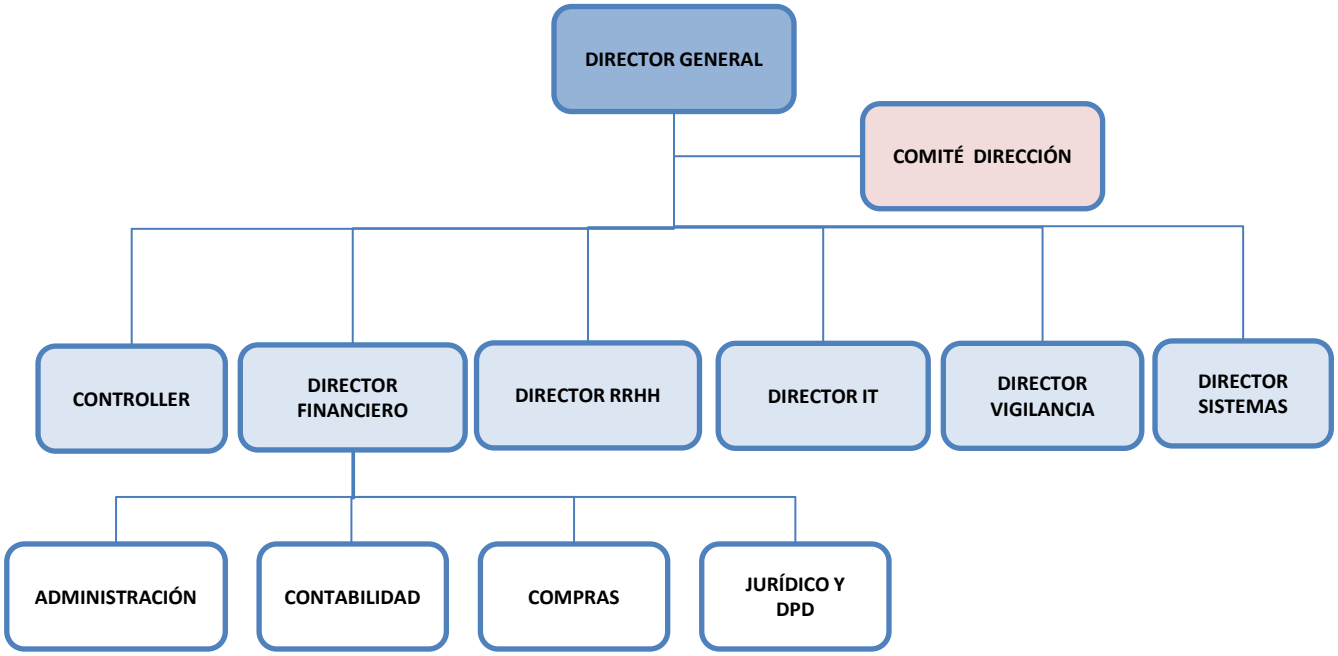
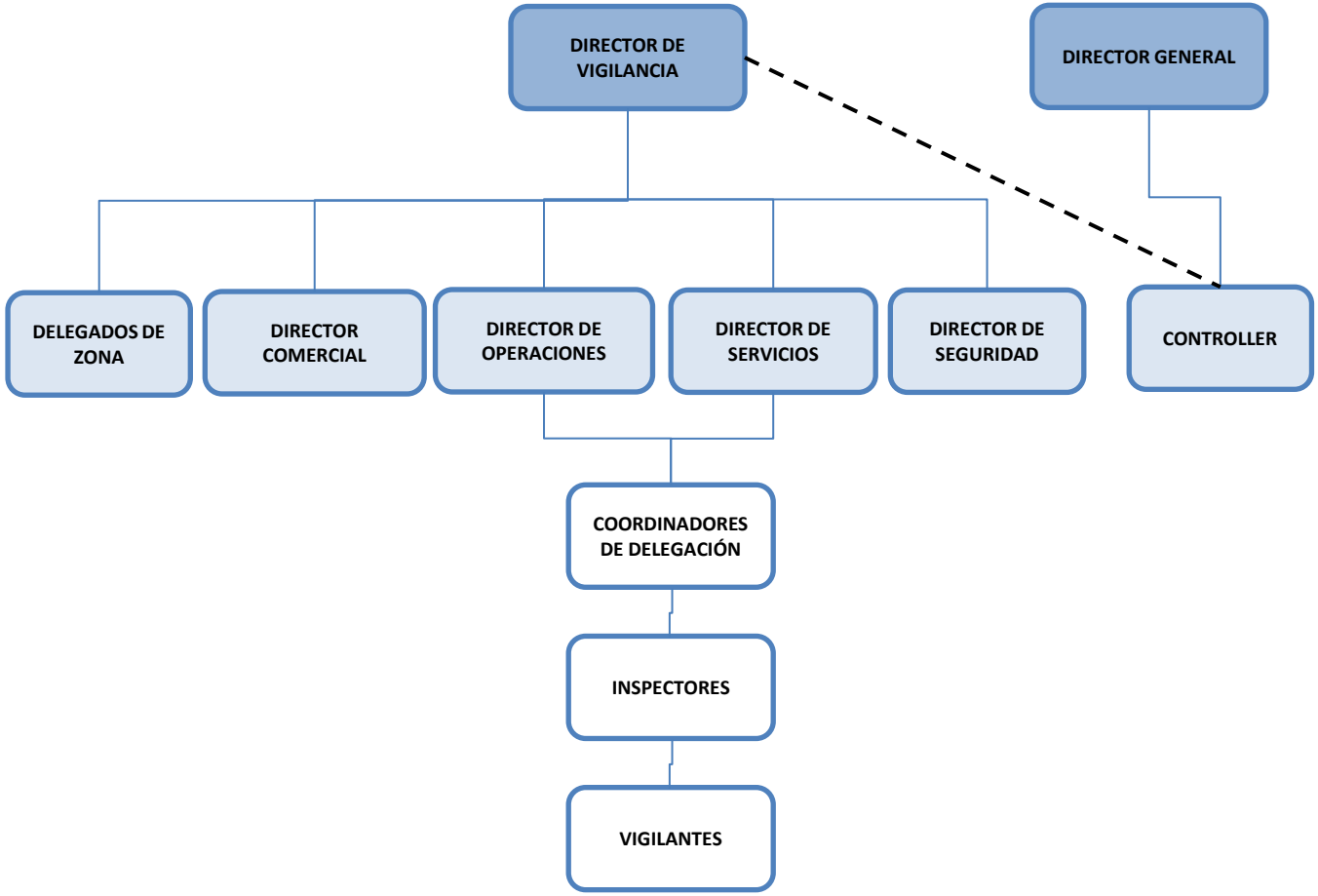
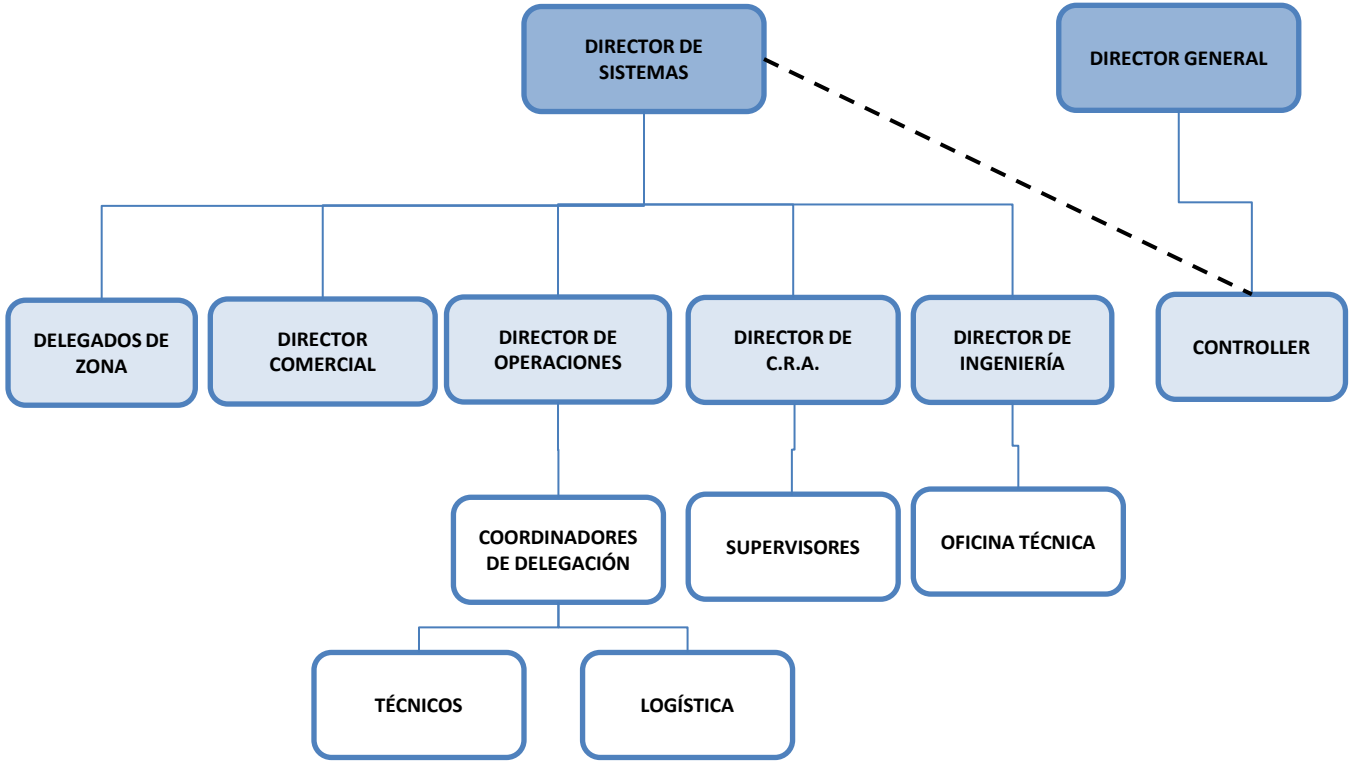
Organigrama de Estructura Corporativa



Organigrama de Unidad de Negocio de Vigilancia



Organigrama de Unidad de Negocio de Sistemas



Código de conducta de PYCSECA SEGURIDAD, S.A.
(Código Ético)

Introducción

El código de conducta ética es nuestra guía de conducta adecuada, junto con las normas y procedimientos de trabajo establecidos, para garantizar lo correcto y que en su consecuencia lógica no se produzca ningún tipo de infracción penal o administrativa grave o muy grave, en la empresa.

