecer y defender que las actuaciones de los miembros de la organización sean conformes al ordenamiento jurídico en general y en particular al de naturaleza penal.
- ✓ Adoptar, implementar, mantener y mejorar el sistema de gestión de compliance penal.
- ✓ Dotar al sistema de gestión de compliance penal, y en concreto al órgano de compliance penal de los recursos financieros, materiales y humanos adecuados y suficientes para su funcionamiento eficaz.
- ✓ Fijar y aprobar la política de compliance penal de la organización.

- ✓ Asegurar que se establecen los procedimientos para el proceso de formación de la política de compliance penal, de toma de decisiones y de ejecución de las mismas promoviendo una cultura de compliance que garantice altos estándares éticos de comportamiento.
- ✓ Comunicar la política de compliance penal con un lenguaje e idioma adecuado a los miembros de la organización, así como a los socios de negocio que puedan representar riesgos penales.
- ✓ Establecer un órgano de compliance penal, asegurándonos de que no tienen conflicto de intereses y demuestran tener:
- ✓ Integridad y compromiso con compliance penal.
- ✓ Habilidades de comunicación eficaz y capacidad de influencia.
- ✓ Capacidad y prestigio para la aceptación de sus consejos y directrices.
- ✓ Competencia necesaria.
- ✓ Asegurarse de estar correcta y puntualmente informados sobre el desempeño del sistema de gestión de compliance penal y de su mejora continua, incluyendo todas las no conformidades relevantes, promoviendo activamente una cultura de información completa y transparente.
- ✓ Tener conocimiento de los resultados de las auditorías.
- ✓ Recibir copia de las revisiones del sistema de compliance penal realizadas por el órgano de compliance penal y la alta dirección, así como la documentación de la evidencia de los resultados obtenidos.
- ✓ Examinar periódicamente el sistema de gestión de compliance penal, con base en la información proporcionada por el órgano de compliance penal y la alta dirección y cualquier otra información que pueda solicitar y obtener, modificándolo cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que lo haga necesario, dejando evidencia de los resultados de las revisión realizada.

II. Orden del día del Órgano de Administración

El cumplimiento normativo penal es una materia habitual en el orden del día de las reuniones del Órgano de Administración.

III. Ámbito de aplicación

La presente política será de aplicación a todos los administradores, directivos, empleados y profesionales que en cada momento integren SYNLAB (en adelante "la entidad"), independientemente de su ubicación territorial hasta el día de su derogación.

SYNLAB cuenta con un modelo de gobierno en el que tienen atribuida la responsabilidad de su control ordinario a través del Órgano de Administración, Órgano de Dirección y sus respectivos responsables de departamentos, que, con la supervisión del Órgano de Control Interno, aseguran la implementación y el seguimiento de los principios de actuación recogidos en esta Política para la prevención de delitos, sin perjuicio de la adecuada coordinación a todos los niveles.

IV. Obligaciones y responsabilidades de la Alta Dirección y el Equipo Directivo:

- ✓ Cooperar activamente en la implementación de una cultura de cumplimiento.
- ✓ Conocer y transmitir a las personas que de ellos dependen toda la normativa aplicable y su actividad profesional en la empresa, incluidos los procesos y procedimientos internos.
- ✓ Cumplir y hacer cumplir a las personas que de ellos dependen, toda la normativa y procesos en materia de cumplimiento.
- ✓ Realizar actividades de formación y supervisión en materia de cumplimiento de las personas que de ellos dependen.

- ✓ Identificar los riesgos de incumplimiento de las normas en su actividad.
- ✓ Asegurar que los procesos relacionados con las conductas legales se pongan en conocimiento de sus subordinados.
- ✓ Formar a sus subordinados en las políticas y normas aplicables a su actividad laboral.
- ✓ Implementar las medidas de mitigación y control de riesgos.
- ✓ Promover sistemas de mejora continua en los procesos.
- ✓ Tomas las medidas correctivas oportunas,
- ✓ Notificar incidentes en materia de cumplimiento que ocurran.
- ✓ Tomas las medidas disciplinarias adecuadas a los incidentes ocurridos junto con el departamento pertinente encargado de ello.
- ✓ Promover la mejora continua y apoyar los diferentes roles de gestión.
- ✓ Fomentar el uso de procedimientos para detectar conductas potencialmente delictivas que puedan afectar a la organización y sus actividades.
- ✓ Garantizar que ningún miembro de la organización es objeto de represalia, discriminación o sanción disciplinaria por comunicar de buena fe violaciones, o sospechas fundadas de violaciones de la política de compliance penal, o por rehusar participar en actuaciones delictivas incluso si ello conduce a una pérdida de negocio de la organización. No tomar represalias contra las personas integrantes del equipo que pongan en de manifiesto algún incumplimiento o incidente.
- ✓ Asegurarse de estar correcta y puntualmente informados sobre el desempeño del sistema de gestión de compliance penal y de su mejora continua, incluyendo todas las no conformidades relevantes, promoviendo activamente una cultura de información completa y transparente.

V. Obligaciones de los mandos intermedios:

- ✓ Cooperar activamente en la implantación de una cultura de cumplimiento.
- ✓ Conocer y transmitir a las personas que de ellos dependen, toda la normativa de cumplimiento aplicable a su actividad profesional en la empresa.
- ✓ Cumplir y hacer cumplir a las personas de las que ellos dependen toda la normativa y procesos en materia de cumplimiento.
- ✓ Realizar actividades de formación y supervisión en materia de cumplimiento de las personas que de ellos dependen.
- ✓ Identificar riesgos e implementar medidas de control y correctivas.
- ✓ Promover sistemas de mejora continua de los procesos.
- ✓ Notificar incidencias en cumplimiento que sean detectadas.
- ✓ No tomar represalias respecto de los integrantes de su equipo que pongan de manifiesto algún incumplimiento.

