

CÓDIGO ÉTICO Y DE CONDUCTA RNB S.L

Septiembre 2017



Índice

1	Cuestiones generales.	4
1.1	Presentación del Código Ético y de Conducta por la Dirección General.	4
1.2	Introducción: misión y objetivos.	5
1.3	Ámbito de aplicación.	5
1.4	Adhesión al Código	5
1.5	Adecuación e interpretación del Código	6
1.6	Responsabilidad de los/as profesionales de RNB S.L.	6
2	Principios Generales de Ética Empresarial	7
2.1	Imparcialidad	7
2.2	Honestidad	7
2.3	Integridad del profesional/colaborador	7
2.4	Equidad de la autoridad	7
2.5	Competencia leal	7
2.6	Calidad del servicio	7
2.7	Prevención de las actividades delictivas	7
3	Código de Conducta	9
3.1	Conflictos de interés	9
3.1.1	Regalos, obsequios y favores	9
3.2	Tratamiento de la información	9
3.2.1	Información Personal	9
3.2.2	Deber de secreto	10
3.2.3	Uso de información privilegiada	10
3.3	Relaciones con interesados/as	10
3.3.1	Deber de colaboración con las autoridades	10
3.3.2	Medios de comunicación	11
3.3.3	Actividades asociativas y políticas	11
3.3.4	Participación en cursos y conferencias	11
3.4	Relaciones con colaboradores/as	11
3.4.1	Selección y contratación	11
3.4.2	Desarrollo de la vida profesional	11
3.4.3	Seguridad y salud	12
3.4.4	Integridad del/la trabajador/a	12
3.4.5	Obligaciones de los/as colaboradores/as	12
3.4.6	Sistemas de información	13
3.5	Relaciones con proveedores/as	13
3.6	Relaciones con clientes	13
3.7	Normas de Prevención de Blanqueo de Capitales	14
3.8	Información financiera	14

3.8.1	Contabilidad	15
3.8.2	Control interno	15
3.9	Normas anticorrupción	15
3.9.1	Corrupción a funcionarios públicos	15
3.9.2	Corrupción entre particulares	16
3.10	Importación y exportación de bienes	16
3.11	Medios de pago	16
3.12	Utilización de materias primas inflamables	17
3.13	Medio ambiente	17
3.14	Urbanismo	17
3.15	Propiedad intelectual e industrial	17
3.15.1	Derechos de propiedad intelectual e industrial de RNB S.L.	17
3.15.2	Derechos de terceras personas	18
4	Organización y funciones	19
4.1	Comité de cumplimiento	19
4.2	Dirección General/Consejo de Administración	19
5	Canal de Denuncias	20
6	Régimen Disciplinario	21
	Control de versiones	22
	Anexo I: Personas vinculadas	23
	Anexo II: Código ETI (Ethical Trading Initiative/ Iniciativa de Comercio Ético).	24
	Anexo III: Política de uso aceptable de los activos de información	27

1 Cuestiones generales.

1.1 Presentación del Código Ético y de Conducta por la Dirección General.

Con este documento queremos hacer llegar a todas las personas que forman parte de RNB S.L. o que tienen algún tipo de relación con la empresa, los principios clave de nuestra cultura y nuestros valores éticos. Supone una guía de comportamiento y reafirma nuestra voluntad de mantener los mejores estándares de honestidad e integridad. Nos ayuda, además, a hacer mejor lo que ya estábamos haciendo bien. Ha sido elaborado por el Departamento de Personas y cuenta con el pleno apoyo de la Dirección.

La ética empresarial se ha convertido en pieza fundamental para la sostenibilidad de las organizaciones y para contribuir de manera positiva a nuestro entorno y por ello, este Código tiene una importancia central para todas las personas que trabajamos en RNB S.L.

Cada uno/a de los/as trabajadores/as de la empresa tenemos la obligación de adaptarnos a las líneas de trabajo y normas internas de la compañía, ya que nuestra conducta en el día a día repercute directamente en la imagen, integridad y credibilidad de la empresa.

Para ayudarnos a que las decisiones y acciones tomadas se hagan con un criterio común y adecuado, este Código recoge el siguiente contenido:

- Los valores éticos que guiarán nuestra actuación.
- La conducta esperada con nuestros grupos de interés significativos.
- Los principios específicos y conductas esperadas ante ellos.
- Las directrices para hacer cumplir el Código y tener canales para comunicar inquietudes, dudas o desviaciones del mismo.

Os animamos a leerlo con detenimiento y a familiarizaros con él.

Asimismo, estamos a vuestra disposición para cualquier consulta, comentario o aclaración sobre el mismo.

Y si, en cualquier caso, se detecta alguna actitud contraria a los principios establecidos en este documento, es vuestra responsabilidad comunicarlo para su debido control y cumplimiento, mediante el protocolo que definiremos más adelante.

Un afectuoso saludo.

Dirección de RNB S.L.

1.2 Introducción: misión y objetivos.

La integridad y el comportamiento ético son los pilares sobre los que queremos fundamentar nuestra actividad. Solo actuando de esta manera internamente y trasladándola hacia el exterior aportaremos el valor añadido necesario a nuestros grupos de interés, y aseguraremos nuestra reputación y continuidad.

Además, los cambios normativos recientes, así como la realidad del mundo empresarial, aconsejan la implantación de un Código Ético y de Conducta como guía de referencia dirigido tanto a empleados/as, como a terceras partes con las que la compañía tenga relaciones.

En aras del cumplimiento de las modificaciones del Código Penal en julio de 2015, este Código Ético no solo es un procedimiento de conducta interna, sino un documento más en el sistema de prevención de delitos que la compañía tiene implantado a estos efectos.

Durante todos los años de trayectoria empresarial de RNB S.L., el correcto desempeño de la actividad profesional ha sido intachable y este Código solo viene a reforzar los valores de nuestra compañía, personalizados en las acciones que día a día realizamos empleados/as, directivos/as, administradores, proveedores/as... y en el establecimiento de un marco normativo interno al que todos/as han de adherirse para seguir avanzando por el buen camino hacia un provechoso futuro.

1.3 Ámbito de aplicación.

Este Código Ético es de aplicación a los Administradores y miembros del Consejo de Dirección, y a todas las personas que trabajan en RNB S.L., con independencia de su nivel jerárquico y de su ubicación geográfica o funcional, considerándose “profesionales” tanto el personal de Dirección como el resto de la plantilla. Especial mención se hace a los/as profesionales con poderes de representación de la entidad o que dirijan o gestionen grupos de personas que, además, deberán velar porque sus equipos conozcan y apliquen el contenido del Código, además de ser referentes de conducta frente a estas personas.

El cumplimiento de este Código no sustituye a otros documentos implantados en la empresa y que sean de necesaria regulación y aplicación con motivo de otras normativas sectoriales: sistemas de buen gobierno corporativo, reglamentos internos de conducta y sus normas de desarrollo, etc.

El Código también será de aplicación a terceras personas o empresas proveedoras, con las que RNB S.L. tenga relaciones de mercado, y se trasladará la obligación de su cumplimiento vía contrato, permitiendo conocer este documento, que estará colgado en la web corporativa de la compañía, para su revisión y conocimiento general.

1.4 Adhesión al Código

Con carácter general la adhesión al Código se producirá en el caso de los/as profesionales de la empresa en el momento de su incorporación mediante la aceptación de la siguiente cláusula incluida en el contrato:

“El/la trabajador/a o proveedor/a, declara expresamente que conoce el código ético y de conducta de la compañía y el plan de prevención de delitos, ha firmado el código ético de la misma y se compromete a cumplirlo íntegramente. En caso de conocerse alguna conducta contraria al código ético es obligatorio ponerlo de manifiesto a través del canal de denuncias”

En el caso de proveedores/as de servicios que deban de estar sujetos/as al presente código, la adhesión al mismo se realizará con carácter previo al inicio de la prestación del servicio. Dicha adhesión se realizará mediante la firma del contrato de prestación de servicios en el cual se incluye dicha cláusula.

Para aquellos/as profesionales que ya tienen una relación previa con RNB S.L. anterior a la entrada en vigor del presente Código, el Departamento que coordine esta relación será el encargado de recabar la aceptación del mismo de todos/as los/as profesionales y directivos/as.

RNB, S.L. está integrada en la plataforma internacional SEDEX, destinada al intercambio de información sobre la producción éticamente sostenible en la cadena de suministro, y como miembros, nos adherimos además a su propio Código Ético. (Anexo II)

1.5 Adecuación e interpretación del Código

Este Código Ético trata de exponer y abarcar las directrices más comunes de actuación que puedan plantear dudas de comportamiento a los/as profesionales que les aplica.

No obstante, es posible que no llegue a todas las situaciones que pueden acontecer en el seno de la compañía, por lo que para la interpretación y adecuación de estas pautas al día a día de la actividad empresarial, el Departamento de Personas estará disponible para colaborar en la fijación de criterios y para resolver las dudas que puedan plantearse en el desarrollo de su actividad profesional.

1.6 Responsabilidad de los/as profesionales de RNB S.L.

Las personas sujetas al presente Código tienen la obligación de:

- Comunicar mediante el canal de denuncias cualquier incumplimiento de este Código.
- Proporcionar la información necesaria para poder realizar las investigaciones que se realicen.
- Comunicar al Departamento de Personas la existencia de cualquier procedimiento judicial penal en el que la persona figure como imputada, acusada o condenada, extendiéndose tal deber de comunicación a los expedientes.

2 Principios Generales de Ética Empresarial

2.1 Imparcialidad

RNB S.L. evita cualquier tipo de discriminación por edad, sexo, sexualidad, estado de salud, nacionalidad, opiniones políticas y creencias religiosas de sus interlocutores/as, en sus relaciones con las partes implicadas, tales como la gestión de personas o la organización del trabajo, la selección y la gestión de los/as proveedores/as y colaboradores/as, la presentación de ofertas a clientes, etc.