El Código constituye una guía para todos los empleados de PYCSECA SEGURIDAD S.A., en adelante PYCSECA, en su desempeño profesional en relación con su trabajo cotidiano, los recursos utilizados y el entorno empresarial en el que se desarrolla. En este se ofrecen las directrices que clarifican los principios básicos de toda gestión y las relaciones interpersonales con compañeros, colaboradores, jefes, proveedores, clientes, accionistas y en general cualquier persona con interés directo o indirecto en la actividad que desarrolla la compañía. Nuestras actuaciones se basan en el respeto de nuestros valores corporativos, y los empleados acomodaremos la actuación a principios de comportamiento respetuosos con la ética empresarial y con la profesionalidad, con el objetivo de que sea un referente en estos términos y sea así reconocida.

El presente Código de Conducta es especialmente relevante, por cuanto, PYCSECA SEGURIDAD, S.A. realiza actividades diversas en el ámbito de la seguridad privada, de acuerdo con la Ley 5/2014, de 4 de abril, de Seguridad Privada, que establece el marco en el que nuestra empresa debe operar, para la más eficiente coordinación de esos servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad, de los que son complementarios, como así dispone en su artículo 1.2). Servicios, para los que dispone de las licencias administrativas correspondientes, incluidas en sus artículos 5 y 6: "Instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad, y de incendios"; "Explotación de centrales para la conexión, recepción y verificación de las señales de alarma"; así como, "Vigilancia y protección de bienes y personas, incluido, "el acompañamiento, defensa y protección de personas físicas determinadas". **PYCSECA SEGURIDAD, S.A**. nace en 1985, con una clara vocación de excelencia en la prestación de servicios de seguridad y dada su especial vinculación con el Ministerio del Interior en el ejercicio de sus actividades, presta especial atención a la legislación y normativa específica del sector, del entorno local, ambiental, social y laboral, dentro de nuestras directrices estratégicas prioritarias.

La actividad de PYCSECA SEGURIDAD, S.A., al ser considerada legalmente como sector económico de regulación específica, nos exige un plus de responsabilidad en el cumplimiento normativo, así como de los Valores y Principios de nuestro Código Ético, contribuyendo positivamente al alcance de los objetivos marcados, incluidos los relativos a la cuenta de resultados, a la sostenibilidad en el tiempo y a su reputación, y que nos

previene sobre los riesgos de incumplimiento en relación con las leyes aplicables, las regulaciones, los códigos de conducta y los estándares de buenas prácticas, exigidos por nuestros clientes, especialmente, por las administraciones públicas, cuya contratación, constituye uno de los pilares importantes de nuestra actividad mercantil, para lo que disponemos de una plantilla superior a los mil trabajadores/as perfectamente formados/as y cualificados/as, que nos permiten proporcionar servicios con los máximos estándares de calidad y eficiencia.

Ámbito de aplicación

El presente Código va dirigido a todos los empleados de PYCSECA SEGURIDAD S.A., con independencia de la modalidad contractual que determine su relación laboral, su especialidad en cuanto a la actividad, posición que ocupen o del lugar en el que desempeñen su trabajo. La promoción de una cultura ética basada en valores donde todos conocen sus responsabilidades y roles involucrando a toda la organización es asegurar la viabilidad de la empresa al más largo plazo. Hay obligación de los relacionados con la empresa de dar a conocer a sus principales proveedores la existencia del presente Código, que estará disponible para su consulta en la página web de la compañía, https://www.pycseca.com/

Valores

Nuestros valores representan nuestra identidad como colectivo. Somos diferentes porque las personas que trabajamos en PYCSECA SEGURIDAD, S.A. hacemos de esta empresa un proyecto único y diferenciador. Somos rápidos, sabemos escuchar, buscamos la innovación, somos serviciales y trabajamos en equipo de forma rigurosa y transparente.

- Tomamos decisiones rápidas y actuamos con celeridad y dinamismo.
- Focalizamos de manera ágil la solución a un problema proponiendo alternativas realistas, de calidad y viables.
- Nos adaptamos rápidamente a los cambios y demandas del entorno profesional.
- Escuchamos con atención a nuestro cliente interno y externo para conocer con exactitud sus necesidades y proponerle soluciones adecuadas.
- Tenemos los ojos y los oídos del cliente en cualquier operación que desarrollemos, preguntándonos continuamente por su satisfacción.
- Escuchamos activamente, con actitud abierta y respeto a la opinión de todas las partes implicadas en una situación.
- Buscamos activamente las ocasiones para mejorar los productos y servicios y crear nuevas oportunidades de negocio.
- Aprovechamos las oportunidades y problemas para dar soluciones novedosas.
- Actualizamos constantemente nuestros conocimientos tecnológicos para conseguir ser pioneros en innovación para lo cual la formación es uno de nuestros

ejes estratégicos más relevantes y evaluamos anualmente las necesidades y establecemos un plan de formación que actualiza y desarrolla nuestros conocimientos y competencias, lo que significa que todos los miembros de la organización, sean internos, externos, plantilla, colaboradores, proveedores, clientes, socios o cualquiera que tenga relación con ésta gozará de ese gran activo que es la formación continuada y pensada para el crecimiento de la empresa y las personas que la conforman.

● Conocemos las necesidades y expectativas de nuestros clientes para desarrollar y aplicar soluciones que aumenten su satisfacción.

● Atendemos a nuestros clientes de manera eficiente manteniendo en todo momento un comportamiento ágil y resolutivo que potencie la credibilidad y reputación de la compañía y sus profesionales.

● Atendemos a los clientes con el máximo interés y nos esforzamos por interpretar sus demandas, siendo esta la característica prioritaria de la actitud de todos nuestros profesionales.

● Sabemos trabajar en equipos multidisciplinares, de distintas unidades, empresas y países generando un clima de confianza y respeto mutuo.

● Cooperamos con el resto de la organización asumiendo compromisos encaminados a la consecución de objetivos comunes.

● Orientamos nuestros esfuerzos hacia un mismo resultado, teniendo en cuenta el aporte de cada uno de los miembros por pequeño que parezca. Respetamos las diferencias, las opiniones y la diversidad.

Somos **respetuosos con el medio ambiente y las políticas de sostenibilidad**, por lo cual siendo conscientes que nuestros procesos, actividades y servicios pueden causar cierto impacto sobre éste, con objeto de garantizar un estricto cumplimiento de la normativa medio-ambiental, la minización de consumos, la correcta gestión residuos, y la disminución de emisiones, nuestra empresa ha implantado un sistema de gestión ambiental, de acuerdo con la norma **UNE-EN ISO 14.001**

El comportamiento ético que rige esta sociedad se basa en los siguientes Principios:

Buena fe

- Ajustamos en todo momento nuestra actuación a los principios de lealtad y buena fe con la empresa, con superiores, compañeros y colaboradores con los que nos relacionamos.

- Enfatizamos el afán de logro y el espíritu de superación. La preocupación por alcanzar los objetivos marcados debe ser constante y continuada. Potenciamos actitudes optimistas *versus* pesimistas. Supeditamos los objetivos personales a los generales de la Compañía.

- Velamos para que no exista conflicto entre ambos, y actuamos dando prioridad a los intereses de la compañía respecto de intereses personales o de terceros. No nos comprometemos en intereses exteriores que desvíen nuestro tiempo y atención de las

responsabilidades con nuestra empresa o requieran trabajo durante el tiempo dedicado a nuestros clientes. Para mejorar la seguridad y salud de los/las trabajadores/as nuestra empresa ha implantado el sistema de gestión de la prevención de riesgos laborales según la Norma UNE-EN ISO 45001

Honestidad

Todos los empleados de PYCSECA SEGURIDAD S.A. nos comprometemos a declarar cualquier relación personal o profesional que pudiera condicionar nuestro comportamiento como empleados de la Compañía. Además, como empleados de PYCSECA SEGURIDAD S.A. no aceptamos compensaciones o ventajas indebidas. Inculcamos la honestidad y ética profesional en las relaciones comerciales y profesionales habituales en el desempeño de nuestro trabajo, tanto en el sector privado como en nuestras relaciones con las Administraciones Públicas. No ofrecemos regalos, ni prometemos un trato de favor indebido a terceros, ya sean de carácter público o privado, con el fin de obtener una ventaja. Promovemos la confianza para declarar los regalos o ventajas que podamos obtener de terceros y los ponemos a disposición de la compañía. Cualquier relación personal o profesional que afecte a los intereses de la Compañía es comunicada al jefe inmediato. No permitimos relaciones personales ni familiares en dependencia directa ni dentro de la misma unidad organizativa.

Evitamos conductas contrarias a la libre competencia, o que supongan un acto de competencia desleal. En campañas publicitarias ofrecemos la información de forma clara y veraz.