VI. Obligaciones de los empleados:

- ✓ Cumplir la normativa vigente: legislación general, sectorial, Códigos, normas, políticas y procedimientos internos de la entidad.
- ✓ Formarse en materia de cumplimiento normativo.
- ✓ Poner en conocimiento del OCI los incumplimientos o incidentes de los que tenga conocimiento.

VII. Órgano de Control Interno (OCI):

Al objeto de ejecutar las funciones de prevención, control y gestión en materia de cumplimiento normativo y responsabilidad penal de la empresa, el Órgano de Administración de SYNLAB ha creado, como medida organizativa y de control, un Órgano de Control Interno que es el responsable de la implantación del Modelo de Prevención de Delitos en la entidad a nivel operativo y funcional, y el encargado de la supervisión de su funcionamiento y cumplimiento, propuestas de área de mejora, debiendo reportar al Órgano de Administración cualquier incumplimiento que se observe y del que tuviese conocimiento.

Se ha creado un Órgano de Control Interno COMPUESTO por:

- **Don Fernando Nuno de Sousa Zuzarte Saraiva**, Legal Counsel en Iberia, nombrado en fecha 1 de abril de 2016 por el Órgano de Administración Compliance Officer.
- **Joan Manuel Braga Ribeiro,** CFO Iberia.

El Órgano de Control Interno reúne los siguientes REQUISITOS.

- Ha recibido formación adecuada en materia de responsabilidad penal de la persona jurídica y tiene pleno conocimiento del Modelo de Prevención de Delitos implementado en la entidad.
- Tiene un conocimiento completo de la estructura organizativa de la entidad, de las funciones de los principales responsables de área y de las actividades supervisadas por los mismos.
- Autonomía e independencia. Tiene atribuidos poderes autónomos, dispone de medios técnicos y recursos materiales y humanos suficientes. Asimismo, tiene acceso a todos los procesos, información interna y totalidad de las actividades que sea necesaria.

- Ocupa una posición diferenciada en la entidad, existiendo mecanismos específicos de comunicación con el Órgano de Administración.
- Tiene acceso al Órgano de Administración y podrá ser convocado a participar en reuniones y comités.
- Para la realización de sus funciones se le ha dotado de los recursos financieros adecuados y suficientes para conseguir sus objetivos, atendiendo al tamaño de la entidad, la naturaleza de la actividad, consignándose específicamente en los presupuestos de la entidad.

Sus FUNCIONES principales consisten en:

- **Supervisión del funcionamiento y cumplimiento del Modelo de Prevención de Delitos.** El Órgano de Control Interno debe verificar que todos los mecanismos encargados de detectar los posibles riesgos funcionan correctamente, realizando inspecciones en los departamentos cuando se considere necesario, realizando entrevistas a los empleados o terceros, asesorando en materia de cumplimiento normativo para la toma de decisiones por parte de la organización o cuando se haya de realizar operaciones de cierto riesgo o grandes dimensiones. El OCI debe garantizar la aplicación de políticas y procedimientos adecuados. Y ser la persona de contacto si los empleados desean plantear preguntas sobre asuntos de Compliance / Modelo de Prevención de Delitos, incumplimientos del Código de conducta o posibles ilícitos.

  Si se sospecha de un problema de incumplimiento, debe investigar el asunto y garantizar que sean resueltos, garantizando que el informante no sufra represalias. Así como responsabilizarse de proponer auditorias de cumplimiento al Órgano de gobierno; elaborar informes periódicos o en situaciones específicas para el Órgano de Administración y mantener una línea de comunicación con la Alta Dirección.

- **Deber de formación y comunicación.** Para el correcto funcionamiento del Modelo de Prevención de Delitos, los empleados y colaboradores de la entidad deben saber cómo actuar ante ciertas ante ciertas situaciones que podrían generar riesgos de incumplimiento normativo. Por ello el Órgano de Control Interno debe poner en conocimiento del personal de la entidad la importancia de la cultura de cumplimiento normativo, la importancia de las denuncias para el buen funcionamiento del modelo, el Modelo existente en la entidad y las políticas y protocolos implementados. Debe organizar la formación adecuada para los empleados sobre el Modelo de Prevención de Delitos implementado, Código de conducta de y otros asuntos esenciales de cumplimiento.

  Para ello se ha elaborado un Plan formativo anual en materia de responsabilidad penal en el que se incluye como mínimo:

  - Formación a las nuevas incorporaciones.
  - Formación a empleados en materia de responsabilidad penal de la empresa y Modelo de prevención de delitos implementado.
  - Formación al Órgano de gobierno y dirección de la entidad en materia de responsabilidad penal de la empresa.

- **Recepción y gestión de denuncias.** Recepción de las denuncias, registro y realización de las investigaciones que sean necesarias con obligación de reporte al Órgano de Administración. Todo ello debe realizarse de conformidad con la Política "Canal de denuncias" de fecha 18 de enero de 2018 implementada en la entidad.

- **Revisión y modificación del Modelo de Prevención de Delitos:** El Órgano de Control Interno responsable de la supervisión del buen funcionamiento del MPD implementado en la entidad debe realizar la revisión y propuesta de modificación periódica del MPD al Órgano de Administración, así como cuando se considere necesario, bien por producirse una infracción o incumplimiento del MPD, cuando se modifique sustancialmente la organización de la empresa o del sector de actividad en el que opera, o cuando se produzcan cambios de la

normativa. Por lo tanto, debe revisar el Código de Conducta y el resto de directrices y políticas de cumplimiento de la entidad con una periodicidad fija y proponer modificaciones o directrices o políticas adicionales en caso necesario. Así como, informar a la organización sobre avances legales importantes que puedan causar problemas de incumplimiento.

Las responsabilidades y tareas delegadas al Órgano de Control Interno están definidas y documentadas, en la "Protocolo Órgano de Control Interno" de fecha 29 de enero de 2018.

El Órgano de Control Interno trabaja conjuntamente con la dirección de la entidad y tiene plena colaboración con los demás órganos de la Organización.