2.2 Honestidad

En el ámbito de su actividad profesional, los/as profesionales/as y otros/as terceros/as vinculados a este Código Ético deberán respetar las leyes vigentes, el Código Ético y cualquier otro procedimiento interno que les sea de aplicación y les haya sido formalmente comunicado de forma previa. La consecución de los intereses de la compañía nunca puede estar soportado en una conducta deshonestas.

2.3 Integridad del profesional/colaborador

RNB S.L. se compromete a velar por la salud y la seguridad de sus empleados/as, contratistas, visitantes y clientes/as, y a ofrecer un lugar de trabajo seguro, con condiciones de trabajo que respeten la dignidad individual.

La compañía no admite, en el entorno laboral, que se produzcan episodios de intimidación o acoso, ni solicitudes o amenazas dirigidas a inducir a las personas a actuar en contra de la ley o del Código Ético. No se tolera la adaptación de comportamientos que tiendan a lesionar convicciones o preferencias personales.

2.4 Equidad de la autoridad

En las relaciones jerárquicas, la organización se compromete a actuar de forma correcta, equitativa y evitando cualquier tipo de abuso.

2.5 Competencia leal

La Compañía se compromete a imponer y preservar el principio de competencia leal, evitando el abuso de posiciones de poder, en la relación con sus terceros y profesionales.

2.6 Calidad del servicio

Los profesionales prestan sus servicios en la Compañía aportando el máximo grado de entrega y profesionalidad, en cumplimiento además del presente Código Ético.

Las prestaciones de servicios, contratos y otros encargos se llevarán siempre conforme a lo establecido de forma voluntaria por las partes, comprometiéndose la Compañía a interpretar la regulación contractual de la relación de forma no maliciosa ni en beneficio propio o diferente del perseguido por el contrato de servicios.

2.7 Prevención de las actividades delictivas

Todas las personas sujetas han de ser conscientes de que, como consecuencia del actual marco legislativo en materia penal, cualquier persona jurídica puede resultar condenada por delitos cometidos por sus administradores/as y empleados/as cuando de su comisión se hubiera derivado algún tipo de beneficio para la persona jurídica en cuestión.

RNB S.L. reniega de cualquier beneficio obtenido ilícitamente o como consecuencia del incumplimiento de alguno de los estándares éticos y compromisos contenidos en este Código. Consecuentemente, las personas sujetas han de cumplir con extremo rigor las normas y procedimientos establecidos.

3 Código de Conducta

3.1 Conflictos de interés

Los/as profesionales de RNB S.L. deben evitar situaciones en las que las partes vinculadas a las operaciones estén en un conflicto de intereses.

Existe conflicto de interés cuando la oportunidad de ganancia de un/a trabajador/a podría interferir con su criterio, objetividad, independencia o lealtad hacia RNB S.L. También cuando dicha ganancia afecta a personas vinculadas al trabajador. En el **Anexo I** se exponen aquellas que se consideran personas vinculadas.

Los Administradores, miembros del Consejo de Administración, directivos/as y profesionales de la compañía deberán poner en conocimiento del COMITÉ DE CUMPLIMIENTO cualquier situación en la que se pueda dar un conflicto de intereses. Así mismo es necesario que se abstenga de intervenir en decisiones que puedan influir en las relaciones con las personas vinculadas, con la finalidad de evitar que se pudiera dar el caso de influencia sobre la decisión.

3.1.1 Regalos, obsequios y favores

Cualquier tipo de regalo que pueda ser interpretado como algo que excede las prácticas comerciales o de cortesía normal o, de cualquier forma, destinado a recibir un trato de favor en la realización de cualquier actividad que se pueda vincular a la entidad, no será admitido. En este sentido, los regalos de agradecimiento recibidos de proveedores/as se entregarán al Departamento de Personas para incluirlos en un sorteo en el que participan todos/as los/as trabajadores/as de la compañía (excepto los miembros del Comité de Dirección) ya que entendemos que cada trabajador/a está contribuyendo con el desempeño de sus funciones a los objetivos de la compañía.

Del mismo modo, quedará prohibida cualquier forma de regalo a funcionarios/as públicos/as españoles/as o extranjeros/as, auditores/as, consejeros/as de RNB S.L. o a sus familiares, que pueda influir en la independencia de juicio o inducir a garantizar cualquier tipo de favor.

Se excluyen de dicha limitación:

- a) Los objetos de propaganda de escaso valor.
- b) Las invitaciones normales que no excedan de los límites considerados razonables en los usos habituales, sociales y de cortesía.
- c) Las atenciones ocasionales por causas concretas y excepcionales siempre que no sean en metálico y estén dentro de límites razonables.

3.2 Tratamiento de la información

La información manejada por los/as profesionales de RNB S.L. puede suponer tanto información interna (de sus socios/as, administradores, directivos/as o empleados/as, *know-how* de la empresa, información sobre la propia empresa) como información que los/as clientes/as faciliten a la compañía en el seno de su relación profesional.

3.2.1 Información Personal

RNB S.L. se compromete a garantizar que todos los datos personales que obran en su poder como responsable de fichero, en virtud de la normativa vigente en materia de protección de datos, son tratados, almacenados y custodiados conforme a las directrices de dichas normas, y que se cumplen los principios de calidad, información y consentimiento respecto de los datos manejados, destinándose en exclusiva al fin que justifique o ampare su tratamiento. Del mismo modo, la

compañía aplica las medidas de seguridad necesarias y garantiza el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición) correspondientes.

RNB S.L. ha informado a toda la plantilla del tratamiento de sus propios datos, pero también de la confidencialidad debida respecto del manejo de información personal que puede efectuar en su día a día laboral. Asimismo, RNB S.L. ha definido, vía contrato, las obligaciones de terceras partes implicadas en el tratamiento de los datos, como encargados/as de tratamiento, a los efectos de lo previsto en la normativa vigente.

3.2.2 Deber de secreto

Además de lo anterior, y respecto de determinado tipo de información relativa a la empresa sobre la que se tiene el deber y la obligación contractual de guardar secreto, con carácter general, los/as profesionales sujetos/as al Código deben guardar secreto profesional respecto a cuantos datos o información no públicos conozcan como consecuencia del ejercicio de su actividad profesional, ya procedan o se refieran a clientes/as, a otros/as empleados/as o directivos/as o a cualquier otra persona. Esta obligación subsistirá incluso cuando haya finalizado la relación contractual.

La persona que se incorpora a la plantilla de la compañía, mediante la siguiente cláusula incorporada en la documentación de acogida, lee, comprende y acepta que:

“Adicionalmente al secreto profesional exigido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el empleado deberá guardar asimismo el debido sigilo profesional respecto de la información confidencial del negocio de RNB S.L. como lanzamientos, estrategias, incidencias, o toda aquella información, ya sea técnica, financiera, comercial o de cualquier otro carácter, que sea suministrada y/o comunicada por la organización al empleado mediante palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro.

También se incluye como información confidencial aquella relativa a los procedimientos internos de diseño, formulación, fabricación, producción y comercialización, materiales, sustancias, mezclas, cantidades, test de producto, diseños, logos, patentes, marcas, imágenes corporativas, la expresión de ideas corporativas, planes de negocio, estrategias de negocio, uso de tecnologías y máquinas en la empresa, información relativa a clientes, proveedores, empleados, solicitantes de empleo, profesionales del sector colaboradores con la empresa, proyectos de investigación en desarrollo, futuros lanzamientos de productos y campañas de publicidad”

RNB S.L. ha establecido internamente que la información anterior no es de carácter público y por tanto está sujeta a total confidencialidad de manera que no puede, bajo ninguna circunstancia, ser utilizada en beneficio personal ni revelada a terceras partes.

3.2.3 Uso de información privilegiada

Asimismo, estas mismas pautas han de cumplirse en caso de tratar información privilegiada, entendiéndose por tal la relacionada con operaciones o negocios de la compañía, estrategia de mercado, objetivos, oportunidades de mejora, información que no se haya hecho pública, pues de hacerlo podría influir sobre el resultado de esa operación. La divulgación a terceras partes de la información privilegiada de la empresa, está prohibida de forma taxativa.

3.3 Relaciones con interesados/as

3.3.1 Deber de colaboración con las autoridades

Los/as profesionales, deberán de colaborar con los requerimientos de las autoridades dentro del ámbito de sus competencias. La información deberá de ser veraz y de acuerdo a lo solicitado.

3.3.2 Medios de comunicación

Se prohíbe la realización de comunicaciones a terceras partes o medios de comunicación de informaciones de la empresa. En el caso de recibir cualquier solicitud, ésta se deberá de remitir al Departamento de Personas para su debida tramitación y resolución.

Está prohibido divulgar noticias o comentarios falsos o tendenciosos. Todas las actividades de comunicación respetan las leyes, las reglas, las prácticas de conducta profesional y se llevan a cabo con claridad, transparencia y oportunidad, salvaguardando, entre otras, las informaciones sensibles y los secretos industriales.

3.3.3 Actividades asociativas y políticas

La compañía no financia, ni en España ni en el extranjero, a partidos ni a sus representantes o candidatos/as, ni patrocina congresos o fiestas que tengan como único fin la propaganda política. Tampoco proporciona ayudas a organizaciones con las cuales puede haber conflicto de intereses (por ejemplo, sindicatos, asociaciones ecologistas o de defensa de los/as consumidores/as).

La pertenencia a una asociación o partido político se realizará dentro del ámbito personal de los/as profesionales, evitando cualquier vinculación con la empresa.

Si alguna persona de la empresa fuera a desempeñar un cargo público, deberá comunicarlo de forma previa al Departamento de Personas, quien determinará si existen incompatibilidades con el puesto desempeñado.