Respeto

Todos y cada uno de nosotros somos responsables de generar un ambiente de cordialidad y amabilidad en nuestro entorno. Potenciamos el respeto y confianza entre las personas. Apreciamos la diversidad en opiniones, formación y cultura como fuente de conocimiento y ventaja competitiva. Cuidamos el lenguaje que utilizamos al hablar de terceros y propiciamos la no existencia de pautas y comentarios difamatorios dentro y fuera de la organización. Promovemos el respeto a la igualdad real de oportunidades entre hombres y mujeres, evitando cualquier escenario de discriminación directa o indirecta. Ninguna persona empleada en PYCSECA SEGURIDAD, S.A. es discriminada en el ámbito profesional por raza, discapacidad física, religión, edad, nacionalidad, orientación sexual, sexo, opinión política u origen social. Mantenemos un entorno de trabajo libre de toda discriminación y de cualquier conducta que implique un acoso de carácter personal, no admitiendo ninguna forma de acoso o abuso físico, sexual, psicológico o verbal. Respetamos el medio ambiente y colaboramos con el desarrollo sostenible de la sociedad, y siendo consciente de que nuestros procesos, proyectos y actividades repercuten en las comunidades en las que operamos, contratamos del personal en la ubicación del centro de trabajo para tratar de garantizar la mejora económica de la comunidad; realizamos nuestra actividad de forma sostenible garantizando la prevención de la contaminación y la mejora del medio ambiente y realizamos inversiones en la comunidad, tales como donaciones a ONG’s, proyectos de colaboración con entidades sociales, etc.

Confidencialidad

Nos abstenemos de proporcionar, interna o externamente, datos confidenciales sobre las personas y/o las actividades desarrolladas en la Compañía. Facilitamos, sin embargo, los datos que sean necesarios para que otros empleados de PYCSECA SEGURIDAD S.A. realicen correctamente su función, con estricto respeto a este deber de confidencialidad. Evitamos conductas contrarias a la libre competencia, o que supongan un acto de competencia desleal. En campañas publicitarias ofrecemos la información de forma clara y veraz. Principios de comportamiento ético, respeto, confidencialidad y uso de la información. Cumplimos con la normativa de protección de datos de carácter personal en relación a los que tengamos acceso debido a nuestro puesto de trabajo. Los empleados de PYCSECA SEGURIDAD S.A. nos caracterizamos por una marcada actitud proactiva en el trato de la información confidencial. La información es propiedad de la Compañía y deberá compartirse siempre que sea beneficioso y necesario para esta.

En nuestra conducta:

- **Facilitamos a los responsables información veraz**, necesaria, completa y puntual acerca de la marcha de las actividades de nuestra área; y a nuestros compañeros, aquella que sea necesaria para el adecuado desempeño de sus funciones.
- **Mantenemos el secreto profesional de los datos**, informes, cuentas, balances, planes estratégicos y demás actividades de PYCSECA SEGURIDAD, S.A. y sus personas, que no sean de carácter público, y cuya publicidad pueda afectar a los intereses de la compañía. No facilitaremos información de estos, salvo cuando nos hallemos expresamente autorizados para ello.
- **Obtenemos la información de terceros de forma ética y legítima**, rechazando toda aquella información obtenida de forma improcedente o que suponga una violación del secreto de empresa o de la confidencialidad de esta.
- En el supuesto de tener dudas acerca del tratamiento adecuado de la información, solicitamos la valoración de nuestro responsable acerca de la correcta catalogación de esta.
- **No podremos usar para fines propios, de terceros, ni para obtener beneficio o lucro, los programas, sistemas informáticos**, manuales, vídeos, cursos, estudios, informes, etc., creados, desarrollados o perfeccionados en PYCSECA SEGURIDAD S.A. dado que la empresa conserva en todo momento la propiedad intelectual de estos.
- En general **mantenemos la más estricta confidencialidad** en la utilización del conocimiento interno fuera del ámbito de la empresa, preservando nuestro saber hacer.
- **Únicamente utilizaremos los sistemas informáticos,** *software,* material, informes, etc. de los cuales PYCSECA SEGURIDAD S.A. haya adquirido la licencia correspondiente, respetando en todo momento la propiedad intelectual e industrial de estos.
- **La utilización de equipos informáticos está sometido a la política de seguridad** de la información de PYCSECA SEGURIDAD S.A. con el objetivo de evitar daños a terceros y/o a la propia empresa.

- No utilizaremos los accesos a los sistemas para actuar de forma fraudulenta o en beneficio propio.

Decálogo de preguntas antes de tomar una decisión

Plantearse estas preguntas ayudará a decidir sobre el comportamiento que debe seguirse.

1. ¿Va contra las normas de trabajo?

2. ¿Parece ser lo correcto?

3. ¿Es legal?

4. ¿Tendrá un efecto negativo sobre mi reputación o sobre la de la empresa?

5. ¿Quién más puede verse afectado por esto (¿otras personas de la entidad, clientes, proveedores?

6. ¿Me sentiría avergonzado si los demás supieran que he resuelto actuar de esta manera?

7. ¿Existe una solución alternativa que no plantee un conflicto ético?

8. ¿Cómo me vería si fuese publicado en los periódicos?

9. ¿Qué pensaría una persona razonable?

10. ¿Podré dormir tranquilo?

Principios de comportamiento profesional

Pasión por el cliente

Todos los empleados aspiramos a ofrecer a nuestros clientes un producto de la máxima calidad y a tener un nivel de atención excelente. La excelencia y la calidad de servicio son guías constantes de actuación, promoviendo una sana inquietud de mejora continua.

Los recursos que provee la empresa buscan el fomento de la innovación y el desarrollo de los servicios a los clientes, con criterio de rentabilidad. Todos, con independencia del área funcional en la que trabajemos, estamos comprometidos con la promoción de actitudes honestas y la satisfacción de nuestro cliente.

Gestión eficiente

Los empleados de PYCSECA SEGURIDAD S.A. trabajamos de forma eficiente durante la jornada laboral, rentabilizando el tiempo y recursos que la empresa pone a nuestra

disposición de manera rigurosa y racional. Todos prestamos la dedicación que exija el desempeño de nuestras funciones, aspirando a la consecución de los resultados de la forma óptima y productiva posible. **La Compañía pone a nuestra disposición todos los recursos necesarios para realizar el trabajo y mejorar el rendimiento a través de una optimización del tiempo y alcance a la información necesaria para cumplir con nuestras responsabilidades**. Por ello deberemos hacer un uso adecuado y razonable según las necesidades profesionales de cada uno. No participamos en actividades personales durante el horario laboral que interfieran o le impidan cumplir con las responsabilidades laborales.

Utilizamos el correo electrónico, el acceso a internet y, en general, los sistemas informáticos de la Compañía para fines y propósitos exclusivamente laborales, quedando expresamente prohibida su utilización para uso personal. Autorizamos expresamente a la Compañía a controlar el uso de estos. El uso inaceptable de los sistemas de comunicaciones de la empresa incluye procesar, enviar, recuperar, acceder, visualizar, almacenar, imprimir o de cualquier otro modo difundir materiales e información que sea de carácter fraudulento, acosador, amenazante, ilegal, racial, sexista, obsceno, intimidante, difamatorio o de cualquier otro modo incompatible con una conducta profesional. **En materia de seguridad en el trabajo y salud profesional, cumpliremos con las medidas preventivas, utilizando los medios de protección individuales y colectivos que la empresa tiene a disposición**. En el caso de disponer de un equipo a su cargo, los responsables se asegurarán de que los miembros de dicho equipo realicen su actividad en condiciones de seguridad.

Actitud de equipo

Los empleados de la compañía favoreceremos el trabajo en equipo y reconocemos la aportación de otros en la obtención de resultados comunes. Como miembros de un equipo contribuimos con igual compromiso tanto dentro como fuera de nuestra área. La actitud de trabajo en equipo predomina y destaca sobre cualquier actuación en el nivel individual. **Un individuo sobresaliente lo es también por su capacidad de trabajo en equipo, y por tanto no existe conflicto entre esta conducta y la de ser excelente individualmente.** No prima el interés individual sobre el interés del equipo. Evitamos las actitudes pasivas: no nos dejamos llevar y no nos quedamos al margen.

Fomentamos el entusiasmo y compromiso con el grupo y por tanto con la organización. Actuamos con espíritu de cooperación poniendo a disposición de las demás áreas y departamentos de la entidad los conocimientos y recursos que faciliten la consecución de los objetivos de la empresa.

Cuidar la reputación

Consideramos la imagen y la reputación de la compañía como uno de sus activos más valiosos para mantener la confianza de sus clientes. Vigilamos el respeto y uso correcto de la imagen y reputación corporativa, por parte de todas las personas en el entorno de la compañía. La imagen de marca se plasma visualmente con nuestro logo de compañía,

del cual existen unas normas de utilización que protegen su uso y que debemos respetar. Somos especialmente cuidadosos en cualquier intervención pública, debiendo contar con la autorización necesaria para intervenir ante los medios de comunicación, participar en jornadas o seminarios profesionales y en cualquier medio de difusión pública, siempre que aparezcan como empleados de PYCSECA SEGURIDAD S.A.

Todos somos parte de la imagen corporativa y por tanto asumimos una conducta ética y responsable que permite preservar la imagen y la reputación de la compañía. En ningún momento actuaremos poniendo de manifiesto comportamientos que puedan dañar la imagen. Nuestra forma de comunicarnos, conducirnos y nuestra propia imagen personal estará en consonancia con el contexto profesional en el que nos desenvolvemos.

Desarrollo profesional

Nuestro crecimiento profesional y el de nuestros equipos es nuestra clave para ser competitivos. Los empleados somos responsables de nuestro crecimiento profesional, y en consecuencia es nuestro deber estar permanentemente actualizados con los conocimientos y técnicas precisas para el eficiente desempeño de nuestro trabajo. Las personas con equipos a cargo han de prestar atención a la motivación y desarrollo profesional de sus colaboradores, comprometiéndose a propiciarles oportunidades de desarrollo con base en el mérito y en su aportación profesional. Para ello, fomentarán su aprendizaje continuo, reconocerán sus esfuerzos de forma específica y valorarán objetivamente sus logros, trazando los planes de acción y acompañamiento precisos para su desarrollo.