VIII. Identificación/evaluación de riesgos

El Sistema de Gestión de Compliance se basa en un proceso documentado en el que se identifican y evalúan los riesgos de cumplimiento penal. La identificación y evaluación de los riesgos se repite con una periodicidad fija o como respuesta específica a un evento extraordinario, cambio significativo en la estructura o actividad de la entidad, cambios en la jurisprudencia o cuando se produzcan cambios legislativos relevantes.

IX. Desarrollo de medidas correctivas

Una vez completado el proceso de identificación y evaluación de los riesgos, se procede a desarrollar medidas para eliminar la causa de la no conformidad y prevenir que se reproduzcan.

SYNLAB desarrolla o, según el caso, revisa los documentos existentes relativos al cumplimiento (teniendo en cuenta los resultados de la identificación y evaluación de los riesgos).

X. Formación

Los empleados reciben formación sobre cumplimiento, riesgos penales y el Modelo de Prevención de Delitos implementado y su asistencia a dicha formación queda documentada.

La contribución del personal de la entidad a la eficacia del Sistema de Gestión de Compliance penal es primordial para que éstos ayuden a prevenir y detectar riesgos penales, evitando su materialización y reconociendo los factores de riesgos.

XI. Competencia

SYNLAB asegura la competencia del Órgano de Control Interno (OCI), basándose en una educación, formación o experiencia adecuada.

Se revisa periódicamente los objetivos de rendimiento para asegurarse que existen salvaguardas razonables para evitar que incentiven la asunción de riesgos penales o promuevan conductas inapropiadas en relación con el Compliance penal.

XII. Investigaciones

Cualquier sospecha de incumplimiento se investiga inmediatamente.

XIII. Auditorias de cumplimiento

Se realizan auditorías internas de cumplimiento normativo penal anuales para abordar e investigar los problemas de cumplimiento.

Alternativamente, se puede contratar a profesionales externos (por ejemplo, un bufete de abogados especializado en auditorías de cumplimiento o una empresa de auditoria de renombre que también realice auditorias de cumplimiento).

El Órgano de Control Interno presenta anualmente, un informe de cumplimiento al Órgano de Administración, que incluirá una descripción de los asuntos de cumplimiento seleccionados a examinar en la misma.

XIV. Canal de Denuncias y mecanismo de reacción

SYNLAB ha procedido a la implementación de un canal de denuncias gestionado por un asesor externo especializado en la materia, Asesoría Penal Corporativa (en adelante APC), empresa externa especializada en prevención de riesgos penales y asesoramiento penal a empresa.

El link de acceso al canal de denuncias es:

http://asesoriapenalcorporativa.es/canal-denuncias/synlab/

Se trata de un link que permite un acceso directo a una plataforma en la que el denunciante, a través de un formulario personalizado para la entidad, podrá denunciar la comisión incumplimientos normativos e indicios de comisión de ilícitos penales.

El Canal de Denuncias cumple con los principios, procedimientos y garantías exigidos por la normativa en materia de Protección de Datos de Carácter Personal.

El funcionamiento del canal de denuncias y la tramitación de las mismas se encuentra regulado en el "Protocolo Canal de Denuncias" de fecha 29 de enero de 2018.

XV. Sistema disciplinario - Sanciones por comportamiento indebido

Los incumplimientos requieren una sanción apropiada con independencia de la condición del empleado en cuestión (incluyendo, por ejemplo, impago de bonificaciones, acciones legales o despido) para ello, en cumplimiento con el art.31bis 5 del Código Penal, se desarrolla un sistema disciplinario establecido para sancionar la violación del principio de legalidad con el objetivo de dotar de eficacia al Modelo de Prevención de Delitos. El Sistema disciplinario se articula en base a las siguientes garantías y criterios:

- Estatuto de los trabajadores art.54.2 (indisciplina o desobediencia) y 58.1 (sanciones y faltas de acuerdo a su gravedad).
- El Órgano de Cumplimiento Interno conservará un registro de sanciones disciplinarias.
- Acorde al Convenio Colectivo aplicable al sector o a la entidad.

A tal efecto, serán constitutivas de infracción muy grave y susceptibles de la imposición de sanción las siguientes conductas:

- El incumplimiento de las previsiones de los distintos protocolos y medidas que se implementen en la entidad en materia de cumplimiento normativo y responsabilidad penal.
- Impedir o dificultar el descubrimiento de actuaciones ilícitas.
- La infracción del deber específico de poner en conocimiento del Órgano de Control los incumplimientos y actividades ilícitas de los que se tenga conocimiento.

XVI. Procedimientos para la delegación de facultades

En los casos en los que la Dirección de SYNLAB delegue la toma de decisiones en ámbitos en los que exista riesgo penal mayor que bajo, SYNLAB establecerá y aplicará un procedimiento y un sistema de controles que garanticen que el proceso de decisión y el nivel de autoridad de los decisores sean adecuados y estén libres de conflictos de interés reales o potenciales.

XVII. Objetivo

Los objetivos de Compliance penal son coherentes con lo establecido en esta Política de Compliance penal y con los resultados de la identificación y evaluación de riesgos penales, son objeto de seguimiento según la planificación establecida una vez se ha realizado el proceso de evaluación de los riesgos penales, comunicados, medibles (si es posible) y se actualizan según corresponda.

Diligencia de entrega de la Política de Compliance

La Política de Compliance de SYNLAB ha sido aprobada por el Órgano de Administración en fecha 29 de enero de 2018.

El acceso o entrega a la Política de Compliance vigente requiere que todos los miembros de la organización la cumplan junto con el resto del sistema de gestión de Compliance penal.

Se adoptarán acciones disciplinarias proporcionales contra aquellos miembros de SYNLAB que incumplan los requisitos derivados de esta Política o del resto del sistema de gestión de Compliance Penal.

- Se hace constar que XXXXXXXXXX, con DNI XXXXXXXXX y cargo en la empresa de XXXXXXX, ha recibido la Política de Compliance vigente de SYNLAB.