En caso de que la empresa conozca que alguno de sus profesionales tiene contacto con una asociación cuyos fines sean ilícitos (organizaciones criminales, paramilitares, xenófobas, discriminatorias, con fines terroristas, etc.), lo pondrá en conocimiento de las autoridades pertinentes de manera inmediata.

3.3.4 Participación en cursos y conferencias

La participación de un/a profesional en cursos y conferencias deberá contar con la autorización de su responsable y del Departamento de Personas.

3.4 Relaciones con colaboradores/as

3.4.1 Selección y contratación

La selección de personal se llevará a cabo respetando los principios de igualdad de oportunidades. El Departamento de Personas y el/la responsable del área en la que se ubica la vacante, llevarán a cabo la selección evitando cualquier discriminación por razones de sexo, edad, raza o religión. No se contratará a menores de edad.

3.4.2 Desarrollo de la vida profesional

El establecimiento de la relación laboral se realizará mediante un contrato laboral, no se establecerán formas de trabajo ilegales. En ningún caso se colaborará con el tráfico de seres humanos para su explotación laboral o sexual.

Los/as trabajadores/as extranjeros/as deberán contar con un permiso de trabajo. En caso contrario no podrán ser contratados/as.

A la persona se le informará de los siguientes aspectos, asegurándose de su comprensión:

- Las características del puesto y las tareas a realizar.

- Los elementos normativos y retributivos regulados conforme al convenio colectivo.
- Las normas y procedimientos a adoptar, con el fin de evitar posibles riesgos para la salud vinculados a la actividad laboral.

3.4.3 Seguridad y salud

A todas las personas que trabajan en la empresa se les proporcionan los medios necesarios para el desarrollo de su trabajo en las mejores condiciones posibles, cumpliendo estrictamente con la normativa en materia de prevención de riesgos laborales.

3.4.4 Integridad del/la trabajador/a

El acoso sexual y cualquier otro tipo de discriminación por razón de edad, sexo, sexualidad, raza, estado de salud, nacionalidad, opiniones políticas o creencias religiosas, etc., no están permitidos en el seno de la empresa.

RNB S.L. dispone de un protocolo de Prevención del Acoso, comunicado a toda la plantilla en el momento de su incorporación, y que marca las pautas a seguir tanto para prevenir este tipo de comportamientos como para actuar en caso de que exista algún tipo de sospecha o denuncia.

La empresa se compromete a no vulnerar el derecho a huelga y cualquier otro derecho reconocido en la legislación laboral y convenio colectivo aplicable.

3.4.5 Obligaciones de los/as colaboradores/as

Los/as colaboradores/as deberán mantener un comportamiento ético evitando en todo momento el consumo de drogas o alcohol durante la jornada laboral, comportamientos violentos, situaciones de discriminación o acoso y cualquier intromisión en la vida privada de compañeros/as de forma no consentida.

Está expresamente prohibido dentro del ámbito laboral cualquier comportamiento que pueda dar lugar a la discriminación de otras personas, dentro de estas conductas se encuentra:

- a) Fomentar, distribuir material u opiniones o actuar contra alguna persona o grupo por motivos de raza, ideología, religión, situación familiar, etnia, nación, sexo, género, orientación, enfermedad o discapacidad, utilizando medios de la empresa.
- b) Emitir opiniones en donde se enaltezca delitos con la humanidad, genocidio o apoyo a los/as autores/as de los mismos, utilizando los medios de la empresa

Respecto a los activos de la empresa, los/as profesionales deberán cumplir con lo siguiente:

- a) Los medios proporcionados por la empresa deberán ser tratados de forma que no sufran menoscabos.
- b) Protegerán y cuidarán los activos de los que dispongan o a los que tengan acceso, que serán utilizados de forma adecuada a la finalidad de las funciones profesionales para cuyo ejercicio han sido entregados.
- c) No realizarán ningún tipo de disposición o gravamen sobre los activos de RNB S.L., sin la oportuna autorización.
- d) Cuidarán de que la realización de gastos se ajuste estrictamente a las necesidades de la empresa.
- e) No realizarán ningún acto de enajenación, transmisión, cesión u ocultación de cualquier bien titularidad de RNB S.L., con la finalidad de eludir el cumplimiento de las responsabilidades del mismo frente a sus acreedores.

Este tipo de comportamiento será sancionado mediante aplicación de régimen disciplinario.

3.4.6 Sistemas de información

RNB S.L. dispone de una política publicada en la que se definen directrices claras en cuanto al uso de medios informáticos. Así mismo, aparecen dichas directrices en la documentación que se hace entrega a toda la plantilla a su incorporación a la compañía (Ver Anexo III).

En relación a los sistemas de información, los/as profesionales deberán de cumplir con lo siguiente:

- a) Respetar las normas específicas de la utilización del correo electrónico, acceso a Internet u otros medios similares puestos a su disposición, sin que en ningún caso pueda producirse un uso inadecuado de los mismos.
- b) La creación, pertenencia, participación o colaboración por en redes sociales, foros o blogs en Internet y las opiniones o manifestaciones que se realicen en los mismos, se efectuarán de manera que quede claro su carácter personal. En todo caso, deberán abstenerse de utilizar la imagen, nombre o marcas de la compañía para abrir cuentas o darse de alta en estos foros y redes.
- c) No se podrán utilizar los sistemas de información con la finalidad de vulnerar la intimidad de terceras personas.
- d) No se utilizarán dichos sistemas para acceder a sistemas de información ajenos, interceptar comunicaciones, utilización de programas de origen ilícito con la finalidad de cometer un delito.
- e) No se compartirán o facilitarán usuarios/as y claves de los sistemas propios o ajenos, con la finalidad de proporcionar, a otros/as, un acceso indebido.

3.5 Relaciones con proveedores/as

Los procesos de compra se basan en la búsqueda de la mejor opción para la entidad garantizando en todo momento, en la selección de los/as proveedores/as, los principios de objetividad, transparencia, no discriminación, respeto, integridad, concurrencia y diversificación de ofertas.

La empresa establecerá los procedimientos de compras que aseguren el cumplimiento de estos principios. Así mismo, en la contratación se establecerá el procedimiento por el cual se asegure la adhesión de las empresas proveedoras al presente Código o, en su caso, la presentación del propio para la evaluación por la empresa.

En el caso de la contratación de proveedores/as en países de riesgo, se les exigirán adicionalmente las siguientes salvaguardas:

- Contar con las medidas que garanticen a la plantilla el respeto de los derechos fundamentales, los principios de igualdad de trato y de no discriminación.
- Protección frente a la explotación laboral infantil.
- La posibilidad de realizar inspecciones en las unidades productivas y las sedes operativas de la empresa proveedora, con el fin de comprobar que se satisfacen dichos requisitos.

3.6 Relaciones con clientes

La compañía se compromete a no discriminar arbitrariamente a sus clientes/as. La contratación de clientes/as se guiará por los principios de precio de mercado, transparencia, no discriminación, objetividad, imparcialidad, respeto, integridad y concurrencia.

Se prohíbe la difusión de información falsa o engañosa a clientes/as directos/as e indirectos/as. La información se transmitirá a clientes/as a través del medio de comunicación más oportuno en cada momento.

La información que se facilite al/a la cliente/a se reflejará en los contratos de la forma más clara y transparente posible, evitándose en todo momento un lenguaje que no sea comprensible por los/as clientes/as y la utilización de cláusulas abusivas.

Se prohíbe participar en operaciones alterando ficticiamente el valor de mercado u otras condiciones de venta, así como realizar acciones orientadas a desabastecer el mercado con la finalidad forzar una alteración de los precios.

3.7 Normas de Prevención de Blanqueo de Capitales

A la hora de establecer relaciones con las siguientes tipologías de clientes/as operaciones, se solicitará la aprobación por parte del Departamento Financiero.

- a) Operaciones en las que intervengan personas físicas o jurídicas domiciliadas en paraísos fiscales o territorios de riesgo.
- b) Operaciones que se realicen a nombre de menores de edad, mayores de 70 años o personas que presenten signos de discapacidad mental o con evidentes indicios de falta de capacidad económica para tales adquisiciones.
- c) Operaciones en las que intervengan personas físicas o jurídicas que ocupen o hayan ocupado puestos políticos, altos cargos o asimilados en países generalmente no democráticos, incluyendo su entorno familiar próximo.
- d) Operaciones en las que intervengan personas que están procesadas o condenadas por delitos o resultase ser público o notorio o se tuviera sospecha de su presunta relación con actividades delictivas, siempre que las mismas permitan un enriquecimiento ilícito y que puedan ser consideradas como subyacentes del delito de blanqueo, así como aquellas operaciones realizadas por personas relacionadas con las anteriores (por ejemplo por lazos familiares, profesionales, de origen, en las que exista coincidencia en el domicilio o coincidencia de representantes o apoderados, etc.).
- e) Operaciones en las que intervengan personas físicas o jurídicas con domicilio desconocido o de mera correspondencia (por ejemplo, apartado de correos, sedes compartidas, despachos profesionales, etc.), o con datos supuestamente falsos o de probable no certeza.
- f) Operaciones en las que intervengan personas jurídicas, de reciente constitución, cuando el importe sea elevado con relación a su patrimonio.
- g) Operaciones en las que intervengan personas jurídicas cuando no parezca que exista relación entre las características de la operación y la actividad realizada por la empresa compradora o bien cuando esta no realice ninguna actividad.
- h) Operaciones en las que intervengan fundaciones, asociaciones culturales y recreativas y, en general, entidades sin ánimo de lucro, cuando no correspondan las características de la operación con los objetivos de la entidad.
- i) Operaciones en las que intervengan personas jurídicas que, aun estando registradas en España, están constituidas principalmente por ciudadanos/as extranjeros/as o no residentes en España.
- j) Entregas en efectivo por un valor superior a 2.500 €, o pago mediante instrumentos negociables en los que no conste la verdadera identidad la persona pagadora.