PYCSECA SEGURIDAD, S.A. valora el compromiso de colaboración con sus proveedores para fomentar el conocimiento y la mejora de los procesos en materia de responsabilidad social, y que se materializa a través propuestas concretas, como, por ejemplo, jornadas formativas y convenios de colaboración específicos.

Los Valores empresariales de PYCSECA SEGURIDAD, S.A. se fundamentan en los siguientes principios:

- **Excelencia**. La calidad llevada al máximo, eso es la excelencia. Si nos exigimos lo mejor, podremos dar lo mejor. Seguimos, por ello, los protocolos de la Norma UNE-EN ISO 9001, que garantiza que nuestros servicios se desarrollan de acuerdo a altos estándares de calidad, de cuya Certificación disponemos

- **Adaptabilidad**. Capacidad para adaptarnos a los requisitos de nuestros clientes y dar soluciones competitivas a sus necesidades y expectativas.

- **Lealtad**. Si nos mostramos leales y fieles con nuestro equipo y nuestros clientes, ellos nos devolverán esa fidelidad. Esta reciprocidad es fundamental en nuestro modelo de negocio.

- **Responsabilidad**. Nuestra empresa no se centra únicamente en los beneficios económicos, y siendo conscientes de nuestra responsabilidad social como parte de la sociedad, tratamos siempre que nuestra conducta forme parte de la colaboración activa con el interés público, compatibilizando nuestra actividad mercantil con el cumplimiento normativo y en un entorno ambiental adecuado, en cuya mejora debemos colaborar todos.

- **Aprendizaje**. Somos capaces de aprender diariamente, formarnos y prepararnos para garantizar la innovación, la adaptación al cambio y la mejora continua en la gestión empresarial y los servicios que ofrecemos a nuestros clientes.

Compromiso del órgano de gobierno

El órgano de administración de PYCSECA SEGURIDAD, S.A., sobre la base de lo establecido en el artículo 1.2, de la Ley 5/2014, de 4 de abril, de Seguridad Privada que establece el marco para la más eficiente coordinación de los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad, de los que son complementarios, **tiene la responsabilidad indelegable del diseño e implantación de programas de cumplimiento normativo, ante la diversidad de normas específicas, regulatorias de sus actividades, así como de la supervisión periódica de su aplicación y efectividad, con objeto identificar cuáles son las posibles infracciones o conductas irregulares y los riesgos de su comisión, tanto los propios de las actividades concretas a las que se dedica, como los comunes, es decir, cualquier posible ilícito penal o administrativo, para que una vez identificados, se analicen las probabilidades de ocurrencia, su impacto y se priorice su mitigación**. La organización cuenta con las políticas de actuación necesarias para prevenir y mitigar los riesgos identificados. Son protocolos que deben seguirse en cada proceso, tanto por los empleados como por los directivos de la empresa, responsables de su ejecución, para los que se imparten cursos de formación periódica.

La empresa tiene definidas las acciones a emprender en caso de posible comisión de un ilícito o riesgo de que se cometa, o incumplimiento del programa de cumplimiento, para la defensa de sus intereses, teniendo en cuenta la normativa legal y su situación procesal.

Sistema interno de información

(CANAL INTERNO DE INFORMACIÓN)

PYCSECA SEGURIDAD, S.A. ha implantado su propio Sistema Interno de Información, dentro del plazo señalado por la Ley, 12 de junio de 2023, **integrado por un Canal Interno de Información, un RESPONSABLE y Procedimiento de gestión de las informaciones**, de conformidad con los arts. 5,6 y 7 de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. El "Canal Interno de Información" permite que los

trabajadores, directivos, empleados, y otras personas, relacionadas exhaustivamente en el artículo 3 de la Ley 2/23 (Ámbito personal de aplicación), puedan poner en conocimiento del RESPONSABLE de la gestión del canal cualquier irregularidad que detecten, conforme a la normativa vigente y conforme al Código Ético de la Entidad, que es accesible a través de la web de la empresa, https://www.pycseca.com/ que incluye una etiqueta identificativa, CANAL INTERNO DE INFORMACION, en una sección separada y fácilmente identificable de la barra principal, que utiliza un programa de gestión, bajo licencia de uso de la empresa Aranzadi La Ley, que cumple con la regulación prevista en esta Ley.

Todas las informaciones recibidas se analizarán de forma independiente y confidencial. Se garantizará, en todos los casos, la máxima confidencialidad y, en su caso, anonimato, en los procesos de investigación de las informaciones recibidas, a los efectos de proteger la identidad del informante y de las personas afectadas y de su reputación. Se informará solo a las personas estrictamente necesarias en el proceso. Cuando proceda, se notificará a la autoridad competente de aquellos hechos que puedan ser constitutivos de ilícito penal, administrativo o laboral.

Se garantiza, igualmente, la ausencia de represalias de cualquier tipo contra el informante. Si se confirmase que las ha sufrido, los autores de las mismas serán objeto de investigación y, en su caso, de sanción. Asimismo, cualquier información dolosamente falsa, maliciosa o abusiva podrá dar lugar a acciones proporcionadas en contra del informante.

Entrada en vigor del código de conducta, interpretación y seguimiento.

Por ACUERDO del Administrador Único de la Entidad, fue aprobado el nuevo Código de Conducta Ética de PYCSECA SEGURIDAD, S.A. el día 27 de junio de 2023. El presente ha sido sometido a la consideración de la Representación legal de los trabajadores en fecha 29 de junio de 2023 para su próxima entrada en vigor e implantación mediante publicación en la Web de la empresa.

El Código se comunicará a todos los miembros de la Entidad. Este Código deroga el vigente hasta ahora en todo aquello que se le oponga, y estará vigente en tanto no se apruebe su modificación o anulación, que será debidamente comunicada.

Cada uno de nosotros asumimos la tarea de revisar y seguir este Código, y cumplimos todas las leyes aplicables, políticas y directrices. Este Código intenta contemplar muchas de las situaciones a las que nos enfrentamos en el día a día, pero no puede considerar todas las circunstancias.

Procura obtener ayuda de:

- Tu superior jerárquico
- Tu responsable de RR. HH.
- Tu coordinador de servicio si eres colaborador externo.

Todos los profesionales debemos informar a nuestro responsable sobre cualquier conducta que creamos, de buena fe, que es una vulneración del Código de Conducta Ética.

Si cualquiera de los tres anteriores está implicado en la situación que deseamos informar o no puede o no ha resuelto adecuadamente nuestras preocupaciones, informaremos a un director de más alto rango o al responsable de RR. HH. del área o al encargado de cumplimiento penal de la empresa, y se informa que todo el personal tiene a su disposición un Canal Interno de Información mediante el cual es posible notificar, de forma totalmente confidencial, comportamientos o hechos contrarios a la ética, a la legalidad vigente, al presente Código de Conducta Ética o a las prácticas de buen gobierno corporativo que rigen nuestra Compañía, con especial énfasis en aquellas que pudieran tener trascendencia penal.

No realizamos discriminación alguna ni tomamos represalias contra empleados por el hecho de haber informado, de buena fe, sobre infracciones reales y probadas. El Departamento de Recursos Humanos, en cuanto a Nombramientos y Retribuciones, velará por el cumplimiento del presente Código, resolverá incidencias o dudas sobre su interpretación y adoptará las medidas adecuadas para su mejor cumplimiento.

El incumplimiento de este código puede dar lugar a la adopción de medidas disciplinarias, incluyendo la posibilidad de despido y, en su caso, el ejercicio de las acciones legales oportunas.

En Madrid, a 29 de junio de 2023

PYCSECA SEGURIDAD, S.A
ADMINISTRADOR

La Dirección de la Compañía se ve obligada a adoptar una serie de medidas encaminadas a garantizar, en lo concerniente al tratamiento de información confidencial, datos personales, el derecho de las personas físicas a su honor e intimidad personal y a evitar la comisión de posibles infracciones en esta materia.

La aplicación de estas medidas de seguridad, tanto técnicas (informáticas) como organizativas, exige la colaboración de todo el personal, ya sea interno o freelance. Para favorecer su aplicación y cumplimiento se recogen las siguientes **definiciones** a título informativo:

- Dato de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

- Fichero: conjunto organizado de datos cualquiera que sea la forma de creación, almacenamiento, organización y acceso.

- Tratamiento: cualquier operación, tanto informática como manual, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación.

- Responsable del Tratamiento: persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento. El responsable del Tratamiento en este caso es PYCSECA SEGURIDAD, S.A.

- Clasificación de la información: El personal deberá clasificar la documentación bajo su responsabilidad como confidencial, interna o pública. Conforme lo establecido a continuación:

    - **Confidencial**: Esta información, aunque no está penado, es de alta sensibilidad personal y/u organizacional; su pérdida, adulteración o eliminación será sancionado debido a que puede generar pérdidas económicas, daños al derecho de la privacidad de las personas y de la organización. Cualquier persona que solicite acceder a este tipo de información deberá, previamente, solicitar la autorización de la persona dueña de la información o de la Dirección para fines estrictamente necesarios.
      Ej.: Información estratégica, operacional, de los trabajadores y contable de la Compañía y documentación de los clientes.

    - **Interna:** Es la información que genera o utiliza la organización continuamente. Las atribuciones de generación, modificación o eliminación están limitadas de acuerdo con las funciones de cada trabajador. Cada trabajador/a tiene la responsabilidad de velar por la seguridad de la información cedida. Todo cambio en los privilegios deberá ser solicitado al superior inmediato y al Responsable del Sistema de Seguridad de la Información.
      Ej.: Contratos con proveedores, Documentación del sistema de gestión.

    - **Pública:** Es la documentación que la Compañía considera sea de conocimiento público.
      Ej.: Revistas, publicaciones, página web.