Fecha:

Firma:

SYNLAB

POLÍTICA DE CONTROL Y VIGILANCIA

SYNLAB	POLÍTICA DE CONTROL Y VIGILANCIA DE LAS INSTALACIONES	Creación: 2/06/2017 Última actualización: 6/07/2017

Elaboración:	Revisión:	Aprobación:
Nombre. OIC Cargo. Firma. Fecha: 02-06-2017	Nombre. OIC Cargo. Firma. Fecha: 06-07-2017	Nombre. O ADM. Cargo. Firma. Fecha: 30-01-2018

Versión	Fecha	Afecta	Breve descripción del cambio
1ª	06-7-2017		

I. VIGILANCIA Y CONTROL DE LAS INSTALACIONES

OBJETO.

El presente protocolo tiene por objeto asegurar la vigilancia de las instalaciones de SYNLAB HOLDING IBERIA S.A. (en adelante SYNLAB), con el objetivo de establecer controles que eviten la entrada de terceros no autorizados así como la práctica de actividades ilícitas por trabajadores de la misma.

ALCANCE.

El presente protocolo será de aplicación a las instalaciones de Barcelona, Madrid y Málaga.

CONTROL DE INSTALACIONES.

En las instalaciones de Madrid y Barcelona existe control de acceso por huella.

De momento, en Málaga al ser un laboratorio de dimensiones más reducidas no se ha instalado el sistema. El acceso al laboratorio de Málaga es controlado desde la recepción.

En el caso de que en la empresa, en algún período concreto, existan espacios de cualquier tipo que no se estén utilizando para la actividad y respecto de los que exista riesgo de acceso por terceros se llevarán a cabo los siguientes controles:

SYNLAB llevará un control de los espacios vacíos que consistirá en la cumplimentación de la tabla que se indica a continuación.

El objetivo de ésta política es la evitación de conductas delictivas por parte de los trabajadores o de terceros en espacios de la empresa que quedan fuera del

control diario de la empresa por estar apartados, o no ser objeto de utilización en la actividad en estos momentos.

Todos aquellos trabajadores que detecten acceso por terceros o prácticas indebidas en los espacios mencionados deberán ponerlo en conocimiento del Comité de Compliance.

Fecha de inicio	Espacio vacío	Control implementado	Fecha de finalización

II. CONTROL DE ACCESOS A LAS INTALACIONES

1. OBJETO

El presente procedimiento tiene como objeto establecer las normas y medidas a seguir para el control y registro de personal y vehículos ajenos a la empresa que accedan al recinto de SYNLAB.

2. ALCANCE

Este documento es de aplicación a todas las personas y vehículos, tanto turismos como industriales, no pertenecientes a la empresa que accedan a las instalaciones sin tener autorización expresa para ello.

3. FUNCIONES DEL PERSONAL DE SYNLAB

- ***Guarda de seguridad en las instalaciones de Barcelona:*** de 20.00h a 8.00h realiza vigilancia de las instalaciones.

- ***Persona destino de la visita.*** Es la persona que recibe la visita, los acompaña durante su estancia en el centro de trabajo. Deberá informarles sobre las normas de comportamiento en las instalaciones y sobre la utilización de EPI,s. Se asegura que la visita ha pasado el control de acceso.

- ***Personal administrativo de recepción en Barcelona.*** Se encarga de registrar el acceso de todas las personas y vehículos que sean afectados por el presente procedimiento a su entrada a la explotación.

Además, se encargará de entregar una hoja informativa con las normas de seguridad y las medidas básicas de actuación en caso de emergencia a toda visita que no haya accedido con anterioridad a las instalaciones.

- Serán las personas encargadas de entregar a las personas que realizan la visita los equipos de protección necesarios.

4. PROCEDIMIENTO

ACCESO DE VEHICULOS

Las únicas instalaciones con acceso de vehículo son las de Barcelona. Todo visitante puede aparcar.

ACCESOS DE PERSONAS

Todas las personas ajenas a la explotación se detienen en recepción, donde la persona de recepción toma los datos identificativos en la ficha de control; En ella consta los siguientes datos:

- Fecha.
- Nombre y apellidos.
- Documento Nacional de Identidad.
- Empresa.
- Persona de destino.
- Hora de entrada y salida.

Al terminar la visita, esta pasa por recepción para hacer entrega de las tarjetas de visita al guarda de seguridad, registrando este la hora de salida.

Visitas a parte técnica y laboratorio, por personal y técnico externos deben ir siempre acompañados o ser autorizados por personal interno de SYNLAB.

SYNLAB

PROTOCOLO DE GESTIÓN DE LOS RECURSOS FINANCIEROS

Elaboración:	Revisión:	Aprobación:
Nombre. OCI Cargo. Firma. Fecha: 01-06-2016	Nombre. OCI Cargo. Firma. Fecha: 29-01-2016	Nombre. O. Aud. Cargo. Firma. Fecha: 30-01-2016

Versión	Fecha	Afecta	Breve descripción del cambio
1ª			

El Código Penal español, en su artículo 31 bis. 5. 3., exige que el Modelo de Prevención de Delitos prevea una adecuada gestión de los recursos financieros para prevenir y detectar tempranamente eventuales riesgos penales en el seno de la empresa.

Por ello, el Órgano de Administración de SYNLAB HOLDING IBERIA, S.A. se compromete a que se desplieguen los recursos necesarios para asegurar que el sistema de gestión logre su objetivo: prevenir la comisión de delitos en el ámbito de la entidad, y así lo ha hecho constar en Acta de fecha 1 de abril de 2016 suscrita por los Administradores Mancomunados.

La correcta gestión de los recursos financieros debe ser analizada desde dos puntos de vista.