3.8 Información financiera

La información financiera se realizará garantizando el máximo rigor, para poder obtener una visión clara, concisa y equilibrada de la situación financiera de la empresa a los/as accionistas.

3.8.1 Contabilidad

La contabilidad deberá reflejar los siguientes aspectos:

- a) Las transacciones, hechos y demás eventos recogidos por la información financiera efectivamente existen y se han registrado en el momento adecuado.
- b) La información refleja la totalidad de las transacciones, hechos y demás eventos en los que la empresa es parte afectada.
- c) Las transacciones, hechos y demás eventos se registran y valoran de conformidad con la normativa aplicable.
- d) Las transacciones, hechos y demás eventos se clasifican, presentan y revelan en la información financiera de acuerdo con la normativa aplicable.
- e) La información financiera refleja, a la fecha correspondiente, los derechos y obligaciones a través de los correspondientes activos y pasivos, de conformidad con la normativa aplicable.

La información financiera incluye toda la información de carácter contable y económico que la empresa presente a los mercados de valores y registre en los órganos de supervisión. Incluye, por tanto, el informe financiero anual, el informe financiero semestral y las declaraciones intermedias, tanto individuales como consolidadas, y los folletos que, sobre emisiones de instrumentos financieros, formule RNB S.L.

Se prohíbe de manera expresa la alteración de la contabilidad para:

- a) La realización de alzamiento de bienes, o cualquier conducta que suponga una insolvencia punible.
- b) Elusión del pago de tributos a Hacienda o pagos a la Seguridad Social.
- c) Obtención de subvenciones mediante la falsificación de las condiciones requeridas.
- d) Llevanza de doble contabilidad, realización de anotaciones ficticias o no incluir en la misma las anotaciones necesarias.

3.8.2 Control interno

La empresa establecerá los procedimientos de control interno que aseguren que la información financiera se ha elaborado siguiendo la legislación vigente y es correcta.

La información financiera será revisada de forma independiente de forma anual por una empresa auditora externa, que emitirá el informe correspondiente.

Queda expresamente prohibido impedir la actividad inspectora por parte de los Administradores de la empresa.

3.9 Normas anticorrupción

3.9.1 Corrupción a funcionarios públicos

Está prohibida la entrega, promesa u ofrecimiento de cualquier clase de pago, comisión, regalo o retribución a cualesquiera autoridades, funcionarios/as públicos/as, empleados/as o directivos/as de empresas u organismos públicos, ya se efectúe directamente a ellos/as o indirectamente a través de personas o sociedades a ellos/as vinculadas y ya tenga como destinatarios/as a funcionarios/as o empleados/as públicos/as o a otra persona indicada por ellos/as. Esta prohibición se refiere tanto a las autoridades, funcionarios/as o empleados/as públicos/as de España como de cualquier otro país.

No se incluyen en dicha limitación:

- a) Los objetos de propaganda de escaso valor.
- b) Las invitaciones normales que no excedan de los límites considerados razonables en los usos habituales, sociales y de cortesía.
- c) Las atenciones ocasionales por causas concretas y excepcionales siempre que no sean en metálico y estén dentro de límites módicos y razonables.

En todo caso se pondrá en conocimiento del Departamento de Personas cualquier solicitud que se realizará a las personas sujetas a este Código.

3.9.2 Corrupción entre particulares

Se prohíbe la entrega, promesa u ofrecimiento de cualquier clase de pago, comisión, regalo o retribución a cualesquiera empleados/as, directivos/as o administradores/as de otras empresas o entidades, ya se efectúe directamente a ellos/as o indirectamente a través de personas o sociedades a ellos/as vinculadas con la finalidad de que, incumpliendo sus obligaciones en la contratación de productos, servicios o compraventa de bienes, favorezcan a la compañía frente a sus competidores.

No se incluyen en dicha limitación:

- a) Los objetos de propaganda de escaso valor.
- b) Las invitaciones normales que no excedan de los límites considerados razonables en los usos habituales, sociales y de cortesía.
- c) Las atenciones ocasionales por causas concretas y excepcionales siempre que no sean en metálico y estén dentro de límites módicos y razonables.

En todo caso se pondrá en conocimiento del Departamento de Personas cualquier solicitud que se realice a las personas sujetas a este Código.

3.10 Importación y exportación de bienes

La importación y exportación de mercancías se realizará con el estricto cumplimiento de la normativa aduanera en vigor. Por ello se realizarán las declaraciones aduaneras, presentación de documentación y transporte en los medios adecuados y permitidos.

Queda expresamente prohibido el transporte de otros bienes distintos de los autorizados para cada uno de los transportes.

3.11 Medios de pago

Los medios de pago admitidos son:

- a) Moneda en metálico de curso legal
- b) Tarjetas de crédito o débito siempre que el/la titular de la misma se identifique, ya sea mediante la presentación de documentación identificativa (DNI, pasaporte, NIE) o PIN.

No se admitirán medios de pago de los que se tenga sospechas que son falsos o robados. En caso de recibir cualquier tipo de medio de pago falso, se procederá a comunicar al Departamento Financiero quien lo pondrá en conocimiento de las autoridades pertinentes.

Está prohibida cualquier actividad relacionada con la falsificación de moneda, como puede ser la creación o distribución de la misma.

3.12 Utilización de materias primas inflamables

Los productos inflamables se almacenarán con las medidas de seguridad necesarias para evitar la pérdida o robo de los mismos.

Para el transporte de estos productos, son necesarias las medidas de transporte de mercancías peligrosas, se tendrán en cuenta al menos estos factores durante el transporte:

- a) Embalaje, señalización, carga y descarga, manipulación, movimiento en ruta, límites de velocidad y de kilometraje, almacenamiento en tránsito, almacenamiento en destino, y entrega para voladura.
- b) Debe ser protegido y controlado correctamente para prevenir el robo, los accidentes, el sabotaje y mitigar el impacto de un eventual incidente, protegiendo la vida de las personas y los intereses de la Empresa.

3.13 Medio ambiente

Quedan expresamente prohibidas las siguientes conductas:

- Realizar cualquier actividad que tenga un impacto negativo en el medioambiente y/o contravenga la legislación aplicable en la materia.
- Gestionar los residuos de forma que se incumpla la legislación aplicable o las normas internas.
- Solicitar licencias o permisos cuando la actividad a desarrollar se considera contaminante y no se han tomado las medidas adecuadas para evitar las consecuencias nocivas.
- Evitar, retrasar o falsear la realización de las inspecciones de carácter obligatorio.
- Corromper a funcionarios/as públicos/as para la concesión de licencias o permisos, así como para la no realización de las inspecciones.
- Dañar espacios naturales protegidos de forma intencionada, conociendo el régimen de especial protección de los mismos.

3.14 Urbanismo

RNB S.L. se compromete a no realizar actividades que puedan ir en contra de la legislación de urbanismo en vigor, especialmente al respeto de las zonas no edificables, solicitud de las licencias y aprobación de los planes de urbanización, así como evitar cualquier actitud que se pueda entender como una solicitud de concesión de licencias o permisos ilegales.

3.15 Propiedad intelectual e industrial

3.15.1 Derechos de propiedad intelectual e industrial de RNB S.L.

Las personas que trabajan en la empresa respetarán la propiedad intelectual e industrial en relación con los cursos, proyectos, programas y sistemas informáticos; equipos, manuales y videos; conocimientos, procesos, tecnología, *know-how* y, en general, demás obras y trabajos desarrollados o creados en la empresa, ya como consecuencia de su actividad profesional o de la de terceras partes. Por tanto, su utilización se realizará en el ejercicio de la actividad profesional en el mismo y se devolverá todo el material en que se soporten cuando sea requerido.

Solo utilizarán la imagen, nombre o marcas de la empresa ,para el adecuado desarrollo de su actividad profesional en la misma. En el caso de las patentes secretas de la empresa, toda la plantilla guardará secreto profesional, incluso una vez finalizada la relación laboral.

3.15.2 Derechos de terceras personas

Las personas que trabajan en RNB S.L. respetarán asimismo los derechos de propiedad intelectual e industrial que ostenten terceras personas ajenas a la empresa. En particular, no incorporarán, utilizarán o emplearán en la empresa cualquier tipo de información o documentación física o electrónica perteneciente a otra empresa que se haya obtenido como consecuencia del desempeño de un cargo previo o sin el debido consentimiento.

En el desarrollo de las funciones asignadas, no podrán realizar las siguientes conductas:

- Uso de obras científicas o literarias sin el consentimiento del/la autor/a o previo pago de los derechos de autor pertinentes.
- Incluir en la página web corporativa enlaces a páginas web en donde se vulneren los derechos de propiedad intelectual e industrial.
- Utilización de patentes y marcas, incluyendo logotipos sin consentimiento del/la propietario/a.
- Utilización de semillas patentadas sin el consentimiento del/la propietario/a de la patente.
- Divulgar o acceder a datos de una patente secreta de terceras partes.

4 Organización y funciones

4.1 Comité de cumplimiento

La ejecución y mantenimiento del presente Código de conducta son responsabilidad del Comité de Cumplimiento. Las responsabilidades que tiene asignadas son:

- Promover el conocimiento del Código en toda la organización.
- Asesorar en la interpretación y aplicación del mismo.
- Proponer las modificaciones y autorizar los desarrollos del Código que considere oportunas. También autorizará o desarrollará acciones y mecanismos de control que fomenten, supervisen o ayuden a su cumplimiento.
- Aprobar por causa justificada, de la que no se deriven riesgos para la empresa, cualquier propuesta de excepción al cumplimiento del Código.
- Velar para que todas las personas sujetas y los/as terceros/as puedan poner en su conocimiento posibles vulneraciones del Código de forma confidencial.
- Conocer y resolver las denuncias y consultas recibidas, dándoles en cada caso el tratamiento que estime más oportuno. Actuará en cada intervención con total independencia, capacidad y pleno respeto a las personas afectadas y garantizará, en todo momento, la confidencialidad en el tratamiento de las denuncias y consultas que tramite.
- Recabar información de cualquier órgano o unidad de la empresa relativa a los asuntos que conozca.
- Dar cuenta a la Dirección de la compañía y al Consejo de Administración, al menos anualmente, de sus actividades, propuestas y de la difusión y cumplimiento del Código.