Se establece por tanto el siguiente **Protocolo Interno de Seguridad**, que será de obligado cumplimiento para todo el personal, interno o freelance, de la Compañía:

1. **CONFIDENCIALIDAD Y DEBER DE SECRETO:**

    - El/la trabajador/a deberá de guardar secreto y mantener la más estricta confidencialidad sobre toda la información y datos de carácter personal a los que tenga acceso en virtud

de sus trabajos. Se compromete a no revelar, transferir, ceder o comunicar, ya sea verbalmente o por escrito, a terceras personas, cualquier información y datos de carácter personal relativa a los trabajadores, clientes y proveedores de la Compañía, excepto cuando sea necesario para la consecución y el buen fin del servicio prestado. Dicha obligación subsistirá incluso después de finalizar su relación con la Compañía.

- Dicho deber de secreto también se hace extensivo a los siguientes aspectos predicables de la Compañía: estrategias, productos, procedimientos internos y comerciales, métodos de trabajo, política de precios, estimación de costes y beneficios, estado de solvencia, ratios, lista de clientes, ventas y resultados, datos financieros, así como cualquier otra información no pública relativa a la Compañía.

- Una vez finalizada la relación laboral o profesional con la Compañía, el/la trabajador/a no podrá mantener bajo su custodia cualquier escrito, nota, listado correspondencia, informe o cualquier otro documento relacionado con las materias mencionadas en los puntos anteriores, sea cual fuere la forma de obtención o tenencia (documental o digital) y, en su caso, deberá entregarlos a la Compañía en el momento del cese de su relación laboral, profesional, independientemente de cuál fuera su causa.

- Si se comprueba que el trabajador ha modificado, eliminado, substraído o perdido información (Confidencial o Interna) podrá suponer causa suficiente de apertura de expediente disciplinario, conforme a la siguiente tabla:

Clase de Información	Proceso Disciplinario
Confidencial	Según el Estatuto de los Trabajadores y el convenio de seguridad privada
Interna	
Pública	

2. SEGURIDAD DE SOPORTES INFORMÁTICOS Y POLÍTICA DE TRABAJO FUERA DE LA OFICINA

- El usuario deberá velar por la seguridad y confidencialidad de la información contenida en los soportes asignados, especialmente cuando se encuentre fuera de las dependencias de la Compañía. Para ello:

  - No es recomendable almacenar en los soportes información interna o confidencial, de darse el caso, el trabajador/a deberá asegurar la realización de copias de seguridad de esta.

  - En caso de tener que viajar con el soporte, nunca se facturará con el equipaje.

  - Nunca se debe dejar el soporte desatendido y a la vista del público, especialmente en situaciones que puedan aumentar el riesgo de robo. En los hoteles, el soporte deberá guardarse con candado o en un espacio cerrado bajo llave.

  - En caso de pérdida del soporte, el incidente deberá ser comunicado inmediatamente al Responsable Informático.

  - Antes de introducir/descargar información en los soportes, desde cualquier dispositivo de almacenamiento, éste deberá ser examinado por la aplicación de

antivirus.

- Para verificar el correcto funcionamiento de los equipos y el buen uso de estos, el Responsable de Informática realizará inspecciones periódicas (de forma aleatoria entre todo el personal de la Compañía según el criterio de esta, tantas veces como ésta estime oportuno) con el objeto de examinar los siguientes aspectos:

  - Aplicaciones instaladas.
  - Estado del antivirus.
  - Configuración estándar del Sistema Operativo (hardware y software).
  - Estado físico del soporte.
  - Estado de los escritorios.

- El/la trabajador/a que posea privilegios de conexión remota deberá tomas las siguientes precauciones:

  - La asignación definitiva o puntual, así como la salida de soportes informáticos de la Compañía, deberá ser expresamente solicitada y autorizada por el Responsable del Sistema de Gestión.
  - En lo posible, no conectar el portátil en establecimientos que tengan redes wi-fi abiertas (no seguros).
  - El/la trabajador/a es responsable de mantener operativo los soportes dispuestos a su cargo. Las labores a realizar de manera cotidiana son:

    - Tomar todas las precauciones necesarias para evitar la pérdida o daño del equipo (traslados, limpieza, ubicación del equipo, etc.).

    - Procurar conectar el portátil a la red interna de la Compañía o a Internet de forma segura para que automáticamente se actualicen las aplicaciones de protección del equipo.

- El mantenimiento o manipulación de los equipos informáticos deberá ser realizado por el Responsable Informático.

- El trabajador/colaborador deberá disponer del equipo, infraestructura y red de comunicaciones necesarios para poder realizar Teletrabajo en los estándares de seguridad establecidos en el presente Protocolo Interno de Seguridad.

- Se prohíbe expresamente el uso de soportes informáticos (pendrive, discos duros externos, portátiles, etc) que no sean proporcionados o no hayan sido autorizados por parte de la Compañía así como la extracción de cualquier tipo de información que no esté autorizada por la compañía a través del Responsable de seguridad de la información.

- El trabajador acepta el uso profesional de su teléfono móvil particular y se compromete a usarlo de conformidad con los estándares de buenas prácticas aquí previstos, en la medida en que conviven en el dispositivo información personal y empresarial.

3. POLÍTICA DE BACKUP DE INFORMACIÓN

- Cada trabajador/a deberá guardar periódicamente la información de los proyectos asignados de la estación de trabajo o soporte, hacia el servidor.

- Las copias de seguridad de los servidores de la Compañía deberán ser registradas y

controladas periódicamente.

4. POLÍTICA DE ESCRITORIOS Y PANTALLAS LIMPIAS

- Escritorios Limpios
  - Toda documentación clasificada como confidencial (impresa o escrita), así como la información contenida en dispositivos de almacenamiento deberán ser guardadas en el armario personal o del departamento, asegurado bajo llave.
  - Está prohibido escribir información confidencial o restringida en soportes fáciles de perder o estropear (Ej.: post it, papel reciclado, etc.)
  - Mantener, en lo posible, el escritorio de trabajo ordenado y libre de documentación obsoleta o inservible ya que podría confundirse con documentación valiosa.
  - Se recomienda no beber (en envases sin tapón) o consumir alimentos en los escritorios de trabajo ya que pueden originar deterioro de los equipos y de la documentación.
- Pantallas Limpias
  - Se recomienda, a todos los trabajadores, no contar con información confidencial alojada en el escritorio de su sesión.
  - El/la trabajador/a deberá bloquear el equipo cada vez que se retire de su puesto de trabajo.

5. PROTECCIÓN ANTE CÓDIGO MALICIOSO

- Únicamente se podrán instalar, en las estaciones de trabajo o portátiles, aplicaciones permitidas por la Compañía, previa solicitud del trabajador/a y posterior autorización del Responsable de Informática. La solicitud de instalación de aplicaciones debe comunicarse al Responsable de Informática mediante el formulario correspondiente.
- El/la trabajador/a que sospeche de un determinado programa o archivo deberá informar inmediatamente al Responsable de Informática.
- El/la trabajador/a que sospeche del contenido de un dispositivo de almacenamiento externo deberá consultar directamente su ejecución al Responsable de Informática.

6. CONTROL DE ACCESOS:

- Cada persona es responsable de los mecanismos de acceso a los locales y sistemas de información para los que ha sido autorizado en función de su cargo o responsabilidades. En la zona habilitada de la CRA (Central receptora de Alarmas) para la custodia de llaves, deberá existir una copia de todas las llaves de acceso a las dependencias de PYCSECA SEGURIDAD, en caso de robo o extravío deberá comunicarse inmediatamente al responsable de la custodia de llaves.
- El personal tendrá acceso únicamente a los datos de carácter personal que precise para

el desarrollo de sus funciones.

- El Administrador del Sistema se reserva el derecho de poder acceder al correo corporativo de cada usuario para realizar tareas de control del sistema, mantenimiento o resolver incidencias de manera excepcional.

7. CONTRASEÑAS:

- A cada usuario se le asignará un nombre de usuario y contraseña de carácter confidencial, personal e intransferible. Es importante no teclear la contraseña a la vista de terceras personas. En caso de no recordar la contraseña, los usuarios deberán ponerse en contacto con el Responsable de Informática.
- Las contraseñas deben cambiarse con una periodicidad de cuatro meses (120 días).
- No utilizar las funciones de recordar las contraseñas en ninguna de las aplicaciones proporcionada o requeridas por la organización.
- Es importante no teclear la contraseña a la vista de terceras personas. En caso de no recordar la contraseña, los usuarios (trabajador/a) deberán ponerse en contacto con el Responsable de Informática.
- Las cuentas administrativas no pueden ser compartidas. En caso de que varios usuarios (trabajadores) requieran este tipo de acceso, sólo serán otorgados a través de un grupo de usuarios administrativos de sistemas.
- Las contraseñas no deberán estar escritas en soportes de fácil extravío o divulgación. (Ej.: post it, papel reciclado, etc.)
- Por ningún motivo el personal informático podrá solicitar las contraseñas de las cuentas al trabajador.
- Guía de generación para la construcción de contraseñas robustas:
  - Longitud mínima de 8 caracteres.
  - Al menos 3 de las 4 características: minúsculas, mayúsculas, números o símbolos.
  - Vigencia máxima de 45 días.
  - Las nuevas contraseñas no pueden haber sido usadas en los últimos 365 días y deben ser validadas contra una lista negra con el fin de evitar palabras predecibles.
  - 45 días de vigencia
  - Limitación de 5 intentos de acceso. El equipo se bloqueará durante 15 minutos.
- Las contraseñas no serán almacenadas en un equipo de manera irreversible.

8. POLÍTICA DE ELIMINACIÓN DE DOCUMENTOS Y UNIDADES DE ALMACENAMIENTO DE INFORMACIÓN

- Toda documentación en papel que contenga información clasificada como confidencial

y se desee eliminar, deberá ser depositada en el contenedor del proveedor de destrucción de documentación.