Por un lado, implica:

1. La creación de una partida presupuestaria destinada a incorporar la figura del Órgano de Control Interno, dotarlo de los medios humanos y técnicos adecuados como así también de la infraestructura organizativa y tecnológica necesaria para un eficaz desempeño de sus funciones.
2. Destinar recursos para implementar un eficaz canal de denuncias en el cual se comuniquen los incumplimientos internos o presuntas actividades ilícitas dentro de la entidad, con el fin de conocer sus causas y poder gestionarlas.
3. Destinar recursos a la divulgación del Modelo de Prevención de Delitos a todo el personal de la entidad.
4. Destinar recursos al desarrollo del plan anual formativo en prevención de riesgos penales y responsabilidad penal de la empresa.

Por otro lado, la correcta gestión de los recursos financieros hace referencia a que SYNLAB debe implicarse con una adecuada y responsable gestión de éstos a fin de *impedir la comisión de los delitos que deben ser prevenidos* (art.31bis.5.3 Código Penal).

A este respecto, esa responsable gestión de los recursos financieros se vislumbra con la implementación, control y supervisión de cada uno de los Protocolos o Políticas internas creadas y actualmente implementadas por SYNLAB a efectos de prevenir los riesgos penales a los que se encuentra expuesta esta área, a saber:

- Código de conducta
- Política de Compliance
- Protocolo antifraude y anticorrupción.
- Protocolo de adopción de decisiones fiscales.
- Protocolo de TIC´s.
- Protocolo de trazabilidad de donaciones.
- Política de control y vigilancia.
- Política de propiedad intelectual e industrial
- Protocolo Órgano de Control Interno
- Protocolo Canal de Denuncias

SYNLAB

POLÍTICA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

TIC

Elaboración:	Revisión:	Aprobación:
Nombre. OCi Cargo. Firma. Fecha: 01-06-2017	Nombre. OCi Cargo. Firma. Fecha: 29-01-2018	Nombre. ADM. Cargo. Firma. Fecha: 30-01-2018

Versión	Fecha	Afecta	Breve descripción del cambio
1ª	29-1-2018	Creación	

INDICE

1. INTRODUCCIÓN

El presente protocolo recoge la normativa y procedimientos de **SYNLAB HOLDING IBERIA, S.A.** (en adelante SYNLAB), en relación con las herramientas puestas a disposición de los trabajadores para el desarrollo de sus actividades laborales, con el objetivo de crear una cultura empresarial de actuación acorde a la legalidad y evitar así cualquier tipo de conductas delictivas que pudieran darse en relación con dichos medios.

Ello debido a que en las empresas es cada vez mayor la utilización de las nuevas tecnologías, lo que ha creado, en ciertas circunstancias, la necesidad de control de estas herramientas por parte del empresario. No obstante, ello puede suponer una quiebra de la intimidad del trabajador constitutivo de un delito contra la intimidad.

Aun así, este derecho a la intimidad del trabajador, debe conciliarse con los derechos e intereses legítimos del empleador, como el derecho a velar por la eficacia de la empresa y protegerse del perjuicio que pudiera ocasionar a la empresa las acciones del trabajador.

Es interesante, hacer una breve referencia a la normativa y jurisprudencia existente en esta materia:

El Convenio Europeo para la Protección de los Derecho Humanos establece que toda persona tiene derecho al respeto de la vida privada y familiar y prohíbe la injerencia que no esté prevista en la ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás.

Asimismo, nuestra Constitución Española, recoge como derecho fundamental el derecho a la intimidad personal y familiar y a la propia imagen, así como el secreto de las comunicaciones.

Por su parte, el Estatuto de los Trabajadores en su art. 20 dispone que el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

Los Tribunales han interpretado esta cuestión y, como ejemplo, la sentencia del Tribunal Supremo de 26 de septiembre de 2007 (Sala de lo Social) establece lo siguiente:

"....**las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario "como propietario o por otro título" y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen.** Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la esfera personal del trabajador.

... Se trata de medios que son propiedad de la empresa y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario,

que, como precisa el artículo 20.3 del Estatuto de los Trabajadores , implica que éste "podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales", aunque ese control debe respetar "la consideración debida" a la "dignidad" del trabajador".

Asimismo, la mencionada sentencia estableció que existe un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esta tolerancia crea una expectativa de confidencialidad que debe ser tenida cuenta. Por ello, dispone a continuación que **las empresas deben fijar previamente las reglas de uso de los instrumentos de trabajo** (p. ej. estableciendo prohibiciones absolutas o parciales, o permitiendo el uso personal por parte de los empleados) **y deben informar a los trabajadores** -y a sus representantes legales, de haberlos- de cuáles son esas reglas, de los controles y medidas aplicables por parte de la empresa. De este modo desaparece la expectativa de intimidad de los trabajadores sobre esos medios y su control no debería generar un posible delito contra la intimidad.

Aunque esta doctrina se ha flexibilizado en virtud de sentencias posteriores del Tribunal Supremo y del Tribunal Constitucional, es recomendable que las empresas dispongan de un protocolo de actuación en materia de uso de TICs.

1.1. Objetivo y alcance

Mediante el presente protocolo SYNLAB pretende establecer un sistema de uso y control del conjunto de las tecnologías de la información que se utilizan por parte de los miembros de la empresa.

Asimismo, se pretende regular el control por parte de la sociedad para que se produzca sin quebranto de la intimidad del trabajador y del derecho al secreto de las comunicaciones, esto es su esfera de privacidad, para evitar la comisión de delitos contra la intimidad en el ámbito de SYNLAB.

Se adjunta al presente protocolo:

- **Anexo I:** las normas de política de uso de las TIC

1.2. Principios generales sobre la vigilancia y control del correo electrónico y la utilización de internet.

Para que la actividad de control por parte del empleador sea legal y esté justificada deben respetarse los principios de protección de datos personales.

Es preciso que las limitaciones impuestas sean necesarias para lograr un fin legítimo y sean también proporcionadas para alcanzarlo y respetuosas con el contenido esencial del derecho a la intimidad.