El Comité de Cumplimiento estará formado por:

- Aurelio Tornero Feliciano, Director General de Fábrica, que actuará como Presidente.
- Justo Peydro Aznar, Director General de Producto, que actuará como Secretario.
- Gemma Collado Fos, Directora de Personas, PRL y Medioambiente, como miembro del mismo.

4.2 Dirección General/Consejo de Administración

Aprobará la política general de cumplimiento de RNB S.L. Así mismo, recibirá al menos anualmente información del Comité de Cumplimiento sobre la aplicación del sistema de cumplimiento penal.

En última instancia, será quien tomará las decisiones respecto a la actuación de la empresa, en relación a las denuncias presentadas.

5 Canal de Denuncias

RNB S.L. proporciona el acceso al Canal de Denuncias. Dicho canal de comunicación será accesible tanto para los/as profesionales como para los proveedores/as, clientes/as y terceras personas que quieran dar a conocer un incumplimiento del presente Código, quieran consultar cualquier duda de interpretación, o proponer mejoras o modificaciones sobre el mismo. El canal de comunicación se realizará a través de etica@rnbcosmeticos.com

La información que se reciba en dicho canal será tratada de forma confidencial. Se garantiza la obligación del receptor de preservar la identidad de la persona comunicante y la salvaguarda de la información que afecta a todas las personas involucradas en el proceso de comunicación y en el eventual proceso de investigación conforme a la normativa vigente. No obstante, y con carácter general, salvo excepción justificada por el Comité de Cumplimiento, se informará a la persona denunciante sobre la resolución finalmente adoptada.

El procedimiento protegerá al comunicante de buena fe, de cualquier acto de represalia.

Los/as responsables inmediatos/as a los/as que les hubieran sido comunicados/as, por parte de las personas a su cargo, incumplimientos o vulneraciones de la presente norma, deberán notificarlas a su vez, de manera inmediata y con carácter previo a cualquier otra actuación, al Comité de Cumplimiento.

6 Régimen Disciplinario

El incumplimiento del Código puede dar lugar a sanciones laborales, sin perjuicio de las administrativas o penales que, en su caso, puedan también resultar de ello.

Podrá ser sancionado conforme a la normativa laboral los siguientes comportamientos:

- No denunciar un incumplimiento del presente Código cuando se tenga conocimiento del mismo.
- Realizar denuncias falsas, con la finalidad de perjudicar a una tercera persona.
- Realizar cualquier comportamiento discriminatorio o de acoso, contra una persona que haya realizado una denuncia.
- El incumplimiento de lo dispuesto en el presente Código.

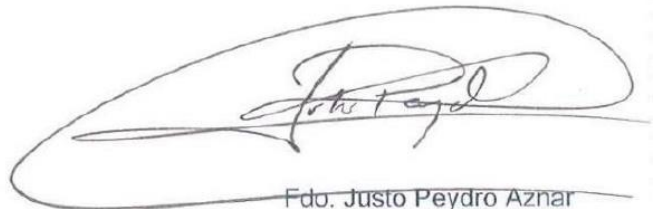
Control de versiones

ESTADO	ELABORACIÓN	REVISIÓN	APROBACIÓN
FECHA	15/07/2017	21/09/2017	21/09/2017
	Gemma Collado	Aurelio Tornero	Vicente Ruiz
		Justo Peydro	Romualdo Bertomeu

En La Pobla de Vallbona, a 22 de Septiembre de 2017



Fdo. Aurelio Tornero Feliciano
Director General de Fábrica



Fdo. Justo Peydro Aznar
Director General de Producto

Anexo I: Personas vinculadas

A los efectos de lo dispuesto en este Código y en cuantas políticas y procedimientos de RNB S.L. sean utilizados estos términos sin atribuirles otra definición, tendrán la consideración de personas equiparadas a la persona sujeta, su cónyuge o persona de análoga relación de afectividad (en los sucesivos, su pareja), hijos/as, nietos/as, padre, madre, abuelos/as, hermanos/as, cuñados/as, yernos, nueras y cualquier persona que conviva con el trabajador y las personas jurídicas que, no siendo sociedades de capital cotizadas en bolsa, se encuentren participadas por alguna de las personas físicas citadas anteriormente.

Anexo II: Código ETI (Ethical Trading Initiative/ Iniciativa de Comercio Ético).

1. El empleo se elegirá libremente

- 1.1.No habrá trabajos involuntarios ni forzados, ni en el marco penitenciario.
- 1.2.Los trabajadores no tendrán que dejar bajo la custodia del empleador "depósitos" ni su documentación de identidad y serán libres de abandonar su empleo con un plazo de aviso previo razonable.

2. Se respetará la libertad de asociación y el derecho a las negociaciones colectivas

- 2.1.Los trabajadores sin distinción alguna, tendrán derecho a afiliarse o constituir los sindicatos de su elección, así como a negociar colectivamente.
- 2.2.El empleador adoptará una actitud tolerante hacia las actividades de los sindicatos, así como sus actividades organizativas.
- 2.3.Los representantes de los trabajadores no serán discriminados y podrán desarrollar sus funciones representativas en el lugar de trabajo.
- 2.4.En aquellos casos en los que la ley restringiera el derecho a la libertad de asociación y a la negociación colectiva, el empleador facilitará y no dificultará el desarrollo de medios paralelos para asociarse y negociar libre e independientemente.

3. Las condiciones de trabajo serán seguras e higiénicas

- 3.1.Se proporcionará un entorno de trabajo seguro e higiénico, teniendo presentes los conocimientos preponderantes de la industria, así como de cualquier peligro específico. Se tomarán las medidas necesarias para evitar accidentes y perjuicios para la salud derivados del trabajo, asociados con él o que ocurrieran en el transcurso del mismo, mediante la reducción, en la medida de lo razonable, de las causas de los peligros inherentes al entorno laboral.
- 3.2.Los trabajadores recibirán formación con regularidad y por escrito en materia de seguridad e higiene, la cual se repetirá para trabajadores nuevos o reasignados.
- 3.3.Se proporcionará acceso a aseos limpios y a agua potable y, si fuera necesario, a instalaciones sanitarias para almacenamiento de comida.
- 3.4.El alojamiento, cuando se proporcione, será limpio y seguro y cumplirá las necesidades básicas de los trabajadores.
- 3.5.La empresa que se acoja al código atribuirá la responsabilidad en materia de seguridad e higiene a un representante de la directiva superior.

4. No se empleará mano de obra infantil

- 4.1.No se contratará mano de obra infantil.
- 4.2.Las empresas desarrollarán o participarán y contribuirán a las políticas que favorezcan el periodo de transición necesario para que cualquier niño/a que desempeñe un trabajo de mano de obra infantil pueda escolarizarse y recibir con continuidad una educación de calidad hasta que deje de ser niño/a. En los anexos se definen los términos "niño/a" y "mano de obra infantil".
- 4.3.No se empleará a niños ni a jóvenes de menos de 18 años para trabajos nocturnos o en condiciones peligrosas.
- 4.4.Estas políticas y procedimientos se ajustarán a las disposiciones de la correspondiente normativa de la OIT.

5. Se pagará un salario digno

- 5.1.** Los salarios y prestaciones abonados por una semana de trabajo estándar habrán de cumplir, como mínimo, la normativa legal nacional o la normativa industrial de referencia, la que fije los salarios y prestaciones más altos. En cualquier caso, los salarios habrán de resultar siempre suficientes para cubrir las necesidades básicas y disponer de ciertos ingresos discrecionales.
- 5.2.** Se proporcionará a todos los trabajadores información por escrito y comprensible sobre sus condiciones de trabajo en relación con los salarios antes de aceptar el empleo y sobre los detalles de sus salarios durante el periodo de pago en cuestión, cada vez que perciban su salario.
- 5.3.** Las deducciones del salario como medida disciplinaria no estarán permitidas ni tampoco se practicará ninguna deducción no prevista por la legislación nacional sin el consentimiento expreso del trabajador en cuestión. Todas las medidas disciplinarias deberán registrarse.

6. Las horas de trabajo no serán excesivas

- 6.1.** Las horas de trabajo deberán ajustarse a la legislación nacional, los convenios colectivos y lo estipulado en los puntos 6.2 a 6.6 siguientes, lo que ofrezca mayor protección a los trabajadores. Los subapartados 6.2 a 6.6 se basan en la legislación laboral internacional.
- 6.2.** Las horas de trabajo, excluidas las horas extraordinarias, se definirán contractualmente y no superarán las 48 horas semanales*.
- 6.3.** Las horas extraordinarias serán voluntarias y se realizarán de forma responsable, teniendo en cuenta los siguientes aspectos: el alcance, la frecuencia y las horas trabajadas por cada trabajador de manera individual y la plantilla en su conjunto. No deberán ocupar el lugar de un empleo habitual. Las horas extraordinarias se compensarán siempre con una prima, que se recomienda que no sea inferior al 125% del salario habitual.
- 6.4.** El número total de horas trabajadas en cualquier período de siete días no superará las 60 horas, salvo si se diese alguna de las situaciones que se indican en el punto 6.5. siguiente.
- 6.5.** Las horas de trabajo podrán superar las 60 horas en cualquier período de siete días en circunstancias excepcionales cuando se den todas las situaciones siguientes:
- La legislación nacional lo permite;
 - Cuando lo permita un convenio colectivo que haya sido negociado libremente con un sindicato que represente una parte significativa de la plantilla;
 - Cuando se tomen las medidas oportunas para salvaguardar la salud y la seguridad de los trabajadores; y
 - Cuando el empleador pueda demostrar que concurren circunstancias excepcionales como, por ejemplo, picos de producción inesperados, accidentes o emergencias.
- 6.6.** Los trabajadores contarán como mínimo con un día libre por cada período de siete días o, cuando la legislación nacional lo permita, dos días libres por cada período de 14 días.