- Los dispositivos de almacenamiento que se desee eliminar y que contengan información clasificada como confidencial deberán entregarse al personal correspondiente para su posterior borrado por la empresa contratada para el reciclado de soportes de almacenamiento. En su defecto, deben ser debidamente borrados.

- Los componentes de almacenamiento (Discos Duros, Cintas, memorias, etc.) que se desee eliminar y contengan información clasificada como confidencial deberán (según sea el dispositivo) entregarse al personal correspondiente para su posterior eliminación por parte de la empresa contratada para el reciclado de dichos componentes. Si se desea reutilizar los dispositivos, previamente se le solicitará al Departamento de Informática que se realicen las siguientes operaciones: eliminación de particiones, formateo del dispositivo a bajo nivel y/o sobreescritura de la información (clasificada como pública).

9. INCIDENCIAS:

- Cualquier persona que advierta alguna incidencia, anomalía, disfunción o fallo en el sistema informático que ponga en riesgo la seguridad de los datos lo pondrá inmediatamente en conocimiento del Responsable de Informática.

- Las incidencias relacionadas con informática deberán comunicarse por correo electrónico al Departamento de Informática a través de la cuenta informatica@pycseca.com para la generación del correspondiente ticket. La prioridad de las incidencias se determinará dentro del departamento según la gravedad e importancia de las mismas por el Responsable de Informática.

- Los equipos que puedan ser comprometidos por incidentes que afecten a la seguridad de los datos quedarán en cuarentena para su análisis y restablecimiento a una situación segura. Solo cuando se haya resuelto el incidente de seguridad el equipo se volverá a restituir al usuario.

10. USO DE INTERNET Y CORREO ELECTRÓNICO

- El uso de Internet por parte del personal queda restringido a fines estrictamente profesionales. A estos efectos, la Compañía se reserva el derecho de control sobre las sesiones de navegación de cada usuario, a fin de mantener el adecuado uso de Internet como herramienta de trabajo.

- No se enviarán mensajes de correo electrónico que contengan datos de carácter personal de terceros ajenos a la relación entre emisor y destinatario o que puedan vulnerar la seguridad de los datos de carácter personal de terceras personas. Por ello se prohíbe enviar mensajes comunes a varios destinatarios incluidos sin la opción de copia oculta (CCO). En particular, no se utilizará el correo electrónico para enviar o recibir mensajes con contenidos obscenos, pornográficos, discriminatorios, difamatorios o dañinos ni que puedan atentar contra los derechos y libertades de las personas.

- Tampoco se permite el envío de información corporativa a cuentas de correo personales ajenas a la actividad profesional de la Compañía.

- Se recomienda no abrir documentos adjuntos de correos electrónicos cuyo emisor sea

desconocido o cuyo asunto del mensaje pueda inducir a sospechar de la presencia de un virus informático.

- El usuario que sospeche que un determinado programa o archivo puede estar infectado por un virus, deberá informar inmediatamente al Departamento de Informática antes de realizar ninguna acción en referencia al correo recibido. En ningún caso debe borrar cualquier mail que pueda resultar sospechoso, especialmente si antes de advertirlo al Departamento de Informática ha abierto, ejecutado o seguido alguna indicación del mismo ya que se debe conservar cualquier evidencia que pudiera ser necesaria para un posterior análisis forense.

- El espacio del correo es finito tanto si está en el equipo del usuario como si se encuentra almacenado en Internet. En ambos casos, el usuario es el responsable de mantener la organización de su correo borrando todos los correos innecesarios para sus tareas profesionales para asegurar un buen funcionamiento de los buzones. En caso de llegarse al límite del espacio permitido por el buzón, el administrador de los sistemas podrá eliminar los mensajes o reiniciar la cuenta por completo. El usuario debe:

  - Revisar periódicamente las bandejas y eliminar los mensajes que no sea imprescindible conservar.

- La Compañía se reserva el derecho de poder acceder al correo corporativo de cada usuario para realizar tareas de control, mantenimiento o resolución de incidencias.

- **Solo se podrán conservar en el buzón de correo elementos con antigüedad no superior a un año.**

- El usuario de correo debe observar ciertas reglas de utilización del correo, teniendo noción clara de a quién van dirigidos los correos para que realicen las acciones o gestiones pertinentes y quién debe estar informado de la situación que genera dicho correo. En la medida de lo posible el usuario debe procurar que la comunicación por mail sea efectiva y ágil y no genere confusión o desinformación. Como medidas generales para optimizar el uso del correo electrónico se debe:

  - Identificar de forma clara y concisa el asunto del correo.

  - No incluir datos personales en el asunto.

  - Minimizar palabras o expresiones que puedan activar puntuaciones de los módulos antispam propios o ajenos (ej: **Mejor Precio, 100%, Gratis, Cash Bonus…**).

  - Revisar las direcciones de los destinatarios antes de enviar el mensaje, especialmente tener en cuenta la opción ‘Responder a todos’.

  - **No utilizar la opción ‘Responder a todos’ si no es estrictamente necesario.**

  - Con objeto de no difundir de manera injustificada direcciones de correo de terceros:

    - Al reenviar un correo, revisar y eliminar las direcciones de destinatarios externos de los que no tenemos autorización explícita para compartir su dirección.

    - Emplear la opción de copia oculta (CCO) cuando se mande mensajes a

destinatarios que no formen parte de PYCSECA SEGURIDAD.

- **Revisar archivos adjuntos antes de enviarlos.**
- En caso de ausencia programada superior a dos días, el titular de la cuenta deberá activar un mensaje de ausencia de oficina para facilitar otra dirección de contacto que garantice la continuidad de la actividad.

- En caso de baja de personal, el correo se mantendrá activo durante un periodo de un mes, redirigiéndose éste a la persona que sustituya a la que cause baja y respondiendo un mensaje automático de aclaración. Una vez transcurrido el periodo mencionado, se procederá a dar de baja la cuenta de correo.

11. COMUNICACIONES DE PARTICULARES

- Cualquier persona que reciba una carta, requerimiento, mensaje de correo electrónico, llamada telefónica o cualquier otra comunicación (incluso verbal) en la que se haga referencia a materias relacionadas con la protección de datos de carácter personal y en especial a la normativa vigente en materia de protección de datos, deberá ponerlo inmediatamente en conocimiento del Responsable del Sistema de Seguridad de la Información, que adoptará las medidas oportunas.

- Este tipo de comunicaciones no deben contestarse sin previa autorización del Responsable del Tratamiento, ya que la normativa de protección de datos exige para ello unos plazos y requisitos legales que, de no cumplirse, podrían comportar una grave responsabilidad para la Compañía.

- Cualquier persona que recoja o reciba un Currículum, ya sea en papel, sea porque se haya entregado personalmente o enviado por correo, o en formato electrónico porque haya sido enviado por e-mail, deberá ponerlo en conocimiento de la persona encargada de su gestión para poder dar curso a la solicitud según el protocolo establecido. No deberá almacenarse ningún Currículum sin la debida información y petición de consentimiento al interesado.

1. PRESENTACIÓN

PYCSECA Seguridad ha establecido como una de sus prioridades capitales, el desarrollo sostenible de su actividad, respetando el Medio Ambiente en todos los procesos de su actividad. Por ese motivo, y como uno de los medios para ayudar a conseguir ese principio, ha implantado en el seno de su organización un sistema de Gestión Ambiental con referencia a la **Norma UNE- EN ISO 14001.**

El presente Manual describe un conjunto de responsabilidades a cumplir por **PYCSECA Seguridad**, así como un conjunto de buenas prácticas relativas a aspectos ambientales (aplicables tanto a trabajos en cliente como a las propias instalaciones del proveedor) y que tiene como objetivo principal promover un correcto comportamiento ambiental, siempre que sea posible, de todos y cada uno de los miembros de la organización.

2. OBLIGACIONES COMO PRODUCTOR DE RESIDUOS

PYCSECA Seguridad, dentro de las obligaciones y responsabilidades, debe:

- ✓ Cumplir con la legislación vigente en materia ambiental.
- ✓ Cumplir con cualquier otro requisito de índole ambiental establecido por las autoridades competentes.
- ✓ Poner todos los medios necesarios para no influenciar de manera negativa en el Medio Ambiente.
- ✓ Asegurar que sus subcontratistas o terceras partes cumplan con todos los requerimientos ambientales establecidos por PYCSECA Seguridad y/o las autoridades correspondientes.

En concreto, en las actividades de instalación que se realicen, los trabajadores deberán:

- ✓ No dejar ningún tipo de residuo en las ubicaciones donde se realicen las instalaciones. Estos residuos se depositan en los contenedores ubicados en el almacén de PYCSECA Seguridad.
- ✓ Gestionar los residuos que se generen con gestores homologados.
- ✓ Está absolutamente prohibido, el abandono, almacenamiento indebido, o entrega como residuo urbano convencional de cualquiera de estos residuos denominados tóxicos o peligrosos.

3. TIPOS DE RESIDUOS QUE SE GENERAN

Residuos urbanos: Son los residuos propios de la actividad, generalmente envases y embalajes, que en la mayoría de los casos se gestionan por los mismos cauces que los residuos sólidos urbanos. En general, papel y cartón, telas y trapos no contaminados, serrín y otros absorbentes, recortes de metales, botellas de vidrio, latas de aluminio, envases ligeros, otros plásticos, restos orgánicos de alimentación, etc.

Peligrosos: Son los principales residuos producidos por cantidad y peligrosidad: baterías, pilas, gases refrigerantes, aceites usados de motor, líquidos refrigerantes, filtros varios, gasóleos y derivados, etc. Todos necesitan una gestión específica.

4. BUENAS PRÁCTICAS AMBIENTALES

4.1 GESTIÓN DE LOS CONSUMOS DE RECURSOS NATURALES

CONSUMO DE AGUA:

- ✓ Cierre los grifos durante la aplicación del producto de limpieza.
- ✓ No utilice el WC como basurero.