Los principios que deben respetarse son los siguientes:

1º.- Necesidad: El empleador, antes de proceder a realizar esta actividad de control, debe comprobar si el mecanismo de vigilancia que ha de llevar a cabo es necesario para el caso concreto. Siempre será más apropiado, de ser posible, la utilización de medios más comunes y de menor injerencia en la privacidad del

trabajador; debiendo recurrir a la vigilancia del correo electrónico o uso de internet en circunstancias excepcionales.

2º.- Finalidad: Debe existir un objetivo o fin determinado previo al inicio de la actividad de control y recogida de datos, y este fin debe ser legítimo. Los datos obtenidos deberán utilizarse única y exclusivamente para este fin concreto.

Ej. El tratamiento de los datos puede realizarse a efectos de seguridad del sistema, pero estos datos no podrán utilizarse para supervisar el comportamiento del trabajador.

3º.- Transparencia: El empleador debe indicar de forma clara y abierta sus actividades. Ello implica que el empleador debe:

- Haber informado a sus trabajadores de la política existente en la asociación relativa a la vigilancia del correo electrónico y de la utilización de Internet.
- Debe comunicar a sus trabajadores en qué medida pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales.
- Determinar en qué circunstancias la SYNLAB puede adoptar medidas de vigilancia.
- Informar a los trabajadores de las medidas de vigilancia adoptadas.
- Debe informarse a cada trabajador de cualquier abuso de las comunicaciones electrónicas detectado, salvo que las circunstancias justifiquen la continuación de la vigilancia.

4º.- Legitimidad: La operación de vigilancia y control de los datos únicamente puede realizarse si la finalidad es legítima.

Ej. Control del trabajador por parte del empleador para evitar la transmisión de información confidencial a un competidor.

5º.- Proporcionalidad: Los datos que se utilicen deben ser adecuados, pertinentes y no excesivos en relación con los fines para lo que se han recabado, teniendo en cuenta el tipo y grado de riesgo al que se enfrenta la empresa. Queda por lo tanto excluido, el control general de los correos electrónicos y de la utilización de Internet del personal de la empresa, salvo que sea estrictamente necesario para la seguridad del sistema. Si el objetivo perseguido puede lograrse por un medio que implique una intromisión menor en la vida privada de los trabajadores, deberá aplicarse preferentemente esta opción.

6º.- Exactitud y conservación de los datos: Los datos recopilados deben ser precisos y no almacenarse más del tiempo estrictamente necesario. Normalmente se establece un periodo de conservación de los mensajes electrónicos en el servidor central de la empresa por un periodo de 3 meses.

7º.- Seguridad: Es necesario que el empleador adopte las medidas técnicas y organizativas adecuadas para proteger todos los datos personales que se hallen en su poder de toda intromisión exterior. La persona que durante las operaciones de control acceda a los datos personales de trabajadores debe estar sometido a una obligación estricta de secreto profesional respecto a la información confidencial a la que va a acceder.

1.3. Control del correo electrónico.

Para que el empleador pueda proceder al control del correo electrónico de sus trabajadores, éstos deben haber otorgado su **consentimiento.** No obstante, este consentimiento no puede ser utilizado por el empleador como medio general para legitimar estos controles.

Los trabajadores tienen el derecho fundamental, reconocido en la constitución, al secreto de la correspondencia.

Si el trabajador dispone de cuentas de correo electrónico personales o correo Web, el acceso a las mismas por parte del empleador sólo podría justificarse en circunstancias muy limitadas, pues prevalecería el derecho fundamental al secreto de correspondencia. Si el empleador fomentara la utilización del correo Web para asuntos personales, este modo facilitaría la distinción entre el correo de uso profesional y el correo de uso privado, y reduciría el riesgo de intromisión de los empleadores en la vida privada de sus trabajadores (siempre que los servidores de correo web cuenten con un sistema adecuado de protección de datos de carácter personal).

Por lo tanto, deberá analizarse caso por caso.

A pesar de ello es necesaria una **información mínima que SYNLAB debe facilitar a sus trabajadores**:

- Determinar si el trabajador está autorizado a disponer de cuenta de correo electrónico de uso estrictamente personal, si está permitida la utilización de cuentas de correo Web en el lugar de trabajo y si el recomienda la utilización de un correo web para utilizar el correo electrónico con fines exclusivamente personales.

- Reglas sobre el acceso al contenido del correo electrónico y las finalidades específicas de este acceso.
- Indicar periodo de conservación de las copias de seguridad de los mensajes.
- Precisar cuándo se borran definitivamente los correos electrónicos del servidor.
- Cuestiones de seguridad.
- Participación de los representantes de los trabajadores en la formulación de la política.

1.4. Control de acceso a internet.

SYNLAB es quien debe decidir si autoriza la utilización privada de internet y en qué medida.

En cuanto al control de la utilización de internet, siempre es más recomendable la implementación de medios técnicos para prevenir la utilización abusiva de internet por ej. Limitando accesos o utilizando avisos o advertencias automáticas.

En todo caso, y cuando se lleven a cabo actividades de control sobre los accesos a internet de los trabajadores, la medida de control debe ser proporcionada al riesgo que corra la empresa o el empleador. En muchas ocasiones, basta con llevar a cabo comprobaciones generales, por ejemplo la elaboración de un listado de los sitios más visitados para comprobar si se está llevando a cabo una utilización abusiva de internet, sin analizar el contenido de los sitios visitados.

Si a través de comprobaciones generales se detecta la posible utilización abusiva de Internet, el empleador podría considerar la posibilidad de realizar otros controles.

En todo caso, deberá comunicarse al trabajador los resultados obtenidos y ofrecerle la posibilidad de defender una correcta utilización de Internet.

La **información mínima que deberían recibir los trabajadores en relación a la utilización de internet** es la siguiente:

- En qué condiciones se autoriza la utilización de Internet con fines privados.
- Restricciones existentes: elementos que no pueden ser visualizados o copiados.
- Informar de los sistemas instalados.
- Precisarse el control que puede realizar o realizará la empresa.
- Uso que se llevará a cabo con los datos recogidos.