7. No habrá discriminación

- 7.1.** No habrá discriminación a la hora de contratar, indemnizar, formar, promocionar, despedir o jubilar por motivos de raza, casta, origen nacional, religión, edad, minusvalía, sexo, estado civil, orientación sexual o afiliación sindical o política.

8. Se proporcionará un trabajo regular

- 8.1.** En todos los aspectos, el trabajo desempeñado deberá basarse en relaciones laborales reconocidas establecidas a través de la legislación y las prácticas de ámbito nacional.

* La legislación internacional recomienda la reducción progresiva de las horas de trabajo normales, cuando proceda, a 40 horas semanales, sin ningún tipo de rebaja en el salario de los trabajadores como consecuencia de la reducción de horas

8.2. Las obligaciones para con los empleados conforme a la legislación y las normativas laborales o del sistema de la seguridad social, dimanantes de las relaciones laborales convencionales, no se eludirán a través del uso de contratos solo laborales, subcontratos o contratos de trabajo doméstico, ni a través de programas de prácticas en los que no exista intención de dotar de habilidades al trabajador o de proporcionarle un empleo regular, como tampoco se eludirán dichas obligaciones a través del uso excesivo de contratos de duración limitada.

9. No se permitirá un trato inhumano o severo

9.1. Quedan prohibidos el abuso o los castigos de tipo físico, la amenaza de abuso físico o acoso sexual o de otro tipo, así como el abuso verbal u otras formas de intimidación.

Anexo III: Política de uso aceptable de los activos de información

1. Objeto, Finalidad y ámbito de aplicación

En RNB SL somos conscientes de lo necesarias que son los activos de información y las comunicaciones en el ámbito laboral, y para garantizar el buen uso de dichos activos hemos elaborado el presente documento, cuyo objetivo es definir el uso aceptable de los activos de información, así como garantizar la seguridad, rendimiento, fiabilidad y privacidad de las comunicaciones, preservar la privacidad y seguridad de las personas y, en general, garantizar el cumplimiento efectivo de la actividad laboral.

Los/as usuarios/as de los activos de información son responsables de no abusar en su utilización, de mantener el respeto a los derechos de los demás usuarios/as y de actuar conforme a las buenas prácticas profesionales.

Este documento será de aplicación a todos los usuarios/as, tanto empleados de RNB como externos, que tengan acceso a activos de información propiedad de la empresa.

Se entiende como activo de información cualquier información tratada en el transcurso de la actividad de RNB o cualquier elemento o recurso tecnológico relacionado o que intervenga en el uso de la misma. Entre los activos de información se incluyen: los sistemas de información, los equipos informáticos (PCs, portátiles, teléfonos móviles, servidores), infraestructuras de comunicaciones, conexión a redes internas o externas, terminales, software, hardware, servicios telemáticos, infraestructura de redes, accesos a Internet, documentos en formato físico y todos los recursos a los que tengan acceso los empleados para el cumplimiento de sus funciones en el ámbito laboral que tengan valor para la Organización.

Todos los activos de información deberán ser devueltos a RNB una vez haya finalizado la relación entre RNB y el usuario de los mismos.

Cualquier excepción a las obligaciones detalladas en la presente norma deberá ser notificada y aprobada por el departamento de Organización y Sistemas.

1.1. Posición de la empresa en cuanto al uso de herramientas y medios informáticos

Mediante el presente documento, la Empresa establece medidas de cumplimiento obligatorio para todos los empleados, los cuales quedan sujetos a esta política, así como a los principios morales y éticos en la utilización de los activos de información puestos a disposición del/la usuario/a para el desempeño de las actividades laborales.

El uso inapropiado, abusivo, o que escape a los hábitos tolerados de los activos de información será sancionado con la eliminación del acceso a los recursos, la aplicación de las sanciones disciplinarias derivadas por incumplimiento de los términos y condiciones que emanen de la relación laboral, además de las sanciones legales establecidas en la normativa vigente aplicable.

La empresa podrá realizar las investigaciones y controles que resulten necesarios tanto de los equipos como de las herramientas facilitadas al usuario/a por parte de la empresa, lo que incluye, entre otros, el correo electrónico empresarial, dispositivos o soportes informáticos tipo ordenadores portátiles, tabletas o smartphones, soluciones cloud, dentro del ámbito de potestades de control del empresario del Art.20.3 del Estatuto de los Trabajadores.

El control de estos medios se llevará a cabo sin dañar y sin atentar contra la dignidad o intimidad del/la usuario/a, dada cuenta del conocimiento que tiene éste del objeto y la existencia del presente control y fiscalización a la que los/las usuarios/as son sometidos.

Las finalidades de este control, a título enunciativo y no limitativo, son las siguientes:

- Protección del sistema y red informática, y de los equipos que lo conforman, a fin de proteger la integridad del Sistema y la Seguridad de la Información.
- Comprobación de la existencia o no del uso abusivo de los medios tecnológicos facilitados por la empresa para usos personales durante el horario laboral.
- Comprobación ante sospechas de un uso inadecuado, ilícito o en contra de esta política corporativa, la seguridad de la empresa o sus intereses de negocio.
- El alcance de estos procedimientos de control o inspección se notificarán a todos los/las usuarios/as de tal forma que quede constancia de los mismos.

El presente documento plantea una serie de normas de obligado cumplimiento que regulan el adecuado uso y disponibilidad de los activos de información, comprometiéndose la empresa a su difusión hacia todo el personal laboral, habilitando los canales necesarios para que los usuarios conozcan cualquier modificación o adición al respecto. Los/as usuarios/as que, de forma reiterada, deliberada o por negligencia los infrinjan, quedarán sujetos a las actuaciones técnicas o disciplinarias que se estimen oportunas.

1.2. Propiedad y especificaciones de los equipos informáticos

Se entiende por equipamiento informático cualquier dispositivo que permita el tratamiento de la información, bien mediante el almacenamiento de la misma o bien mediante la conexión con cualquiera de los sistemas de información corporativos de RNB.

Los equipos informáticos proporcionados al trabajador para el desempeño de sus funciones laborales (equipos de trabajo sobremesa, equipos de trabajo portátiles, smartphones, teléfonos móviles, tabletas, memorias USB, discos duros externos, cuentas de correo electrónico, certificados digitales, firmas electrónicas, etc.) son propiedad exclusiva de la empresa.

Los/as usuarios/as se comprometen a respetar la integridad de los recursos y equipos informáticos a los que tengan acceso para el cumplimiento de las tareas dentro del ámbito exclusivamente laboral, quedando estrictamente prohibido llevar a cabo o facilitar a cualquier tercero la comisión de cualquiera de los siguientes supuestos:

- El uso con fines personales del equipamiento informático facilitado por RNB.
- El tratamiento de la información corporativa o la conexión a los sistemas de información de RNB a través de equipamiento que no haya sido facilitado por RNB, o en su defecto, aprobado por el departamento de Organización y Sistemas.
- Alterar de forma total o parcial los componentes hardware, software y las configuraciones de seguridad de los equipos informáticos asignados al mismo usuario/a o a otros/as usuarios/as, sin la debida autorización.
- Instalar o utilizar aplicaciones informáticas (software) no proporcionadas u homologadas por el Departamento de Organización y Sistemas.
- Hacer modificaciones de privilegios o permisos sin autorización del departamento de Organización y Sistemas.
- Ocasionar daños físicos o lógicos, por mal uso o negligencia de los equipos informáticos, aplicaciones, herramientas informáticas y todo dispositivo o medio tecnológico.
- Desarrollar o usar intencional o accidentalmente programas maliciosos o accesos a recursos restringidos por el departamento de Organización y Sistemas.
- Dejar portátiles, smartphones o tabletas en lugares inseguros de forma que se pueda producir su pérdida o robo accidental. Se debe prestar especial atención en lugares públicos y en medios de transporte.

2. Equipos

El usuario que tenga algún dispositivo empresarial (PCs, tabletas, smartphones, etc....) debe cumplir con estas normas de uso:

- Asegurarse que tiene su dispositivo protegido con contraseña de acceso.
- Manipular el dispositivo de forma adecuada para que no reciba golpes, ni quede expuesto a condiciones que puedan dañarlo tales como temperaturas extremas, humedad, suciedad, etc.
- El usuario se compromete a hacer un uso profesional y no personal del dispositivo.
- Se deberán tomar medidas para evitar hurtos.
- La empresa podrá borrar los dispositivos en caso de pérdida.
- En caso de hurto o pérdida, el usuario debe ponerse en contacto con el departamento de Organización y Sistemas para intentar localizar, o para borrar directamente. La empresa utilizará las herramientas de búsqueda por geolocalización con el consentimiento del empleado.
- Los dispositivos empresariales se entregarán con las aplicaciones permitidas.
- No está permitida la instalación, por parte del usuario, de programas que pudieran afectar al rendimiento del dispositivo. Si el empleado precisara algún programa específico no contemplado actualmente en su dispositivo, debe comunicarlo a su responsable de inmediato.
- Cualquier mensaje de seguridad que requiera introducir el usuario y contraseña del tipo “Administrador” debe ser comunicado al responsable de sistemas.