CONSUMO DE ENERGÍA:

- ✓ Acondicione las áreas de trabajo, cuando sea posible, para aprovechar al máximo la luz y el calor natural.
- ✓ Desconecte las luces y los equipos cuando no sean necesarios.
- ✓ Active los sistemas de ahorro de energía en impresoras, fotocopiadoras, ordenadores y otros equipos, para que no funcionen durante largos periodos de tiempo de inactividad.
- ✓ Evite el uso del aire acondicionado cuando no sea necesario, y considere otras alternativas como, ventilación natural, etc.
- ✓ Revise el aislamiento para comprobar que no existen fugas de calor innecesarias.

CONSUMO DE PRODUCTOS:

- ✓ Comprobar que los productos están debidamente etiquetados y con instrucciones claras de manejo.
- ✓ Elegir productos certificados, como los ecológicos.
- ✓ Adquirir productos que no tengan efectos negativos sobre el medio y la salud: bajo consumo, reducido nivel de ruido, carcasas reciclables., etc.
- ✓ Implantar controles de calidad en el proceso productivo para evitar desperdicio de material.
- ✓ Emplear los equipos y herramientas más adecuados para cada tarea para disminuir el consumo de recursos.
- ✓ Utilizar siempre consumibles homologados, puesto que están sometidos a controles de calidad que incluyen aspectos ambientales.
- ✓ Elegir útiles y herramientas de larga duración.
- ✓ No cambiar las piezas de forma innecesaria.
- ✓ Proteger los almacenes de las inclemencias del tiempo para evitar el deterioro de los productos.

CONSUMO DE PAPEL:

- ✓ Trabaje en soporte informático, reduciendo el uso de papel.
- ✓ Use la vía informática como método de correo.
- ✓ Reutilice sobres y carpetillas para envíos internos
- ✓ Utilice papel con etiqueta ecológica reconocida oficialmente (ecológico 100% reciclado):
- ✓ Imprima y fotocopie por las dos caras del papel.
- ✓ Deposite el papel y el cartón en los recipientes habilitados en cada centro de trabajo para su recogida selectiva.

CONSUMO DE CARTUCHOS DE TINTA Y TÓNER:

- ✓ Agite el cartucho de tóner cuando la impresora dé el aviso de que está bajo (puede dar 100 copias más).
- ✓ Deposite los cartuchos de tinta y tóner agotados en los recipientes habilitados en cada centro de trabajo para su recogida selectiva.

TRANSPORTE:

- ✓ Planificar las rutas correctamente, teniendo en cuenta también la distribución de materiales.
- ✓ Comparta el vehículo en sus trayectos.
- ✓ Mantenga y revise los vehículos de la empresa con regularidad.
- ✓ Utilice vehículos con bajo consumo en combustible.
- ✓ No acelere ni frene bruscamente.
- ✓ Apague el motor del vehículo cuando no esté circulando.
- ✓ Identificar la ubicación de absorbentes industriales para líquidos peligrosos en caso de fugas.

COMPRAS:

- ✓ Adquiera materiales y productos en zonas geográficamente cercanas para reducir costes de transporte y la contaminación derivada del mismo.
- ✓ Tener en cuenta criterios ambientales en la adquisición de materiales y en la contratación de servicios mediante la elección de materiales, productos y suministradores con certificación ambiental.
- ✓ Informar al departamento de compras sobre los productos que pueden ser perjudiciales para el medio ambiente.
- ✓ Acordar con los proveedores la reducción de envases o la utilización de retornables, así se generarán menos residuos.
- ✓ Compre productos biodegradables y que hayan sido diseñados para su reutilización:

El envasador, fabricante o responsable de la primera puesta en el mercado del producto, abona una cantidad por envase para financiar su recogida selectiva por Ecoembes y Ecovidrio.

En la materia prima del producto está contenida una cierta cantidad de material recuperado o bien que éste es reciclable.

Según el número que vaya en el centro, permite identificar el tipo de plástico, facilitando su clasificación y reciclaje.

- ✓ Busque productos con etiquetas ecológicas reconocidas oficialmente.

Etiqueta Ecológica Europea

Marca AENOR Medio Ambiente

Ecoetiqueta IPE

Ángel Azul

Nordic Ecolabelling

- ✓ Adquiera equipos que optimicen el consumo de energía, agua o materiales.

- ✓ Compre el material a granel o en grandes sacos, son más baratos y generan menos residuos de envases.

MANIPULACIÓN Y ALMACENAMIENTO DE MATERIALES:

- ✓ Mantenga las zonas de transporte limpias, iluminadas y sin obstáculos para evitar derrames accidentales.
- ✓ Mantenga cerrados los envases de productos químicos para evitar derrames en el transporte y durante el almacenamiento.
- ✓ En caso de derrame de productos químicos se procederá a recoger dicho derrame gestionando los residuos producidos adecuadamente en función de la naturaleza de los mismos.

4.2 GESTIÓN DE RESIDUOS:

- ✓ Colabore con los sistemas de recogida de basuras implantados en cada municipio.
- ✓ Deposite los residuos en los recipientes habilitados para su recogida selectiva.
- ✓ Deposite los residuos sólidos urbanos en los contenedores municipales.
- ✓ Cierre bien las bolsas de basura.
- ✓ Segregue todos los residuos que sea posible, esto evitará generar más residuos de los necesarios o convertir en peligrosos los residuos que no lo son al mezclarlos.
- ✓ Gestionar los residuos de forma que se facilite su recuperación.
- ✓ Separar los residuos y acondicionar un contenedor para depositar cada tipo en función de sus posibilidades y requisitos de gestión.
- ✓ Utilizar productos que al final de su vida útil sean reciclables.
- ✓ Emplazar los contenedores de residuos peligrosos en zonas bien ventiladas, a cubierto del sol y la lluvia, separados de focos de calor y colocados de forma que no puedan reaccionar entre sí.
- ✓ Separar y aislar los fluidos de motor para evitar derrames.
- ✓ Depositar los residuos peligrosos generados en caso de derrames de fluidos de motor en los contenedores para residuos peligrosos.
- ✓ Reutilizar, en la medida de lo posible, las aguas de lavado.
- ✓ Aislar las zonas donde se trabaje con productos peligrosos.
- ✓ Almacenar en los recipientes adecuados los residuos peligrosos, evitando el contacto con el exterior.
- ✓ Evitar la realización de reparaciones en zonas de vía pública o espacios abiertos.
- ✓ Evitar el vertido de los productos de limpieza o restos de éstos a la red de saneamiento público.
- ✓ Evitar que los cables y otros elementos conductores contengan halógenos en su composición para evitar la emisión de gases nocivos en caso de incendio y para poder reciclarlos sin contaminar
- ✓ Tras una situación de incendio, se procederá a gestionar los residuos producidos adecuadamente en función de la naturaleza de los mismos.

1. <u>OBJETO:</u> Establecer la sistemática para cumplir los requisitos del sistema de gestión profesional y deontológico de los servicios de seguridad privada.	**2. <u>APLICACIÓN</u>** General ☑

3.- Requisitos

3.1 Requisitos generales.

Requisito	Responsable	Descripción
Formar parte de Aproser y estar al corriente de pago	Responsable del SIG	Cumplir con este requisito dejando evidencia con la aceptación de la adhesión y el recibo de pago.
La empresa de seguridad debe disponer de certificaciones	Responsable del SIG	Ver punto 4: Sistema de gestión profesional y deontológico
La empresa debe disponer de infraestructura y material adecuado	Dirección	Asegurar que se dispone de autorización administrativa y local con las medidas de seguridad oportunas dejando evidencia en el **registro evaluación de cumplimiento legal** del **procedimiento P-082 Requisitos legales**.

3.2 Requisitos orientados a personas trabajadoras.

Requisito	Responsable	Descripción
Requisitos de igualdad y no discriminación negativa	Responsable del Sistema Integrado	Ver punto 4: Sistema de gestión profesional y deontológico
Personal debe ser competente	Responsable del Sistema Integrado	Cumplir con la ficha de perfil tal y como establece el **procedimiento P-097 Recursos humanos.**
Facilitar al personal elementos necesarios para desarrollar su trabajo	Responsable PRL	Entrega de EPI's y uniformes tal y como establece el **procedimiento P-097 Recursos humanos y el procedimiento P-047 Entrega EPI's**
Informar al personal subrogado	Responsable RRHH	Cumplir con lo que se establece el **procedimiento P-097 Recursos humanos.**
Firma del compromiso de confidencialidad	Responsable RRHH	Cumplir con lo que se establece el **procedimiento P-097 Recursos humanos.**
Cumplir normativa relativa a protección de datos	DPD	Ver punto 4: Sistema de gestión profesional y deontológico
Código deontológico	DPD	Ver punto 4: Sistema de gestión profesional y deontológico
Requisito de participación	Responsable RRHH	Ver punto 4: Sistema de gestión profesional y deontológico
Requisito de seguridad y salud	Responsable PRL	Ver punto 4: Sistema de gestión profesional y deontológico
Conciliación vida laboral y personal	Responsable RRHH	Ver punto 4: Sistema de gestión profesional y deontológico
Protocolo de violencia de género	Responsable RRHH	Ver punto 4: Sistema de gestión profesional y deontológico