2. NORMAS DE LA ENTIDAD

La política de uso de las herramientas TIC (Tecnologías de la Información y Comunicación) de SYNLAB persigue garantizar la seguridad en la utilización de los sistemas de información y de las comunicaciones, establecer los sistemas de control y las consecuencias que el incumplimiento de la misma tiene para los empleados.

Las normas contenidas en el presente protocolo son de obligado cumplimiento por parte de todo el personal de SYNLAB y su vulneración podrá conllevar acciones disciplinarias.

SYNLAB implementará las medidas necesarias para llevar a cabo un adecuado control sobre el cumplimiento y respeto de la política de uso de las herramientas TIC.

SYNLAB es una entidad concienciada con la seguridad de sus sistemas de información y vela por el mantenimiento de su seguridad. Asimismo, pretende estar alineada con el cumplimiento de la legalidad y, en concreto:

a. Todos los equipos, infraestructuras y aplicaciones dispuestos al servicio del personal contratado es propiedad de SYNLAB y sólo se permite su utilización para el desarrollo de las tareas establecidas en el ámbito laboral.
b. Todos los datos procesados por los elementos anteriormente mencionados y los resultados son propiedad de SYNLAB conforme a la legislación sobre propiedad intelectual.
c. La empresa no admite la utilización particular de las TIC y herramientas puestas a disposición de los usuarios.
d. El uso de las TIC será controlado tanto por motivos de seguridad como por motivos de control de la actividad laboral.

e. El sistema de control se basará en un sistema proporcional basado en las siguientes premisas:
    a. Ante herramientas que permitan sistemas de control menos invasivos, se procurará previamente el control de estos elementos y, posteriormente, el control de aspectos más concretos que contengan dato.
    b. En todo caso, podrán establecerse sistemas de control basados en catas aleatorias pero que no supongan de inicio un control total de la actividad.
f. Se podrán adoptar las medidas legales oportunas frente al incumplimiento de estas políticas y, en general, frente al incumplimiento de la legalidad vigente.

Esta política se basa en las siguientes premisas:

- Respeto a las normas vigentes en materia de protección de datos.
- Desarrollo de procedimientos y adopción de medidas para el cumplimiento de las obligaciones que afectan a datos personales.
- Diseño de un plan de mejora continua de los procedimientos adoptados.

2.1. CORREO ELECTRÓNICO

Se considerará correo electrónico corporativo tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas y, especialmente, Internet.

En la utilización del correo electrónico corporativo, SYNLAB adopta un modelo de uso no abusivo o desmedido.

Este servicio, en todo caso, no deberá ser utilizado para realizar las siguientes actividades:

- Enviar mensajes con contenidos o ficheros adjuntos ofensivos o inapropiados que puedan considerarse, para quien los recibe, un atentado contra su intimidad personal, honor o dignidad, absteniéndose de efectuar referencias peyorativas de carácter personal en relación con la ideología, religión, creencias, afiliación política o sindical, o realizar comentarios basados en el género, edad, raza, preferencias sexuales, discapacidades físicas o psíquicas, o en la apariencia de las personas.

- Enviar mensajes y/o documentos corporativos a cuentas privadas del trabajador para uso no vinculado a su trabajo, o a cuentas externas de sus familiares o amigos.

- Enviar o reenviar mensajes de correo en cadena o de tipo piramidal.

2.1.1. Normas:

Se establecen las siguientes normas:

1) El correo electrónico sea cual fuese la dirección asignada, se configura como una herramienta de trabajo no exclusiva, colectiva y de libre acceso, asignada a áreas o puestos de trabajo y no a personas.

2) Queda prohibido el uso del mismo para fines no relacionados con las funciones laborales encomendadas. El correo electrónico que SYNLAB pone a disposición de sus empleados es única y exclusivamente para fines laborales.

3) El empleo del nombre o apellidos del trabajador junto al dominio de la empresa en la dirección de correo no significa la asignación por la empresa de un correo personal, es así por motivos organizativos internos.

4) Se podrá realizar copia de seguridad de los emails y acceder al contenido de los mismos ante problemas técnicos o de seguridad o cuando existan sospechas de que no se cumplen estas normas.

5) No se permiten el uso de cuentas de correo distintas a las proporcionadas por la empresa. En el caso de precisar acceso al correo electrónico personal, este constituirá un caso excepcional y deberá realizarse vía web (mediante navegador), en ningún caso mediante el Outlook instalado en el ordenador.

6) El correo electrónico no debe utilizarse como herramienta de difusión de información masiva. Se prohíbe el envío de correos masivos (spam) empleando la dirección de correo electrónico corporativa.

7) Queda prohibido participar en "cartas en cadena".

8) No está permitido manipular las cabeceras de los correos electrónicos con la finalidad de ocultar o falsear la identidad del remitente del mensaje.

9) El correo electrónico es una de las fuentes más importantes de difusión de virus, por lo que se recomienda no abrir mensajes sospechosos.

2.1.2. Controles:

La empresa podrá controlar el uso del correo electrónico mediante un sistema de dos niveles:

- Un primer nivel de control de tráfico y de archivos adjuntos
- Un segundo nivel de control de contenidos

La empresa podrá utilizar también sistemas de control de correos basados en palabras clave u otros sistemas que estime oportunos siempre que esté justificado.

2.2. ACCESO A INTERNET

Los medios técnicos que se ponen a disposición de los empleados de SYNLAB son propiedad de la entidad, que los facilita para que sean utilizados en el cumplimiento de la prestación laboral.

No obstante, el acceso a redes públicas como Internet está abierto para los usuarios de la entidad pero se condiciona a un uso del sistema no abusivo o desmedido.

En este sentido, podrá considerarse una utilización abusiva de las herramientas TIC si causa una disminución en el rendimiento laboral del empleado o si perturba o altera el sistema informático de SYNLAB.