Apps móviles

La empresa podrá restringir la instalación de apps móviles en los smartphones corporativos a través de herramientas de bloqueo para usuarios no administradores.

En cualquier caso y si no pudieran instalarse o no existieran herramientas de bloqueo de instalación de apps móviles para usuarios no administradores, queda prohibida la instalación de apps móviles no corporativas sin la supervisión del departamento de Organización y Sistemas.

Nota de uso interno.

3. Programas

Los ordenadores están preparados para desempeñar las tareas habituales del puesto de trabajo de cada empleado/a. Si el/la trabajador/a precisara algún programa específico no contemplado actualmente en su ordenador, debe comunicarlo a su responsable.

Cualquier mensaje de seguridad que requiera introducir el/la usuario/a y contraseña del tipo “Administrador” debe ser comunicado al departamento de Organización y Sistemas.

No está permitida, por tanto, la instalación de software sin autorización de la empresa, ni el uso de software de tipo portable (que no precisa ser instalado) pero que puede ser igualmente dañino para el sistema de información, entre otros:

- Software P2P.
- Software de descarga directa.
- Navegadores.
- Juegos.
- Software de imagen/audio/video.
- Software de descarga multimedia (radio, música o video en streaming).
- Software de redes, tráfico y comunicaciones.
- Software de ofimática.
- Software de desarrollo.

- Software de productividad.

4. Almacenamiento

La empresa pone a disposición del usuario una serie de medios de almacenamiento tales como las carpetas de red, Sharepoint, One Drive, otras soluciones cloud, etc. Estos medios deben ser utilizados para contenidos profesionales, no de tipo personal o que no tengan relación con su puesto de trabajo en la empresa.

Dado que estos medios de almacenamiento tienen sistemas de copias de respaldo, deben ser utilizados para el almacenamiento de la información corporativa en lugar del almacenamiento en discos locales de los equipos.

En caso de que sea necesario almacenar información corporativa en los discos locales de los equipos se comunicará la necesidad al departamento de Organización y Sistemas a fin de que se habiliten los mecanismos de respaldo oportunos.

El uso de dispositivos de almacenamiento extraíble (pendrive, discos duros externos) está restringido a dispositivos de origen conocido y confiable. En cualquier caso, se deberá evitar el uso de estos medios de almacenamiento, utilizando prioritariamente los mencionados anteriormente.

En caso de necesitar compartir información con algún proveedor de deberá evitar el uso de pen drive y usar otros medios como almacenamiento en la nube o sistemas de transferencia de ficheros por internet, siempre bajo el asesoramiento del departamento de Organización y Sistemas.

Servicios de cloud computing (computación en la nube)

La empresa pondrá a disposición de los usuarios una serie de servicios cloud para compartir ficheros e información. Se proporcionará una lista de los servicios soportados que será actualizada conforme sea necesario.

Los servicios no incluidos en esta lista, como en estos momentos Los servicios de cloud computing o computación en la nube, como Dropbox, Google Drive, Mega, Wuala o OneDrive, entre otros, quedan prohibidos salvo autorización expresa por parte de la empresa. Al tratarse de servicios gratuitos, actualmente son considerados servicios no seguros, no confiables y sin garantías de confidencialidad e integridad.

5. Dispositivos propios del usuario

La empresa permitirá el acceso al correo electrónico corporativo desde el Smartphone particular del usuario siempre que se cumplan estas condiciones:

- Exista una justificación profesional para la activación del servicio.
- Solicitar permiso al responsable directo.
- Comunicarlo al departamento de Organización y Sistemas.
- Cumplir las condiciones de seguridad:
 - El terminal debe estar protegido por contraseña.
 - En caso de pérdida del dispositivo, el usuario debe comunicarlo rápidamente a RNB.
 - El usuario debe permitir a RNB instalar las apps que se considere conveniente para proteger el terminal.
 - El usuario debe permitir a RNB la opción de borrar el terminal en caso de pérdida.

Como regla general, en caso de que el usuario pretenda utilizar para tareas profesionales cualquier tipo de dispositivo propio (p.e.: un portátil o una tableta, deberá comunicarlo a Organización y Sistemas que podrá aceptar o denegar la solicitud. En caso de que se considere necesario, el usuario deberá aceptar poner una serie de medidas de seguridad que pueden incluir la instalación de aplicaciones específicas de seguridad.

En caso de requerir el acceso a una red WiFi de la empresa, la compañía ofrece una red WiFi “de cortesía” específica para este tema.

6. Herramientas de comunicación

6.1. Uso del correo de empresa

El correo electrónico de empresa, las listas de distribución, los servicios de mensajería instantánea y demás servicios de comunicación electrónica, son herramientas de uso exclusivo en el ámbito laboral.

RNB se reserva el derecho de conceder o anular el derecho de acceso a estas herramientas conforme a los criterios que se estimen convenientes.

La utilización de los servicios de comunicación y difusión de la información quedará sujeta a las siguientes condiciones:

- Se utilizarán únicamente para uso profesional.
- Se prohíbe el envío de correos electrónicos con mensajes ofensivos, amenazantes, contenido ilícito o fraudulento.
- Queda prohibido la utilización del correo electrónico de empresa con fines lucrativos o comerciales, para uso recreativo o cualquier otro que no guarde relación con la actividad laboral.
- No está permitido el reenvío desde cuentas profesionales de información corporativa propia del trabajo a cuentas de correo electrónico personales.
- No está permitida la redirección del buzón de correo electrónico corporativo a cuentas de correo electrónico personales (no corporativas).
- No está permitida la inscripción a “newsletter”, grupos de noticias, o similares que no estén directamente relacionadas con la actividad profesional desarrollada por el/la usuario/a y que resulten de plena confianza.
- Las listas de distribución de correo solo podrán ser utilizadas para los fines propios de la empresa, y nunca con fines publicitarios, comerciales o de índole personal que no vayan relacionadas con actividades propias del desempeño laboral.
- El límite del tamaño de ficheros adjuntos en el correo será de 10 Mb. Si se precisa enviar ficheros de mayor tamaño se deberá consultar opciones con el departamento de Organización y sistemas.
- Como norma general no se deben enviar correos masivos y en caso de hacerlo, ha de ser bajo la autorización del responsable o director.
- El correo no es un sistema de almacenamiento, el usuario debe extraer los ficheros adjuntos y almacenarlos en un medio alternativo.
- No abrir ni ejecutar anexos de correos procedentes de direcciones desconocidas, sin asunto especificado o que no ofrezcan las suficientes garantías. En caso de detectar correos de dudosa procedencia, el usuario debe ponerse en contacto con el área de IT dentro del departamento de organización y sistemas para su análisis.

6.2. Uso del correo personal

El uso de cuentas de correo personales, basadas en acceso a web, tipo Gmail, Hotmail, Yahoo, etc. podrán ser utilizados con moderación, bajo las siguientes condiciones:

- El uso de cuentas de correo electrónico personales (no corporativas) está permitido únicamente con fines personales. No está permitido el envío o recepción de información corporativa desde cuentas de correo electrónico personales (no corporativas).

- El acceso deberá ser exclusivamente a aquellos correos que sean de plena confianza, y en ningún caso deben abrirse enlaces o descargarse ficheros adjuntos en el ordenador del/la usuario/a o de otros/as usuarios/as, aunque provengan de personas conocidas, para evitar así la intrusión de virus o códigos maliciosos.

6.3. Mensajería Instantánea

La empresa facilita al usuario cuyo puesto lo requiere las herramientas de mensajería instantánea necesarias. Estas herramientas pueden variar a lo largo del tiempo. En estos momentos las autorizadas son: Outlook (correo), Slack, Skype empresarial, Microsoft Teams:

- No se podrá instalar ningún software de servicio telemático o de mensajería instantánea sin autorización expresa del director del departamento o del Responsable de IT.
- No está permitido utilizar lenguaje obsceno, agresivo, ofensivo o discriminatorio en el envío de comunicaciones a través de servicios de mensajería instantánea.
- La utilización del servicio de mensajería instantánea será de uso exclusivo para el cumplimiento de las actividades relacionadas dentro del ámbito laboral de la propia empresa y nunca con el exterior.
- En caso de necesitar el uso de alguna herramienta distinta de las autorizadas en la actualidad deberá contactarse con el departamento de Organización y Sistemas.

6.4. Internet

En RNB el servicio de Internet tiene carácter profesional y no debe utilizarse con fines distintos. La navegación no podrá interferir en ningún caso en el desarrollo de las funciones profesionales del empleado o sus compañeros.

La empresa dispone de una solución para filtrar y monitorizar los accesos a los sitios que a consideración del Departamento de Organización y Sistemas sean inapropiados para la empresa, o innecesarios para la actividad laboral.

La navegación por sitios web, el envío de mensajes, registros, altas, relleno de formularios y cualquier otra actividad realizada vía Internet, serán completa responsabilidad del/la usuario/a emisor y en todo caso deberá asumir las consecuencias que emanen de su actuación.

Está estrictamente prohibido el acceso a páginas con contenidos ilícitos, material pornográfico, de contenido racista, sexual, o cualquier material que atente contra la dignidad y los principios morales.

Está estrictamente prohibido descargar ficheros de Internet de sitios en los que no se confíe ni instalar programas sin su correspondiente licencia.

No deberán modificarse las configuraciones de los navegadores (opciones de Internet) sin autorización del departamento de Organización y Sistemas.

Todo daño causado en los equipos informáticos, así como de los sistemas de información por la intrusión de virus informáticos o programas maliciosos que deriven de la utilización de programas de intercambio de archivos, será sancionado por la legislación vigente aplicable, así como por las sanciones impuestas por incumplimiento en la relación laboral.