2.2.1. Normas de Uso:

1) El acceso a internet se configura como una herramienta a disposición de los empleados para el cumplimiento de sus tareas.
2) Queda prohibido el uso del mismo para fines no relacionados con las funciones laborales encomendadas.
3) Debates en tiempo real (Chat), redes sociales, sistemas de mensajería instantánea tipo Messenger, así como la instalación de programas P2P (Peer-to-Peer) y de cualquier otro tipo de acceso a entornos o plataformas de intercambio de ficheros.
4) Páginas de ocio, entretenimiento o webs de contenido sexual, xenófobo o que inciten a la violencia.

2.2.2. Controles:

SYNLAB podrá controlar el uso del acceso a Internet proporcionado mediante un control de las páginas visitadas, almacenamiento y control de las cookies, y su utilización en procedimientos disciplinarios o en cualquier orden administrativo o judicial.

La empresa también podrá utilizar otros sistemas de control de la navegabilidad que estime oportunos.

2.3. EQUIPOS

2.3.1. Normas de uso:

1) Los equipos proporcionados por la empresa se configuran como herramienta puesta a disposición de los empleados para el cumplimiento de sus tareas.
2) Queda prohibido el uso del mismo para fines no relacionados con las funciones laborales encomendadas.
3) Queda prohibido trabajar con equipos personales que no sean proporcionados por la empresa, salvo autorización expresa por escrito.
4) Sólo podrán trabajar con equipos portátiles las personas autorizadas a ello por la organización.
5) Cuando se proporcionen equipos portátiles o en general dispositivos móviles el empleado será el responsable de su custodia cuando estén fuera de la empresa.
6) Se procurará en todo caso el acceso del trabajador a los servidores corporativos. Cuando se trabaje en modo local el empleado será

responsable de que la información sea guardada debidamente en el servidor habilitado al efecto para evitar la pérdida de la misma.

2.3.2. Controles:

La empresa podrá controlar el uso de los equipos, incluso el contenido de los mismos, mediante el sistema que estime oportuno.

2.4. DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

2.4.1. Normas de uso:

1) Los usuarios no pueden utilizar dispositivos de almacenamiento externo, salvo en los casos en que se autorice expresamente por escrito y se adopten las debidas medidas de seguridad. No se podrá conectar dispositivos de almacenamiento externo. De igual modo no se podrá utilizar dispositivos propios para uso empresarial, en particular no se permite el uso del correo profesional en dispositivos no suministrados por SYNLAB.

2) La información que se contenga en dichos dispositivos, contenga o no datos de carácter personal, se mantendrá cifrada.

2.4.2. Controles:

La empresa podrá controlar el uso de los dispositivos externos, incluso el contenido de los mismos, mediante el sistema que estime oportuno.

2.5. APLICACIONES

No se podrán descargar o utilizar programas que no estén previa y expresamente autorizados por SYNLAB.

2.6. CÁMARAS DE VIDEOVIGILANCIA

Es posible el uso de cámaras de vídeo vigilancia en zonas comunes y no invasivas cuya finalidad es la seguridad, no obstante, sus grabaciones podrían ser utilizadas para aspectos laborales o penales de importancia.

Existen cámaras de video vigilancia en la zona exterior y zonas de acceso al interior de los laboratorios centrales de Esplugas de Llobregat (Barcelona).

2.7. OTROS ASPECTOS

- No está permitido emplear identificadores y contraseñas de otros usuarios para acceder al sistema.
- No está permitido burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o programas no autorizados.
- No está permitido modificar la configuración de redes, equipos y de cualquier dispositivo de trabajo.
- No está permitido, en general el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario, vulnerando el derecho de terceros, los propios de la

organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

- No está permitido destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de SYNLAB o de terceros.
- No está permitido introducir voluntariamente programas maliciosos (troyanos, keyloggers), virus o cualquier fichero que cause o sea susceptible de causar cualquier tipo de alteración en los sistemas informáticos de SYNLAB o de terceros.
- No está permitido acceder ilegalmente sin autorización o intentar vulnerar medidas de seguridad de ordenadores o redes que pertenezcan a un tercero, así como cualquier actividad previa al ataque de un sistema para recoger información sobre éste, como, por ejemplo, el escaneo de puertos.
- No está permitida cualquier actividad que infrinja o haga uso indebido de los derechos de propiedad intelectual de un tercero.

3. RÉGIMEN DISCIPLINARIO

La infracción de las instrucciones contenidas en la presente política constituirá falta muy grave, y en atención al régimen sancionador interno será susceptible de la imposición de la sanción que corresponda a la conducta de los Destinatarios según el convenio de aplicación correspondiente.

4. DENUNCIAS / MECANISMOS DE REACCIÓN

Todo directivo, trabajador o persona relacionada con la entidad que detecte el incumplimiento de cualquier norma del presente polític deberá denunciarlo en el canal de denuncias habilitado por la Entidad:

http://asesoriapenalcorporativa.es/canal-denuncias/synlab/

Siempre que se detecte cualquier práctica contraria al presente protocolo, la Entidad aplicará los mecanismos de reacción previstos en el Protocolo de funcionamiento del Órgano de Control y del Canal de Denuncias aprobado.

5. REVISIÓN Y ACTUALIZACIÓN

La presente Política deberá revisarse, y en caso que proceda, actualizarse anualmente, así como siempre que se aprecie un riesgo que no había sido previsto, por ejemplo, por estarse utilizando nuevas fórmulas corruptas que no hayan sido evaluadas.

Además, siempre deberá revisarse y actualizarse cuando se detecte la posible existencia de conductas corruptas, así como cuando se inicie un procedimiento judicial o investigador por prácticas que pudieran ser constitutivas de corrupción. En estos casos, además deberá valorarse las nuevas medidas a implantar para evitar que se puedan cometer en el seno de la Entidad prácticas corruptas.

Este Protocolo ha sido aprobada por el Órgano de Administración, cualquier revisión que se realizara deberá informarse de las conclusiones que se alcancen al

Consejo y cualquier modificación o actualización deberá someterse a la aprobación expresa del mismo.