6.5. Conexión a la red local corporativa

El acceso debe estar siempre protegido por usuario y contraseña. En el uso de las contraseñas se deben tener en cuenta las siguientes directrices:

- No comunicar las contraseñas a ningún otro usuario, independientemente de su rol en RNB. Las cuentas de usuario son personales e intransferibles, siendo los usuarios los responsables de las consecuencias que se puedan derivar del mal uso de su cuenta por la divulgación o pérdida de sus contraseñas.

- No mantener un registro de las contraseñas de acceso a los sistemas en papel ni en un sistema informático, a menos que se trate de un mecanismo seguro y que haya sido previamente aprobado por el departamento de Organización y Sistemas.
- Cambiar la contraseña de acuerdo con la política de las aplicaciones corporativas.
- No utilizar para el acceso a los sistemas de RNB las mismas contraseñas que utilizemos para acceder a otros servicios o sistemas de uso personal (e.g.: contraseñas de acceso a correo electrónico, redes sociales, etc.)
- Adoptar los siguientes criterios para la construcción de contraseñas seguras:
 - Fácil de recordar.
 - No basada en información que un tercero podría adivinar fácilmente (p.e.: nombres, fechas, etc.).
 - No contenga palabras que se encuentren en un diccionario.
 - Formada por diferentes juegos de caracteres (p.e.: mayúsculas, minúsculas, números, símbolos, etc.).
 - No compartida con contraseñas del ámbito personal.

En este sentido, los usuarios pueden ponerse en contacto con el Departamento de Organización y Sistemas para conocer técnicas de construcción de contraseñas seguras que sean fácilmente recordables.

En caso de detectar accesos no autorizados a su cuenta de usuario, los usuarios deberán ponerlo en conocimiento del Responsable del Sistema a la mayor brevedad posible.

Los accesos remotos por VPN u otros medios están permitidos sólo a usuarios con autorización explícita y siempre se realizarán desde dispositivos proporcionados por la empresa. Para utilizar un dispositivo particular en una conexión remota a la red de RNB se deberá tener autorización por parte del departamento de Organización y Sistemas.

En caso de necesidad de trabajar remotamente se debe solicitar a dicho departamento para que determine cuál es la mejor manera de conectar.

Adicionalmente, destacar que no está permitido establecer conexiones de red (por ejemplo conexiones VPN, red Tor, etc.) a redes externas a RNB a menos que se cuente con autorización por parte del departamento de Organización y Sistemas.

La red WiFi genérica para usuarios se llama, en el momento de generar este documento, RNB_USER (Ofimática). Esta red WiFi debe ser usada exclusivamente por personal de la empresa y utilizando dispositivos de la empresa o aprobados por el departamento de Organización y Sistemas, que requieran conexión a los aplicativos empresariales internos.

La empresa pondrá a disposición más redes WiFi, de cortesía *diferenciadas* para los siguientes usos:

- Para proporcionar servicio de acceso a Internet a equipos con información corporativa, pero que no necesitan acceder a las aplicaciones. Por ejemplo, un smartphone.
- Para proporcionar acceso a Internet a personal externo a la empresa

El departamento de Organización y Sistemas comunicará cualquier modificación de estas normas de caso de ser necesario.

6.6. Conexiones a redes externas

Las conexiones a redes de terceros, generalmente por medio de WiFi, puede ser utilizada fácilmente para acceder a nuestra información o para “leer” los datos que intercambiamos.

Los usuarios que se desplacen por motivos de trabajo y necesiten conectarse a internet con los dispositivos proporcionados por la empresa, lo harán utilizando la red de datos del operador de telefonía.

La conexión de dispositivos empresariales a redes proporcionadas por terceros (hoteles, aeropuertos, hotspots, etc.) debe realizarse sólo en ocasiones de clara necesidad por razones profesionales, como por ejemplo:

- Poca cobertura móvil (bajo rendimiento conexión de datos).
- Conexiones remotas a la empresa prolongadas (varias horas).
- Visualización de contenidos multimedia.

Consideraciones:

- Los empleados que necesiten conectarse a redes WiFi ofrecidas por hoteles, aeropuertos y otros, deberán asegurarse que es una red WiFi protegida (nos generan una contraseña para nosotros).
- En caso de necesitar conectarse a una WiFi con poco nivel de protección asegurarse que las páginas web visitadas esta cifradas (https://).

7. Líneas y bonos de datos

Las líneas de datos que proporciona la empresa, por ejemplo, los datos asociados a un teléfono, deben ser usados de manera responsable.

La empresa realiza un seguimiento de las facturas telefónicas de las líneas móviles proporcionadas por el proveedor de servicios de comunicaciones.

En caso de tener que realizar un viaje al extranjero se deberá contactar con el departamento de Organización y Sistemas para revisar la conveniencia de contratar bonos para roaming.

8. Programas y dispositivos de control y monitorización

La empresa dispone de herramientas de control automatizadas para analizar y detectar los usos y comportamientos indebidos o ilícitos en la red y los sistemas que dependen de ellas (correo electrónico, equipos de la red de trabajo, navegación por Internet, etc.), no implicando dicho control violación a la privacidad o a la intimidad de los/as usuarios/as.

Por cuestiones de seguridad toda la información que circula por la red, así como por el correo electrónico de las cuentas administradas por la empresa, podrá ser monitoreada y sujeta a controles y reportes sobre su uso.

9. Manejo de documentación en formato físico

La protección de la información de RNB contempla no sólo la información en soporte electrónico, sino en general, en cualquier tipo de soporte. Así, en el uso de la documentación impresa, se debe cumplir con las siguientes directrices:

- En caso de imprimir información confidencial en impresoras que no se encuentren situadas en el área de visión del usuario, utilizar los mecanismos de seguridad de dichos dispositivos que se encuentren disponibles.
- No abandonar documentos en fotocopiadoras, impresoras o faxes. En el caso de encontrar documentación abandonada en dichos dispositivos, proceder a su destrucción de forma segura.
- Al finalizar una reunión, verificar que en la sala no quede documentación confidencial (papeles de trabajo, copias impresas de presentaciones, etc.).

- Al finalizar la jornada laboral, no dejar documentación encima de mesas o estanterías. Toda la documentación confidencial debe ser almacenada en los archivos habilitados al efecto.
- Evitar generar y acumular de manera innecesaria documentación impresa. En la medida que sea posible, tratar la información en formato digital y, si es necesaria imprimirla, destruirla de forma segura una vez haya dejado de ser útil.
- Utilizar las destructoras de papel para la destrucción segura de documentación. No tirar directamente a la papelera información impresa que contenga información confidencial.

10. Consecuencias derivadas del mal uso de los ACTIVOS DE INFORMACIÓN

Los/as usuarios/as se comprometen a colaborar con el departamento de sistemas para llevar a cabo toda investigación que tenga por objeto encontrar las posibles causas derivadas del mal uso de los activos de información.

Toda incidencia detectada en los equipos informáticos, así como en los sistemas de información, podrán derivar en la suspensión o restricción del acceso o uso de los servicios al usuario/a, así como la aplicación de las medidas que la Dirección considere oportunas al incumplimiento de lo establecido en el presente documento.

Del mismo modo, el incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado se sancionará conforme al régimen disciplinario interno, el Estatuto del Trabajador y/o el régimen sancionador asociado al convenio colectivo aplicable.

10.1. Implicaciones legales

Determinados comportamientos relacionados con el uso de los recursos tecnológicos suponen la comisión de actos delictivos. RNB no aprueba ni tolera este tipo de comportamientos y así está reflejado en el Código de Conducta de la compañía. A continuación, se detallan los más importantes:

Descubrimiento y revelación de secretos:

- Acceder o facilitar a otro el acceso a un sistema de información, vulnerando las medidas de seguridad establecidas y sin estar autorizado.
- Sin estar autorizado, apoderarse, utilizar o modificar, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos.
- Utilizar medios técnicos, sin estar autorizado, para interceptar transmisiones no públicas de datos informáticos o para descubrir los secretos o vulnerar la intimidad de otro.
- Apoderarse de mensajes de correo electrónico u otras comunicaciones para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento.
- Difundir, revelar o ceder a 3º datos o hechos descubiertos o imágenes captadas, en perjuicio de 3º y sin autorización, datos de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, o acceder por cualquier medio a esa misma información y alterarla o utilizarla en perjuicio del titular de los mismos.
- Producir, adquirir, importar o facilitar a terceros un programa informático concebido o adaptado para cometer delitos relacionados con el descubrimiento y revelación de secretos o facilitar a terceros una contraseña o código de acceso que permitan el acceso a un sistema de información.

10.2. Contra la propiedad intelectual e industrial, el mercado y los consumidores

- Alterar o duplicar el número identificativo de equipos de telecomunicaciones, o comercializar equipos que hayan sufrido alteración fraudulenta, con ánimo de lucro. Utilización o almacenamiento o exportación de cualquier forma de una obra literaria, artística o científica o software.

- Apoderarse de datos, documentos escritos o electrónicos, soportes informáticos, u otros, para descubrir un secreto de empresa.
- Utilizar los equipos o programas que permitan el acceso no autorizado a servicios de acceso condicional o equipos de telecomunicación.

10.3. Daños informáticos

- Dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos.
- Producir, adquirir, importar o facilitar a terceros, con la intención de facilitar la comisión de este tipo de delitos, un programa informático, concebido o adaptado para ello o una contraseña de ordenador o código informáticos.
- Producir, adquirir, importar o facilitar a terceros un programa informático concebido o adaptado para cometer delitos relacionados con el descubrimiento y revelación de secretos.
- Producir, adquirir, importar o facilitar a terceros una contraseña o código de acceso que permitan el acceso a un sistema de información.

Cualquier empleado que sospeche de la comisión de alguno de estos delitos debe denunciarlo ante el comité de Cumplimiento (ver código conducta).

La comisión de estas faltas, además de suponer delitos castigados por el Código Penal, están sujetas a la aplicación del régimen disciplinario vigente, dando lugar a sanciones laborales.