Requisito	Responsable	Descripción
Protocolo contra el acoso laboral	Responsable RRHH	Ver punto 4: Sistema de gestión profesional y deontológico
Reconocimiento del trabajo	Dirección	Realizar esfuerzos necesarios para el reconocimiento de la profesión
Remuneración de las personas trabajadoras	Responsable RRHH	Ver punto 4: Sistema de gestión profesional y deontológico
Proactividad con personas con discapacidad y su inclusión social	Responsable RRHH	Establecer indicadores en el **registro R-045 del procedimiento P-041 Contexto de la Organización** que superen el mero cumplimiento de la legislación aplicable.
Cumplimiento de las condiciones de habilitación del personal	Responsable RRHH	Cumplir requisitos legales dejando evidencia en el **registro evaluación de cumplimiento legal** del **procedimiento P-082 Requisitos legales.**
Requisitos de formación	Responsable RRHH	Cumplir con lo que establece el **procedimiento P-097 Recursos humanos.**
Cumplimiento de la normativa laboral y convenio colectivo	Responsable RRHH	Cumplir requisitos legales dejando evidencia en el **registro evaluación de cumplimiento legal** del **procedimiento P-082 Requisitos legales.**
Corriente de pago en la Seguridad Social	Responsable RRHH	Cumplir requisitos legales dejando evidencia en el **registro evaluación de cumplimiento legal** del **procedimiento P-082 Requisitos legales.**
Cumplimiento de legislación respecto a representación y libertad Sindical	Responsable RRHH	Ver punto 4: Sistema de gestión profesional y deontológico

3.3 Requisitos orientados a clientes y proveedores.

Requisito	Responsable	Descripción
Cumplir requisitos legales y reglamentarios	Responsable del Sistema Integrado	Cumplir requisitos legales dejando evidencia en el **registro evaluación de cumplimiento legal** del **procedimiento P-082 Requisitos legales.**
Disponer de confirmaciones de buena ejecución del servicio	Dir. Operaciones/ Comercial	Realización del informe de satisfacción y de las felicitaciones enviadas por el cliente.
Estados financieros	Dir. Financiero	Aportar estados financieros que garanticen que no hay deterioro en las reservas.
Póliza de seguro	Dir. Financiero	Seguro de responsabilidad civil y cualquier seguro adicional.
Norma ISO 27001	Responsable del Sistema Integrado	Ver punto 4: Sistema de gestión profesional y deontológico
Adaptación al Reglamento europeo de protección de datos	DPD	Ver punto 4: Sistema de gestión profesional y deontológico
Cumplir los acuerdos establecidos en el contrato	Responsable del Sistema Integrado	Mantenimiento certificación ISO 9.001 y cumplimento de los procedimientos del SIG
Establecer procesos de control e inspección	Responsable del Sistema Integrado	Mantenimiento certificación ISO 9.001 y cumplimento de los procedimientos del SIG
Aplicar un código ético en la selección de proveedores	Responsable de compras	Realización, comunicación y aplicación en la selección de proveedores.

Requisito	Responsable	Descripción
Cuentas anuales	Dir. Financiero	Cumplir requisitos legales dejando evidencia en el **registro evaluación de cumplimiento legal** del **procedimiento P-082 Requisitos legales.**
La empresa debe cumplir sus obligaciones con los proveedores	Responsable del Sistema Integrado	Mantenimiento certificación ISO 9.001 y cumplimento de los procedimientos del SIG

3.4 Requisitos orientados a la sociedad.

Requisito	Responsable	Descripción
Colaborar con las administraciones públicas	Direcciones de al empresa	Ver punto 4: Sistema de gestión profesional y deontológico
Fomento y estabilidad de empleo local	Dir. RRHH	Ver punto 4: Sistema de gestión profesional y deontológico
Código deontológico	DPD	Ver punto 4: Sistema de gestión profesional y deontológico
ISO 27.001	Responsable SIG	Ver punto 4: Sistema de gestión profesional y deontológico
Formación en materia de ética	Dir. RRHH	Cumplir los requisitos establecidos en el plan de formación de la empresa
Cumplimiento de la legislación	Dirección	Cumplir requisitos legales dejando evidencia en el **registro evaluación de cumplimiento legal** del **procedimiento P-082 Requisitos legales.**
Cumplir con la normativa en ámbitos mercantil, tributaria, laboral, de protección de los consumidores, blanqueo de capitales, protección de datos, urbanístico, contratación administrativa y de seguridad privada que le sea de aplicación	Dirección	Cumplir requisitos legales garantizando que no existen denuncias a través del **canal de denuncias** de la empresa o cualquier otro canal.

4.- Sistema de gestión profesional y deontológico

4.1 Establecimiento del sistema de gestión profesional y deontológico.

La Dirección de la empresa establecerá los objetivos profesionales y deontológicos y realizará su seguimiento tal y como se define en el **procedimiento P-043 Planificación**.

El control y seguimiento de la información documentada se realizará tal y como se define en el **procedimiento P-091 Información documentada**.

4.2 Responsabilidad de dirección.

La Dirección de la empresa definirá y comunicará la política de gestión tal y como se define en el **procedimiento P-042 Liderazgo y participación.**

Las funciones como responsable del sistema de gestión profesional y deontológico serán asumidas por el responsable del sistema integrado de gestión de calidad y medio ambiente que documentará adecuadamente el sistema y lo difundirá tal y como se define en el **procedimiento P-083 Comunicación y consulta.**

4.3 Descripción del sistema de gestión profesional y deontológico.

4.3.1 Documentación del sistema de gestión profesional y deontológico.

La documentación generada por el sistema de gestión profesional y deontológico se controlará tal y como se define en el **procedimiento P-091 Información documentada**.

4.3.2 Identificación y comunicación interna de los aspectos legales que son de aplicación.

La identificación de aspectos legales se realiza tal y como se define en el **procedimiento P-082 Requisitos legales** y la comunicación de éstos tal y como se define en el **procedimiento P-083 Comunicación y consulta.**

4.3.3 Gestión de recursos humanos.

Requisito	Responsable	Descripción
Elaboración, ejecución, control y mejora de planes de igualdad	Director RRHH	Garantizar el seguimiento del plan de igualdad y la realización de las reuniones de seguimiento de la Comisión.
Promoción profesional del personal	Director RRHH	Realizar promociones de acceso libre
Contratos de trabajo	Director RRHH	Tener un porcentaje de indefinidos superior a lo establecido en el convenio colectivo de seguridad
Establecimiento y uso de canales de participación	Director RRHH	Disponer de: – Comité de Empresa – Comité de seguridad y salud en el trabajo – Canal de denuncias – Proceso de incidencias según P-095. – Correo electrónico Agente de igualdad y Mediador
Recepción de peticiones de conciliación de vida laboral y familiar	Director RRHH	Se recogen siguiendo los canales de participación y Correo electrónico responsable de RRHH.
Canal específico de acceso público e interno para recibir quejas o incidencias	Director RRHH	Disponer de un canal de denuncias y aplicación del **procedimiento P-093 Reclamaciones de cliente**.
Remuneración del personal	Director RRHH	Realizar una correcta remuneración cumpliendo la normativa laboral y el convenio estatal. Asegurar que no se dispone de denuncias por cualquiera de los canales disponibles de la empresa.
Representación y libertad sindical	Director RRHH	Cumplir requisitos legales disponiendo de Comité de Empresa, Comité de seguridad y salud laboral. Asegurar que no se dispone de denuncias por cualquiera de los canales disponibles de la empresa.
Protocolo contra la violencia de género	Director RRHH	Disponer, comunicar y aplicar el protocolo
Protocolo contra el acoso laboral	Director RRHH	Disponer, comunicar y aplicar el protocolo
Normativa en materia de protección de datos	DPD	Disponer de los protocolos necesarios en materia de protección de datos.
Código deontológico	DPD	Disponer, comunicar y aplicar el protocolo

Requisito	Responsable	Descripción
ISO 9.001, ISO 14.001, ISO 45.001 e ISO 27.001	Responsable del SIG	Disponer de las certificaciones vigentes
Comité de Seguridad y Salud	Responsable PRL	Que esté constituido y se realicen las reuniones trimestrales tal y como establece el **procedimiento P-083 Comunicación y consulta.**
Auditorías financieras	Dir. Financiero	Cumplir requisitos legales dejando evidencia a través de la auditoría financiera realizada.
Contratación de seguros	Dir. Financiero	Cumplir requisitos legales dejando evidencia a través de los seguros contratados.
Obligaciones fiscales y de la tesorería de la seguridad social	Dir. Financiero	Disponer de los certificados de corriente de pago.
Reducir la conflictividad laboral	Responsable del Sistema Integrado	Establecer indicadores en el **registro R-045 del procedimiento P-041 Contexto de la Organización.**
Conservación de los registros	Responsable del Sistema Integrado	Aplicar el **procedimiento P-091 Información documentada**
Realización de auditorías internas	Responsable del Sistema Integrado	Aplicar el **procedimiento P-092 Auditorías**
Aplicación de acciones correctivas y mejora continua	Responsable del Sistema Integrado	Aplicar el **procedimiento P-095 Mejora**

DEFINICIONES

No aplica

REFERENCIAS

Norma UNE-EN ISO 9001:2015
Norma UNE-EN ISO 14001:2015
Norma UNE-EN ISO 45001:2018
Norma ISO/IEC 27001:2013
Especificación Sistema de gestión profesional y deontológico de los servicios de seguridad privada. 2013.

CONTROL DE REGISTROS

Código	Titulo	Responsable	Retención
---	Adhesión a Aproser	I: Resp.. SIG	I: 3 años
---	Recibo pago adhesión Aproser	I: Dir. Financiero	I: 6 años
---	Certificado corriente de pago en la seguridad social	I: Dir. Financiero	I: 3 años
---	Auditoría financiera	I: Dir. Financiero	I: 3 años
---	Contrato/s de seguros	I: Dir. Financiero	I: 3 años
---	Certificado ISO 9.001	I: Resp. SIG	I: 3 años
---	Certificado ISO 14.001	I: Resp. SIG	I: 3 años
---	Certificado ISO 45.001	I: Resp. SIG	I: 3 años

---	Certificado ISO 27.001	I: Resp. SIG	I: 3 años
---	Cuentas anuales	I: Dir. Financiero	I: 3 años
---	Certificados corriente de pago	I: Dir. Financiero	I: 3 años
---	Contratos con proveedores y clientes	I: Dir. Financiero	I: 6 años
---	Plan de igualdad	I: Dir. RRHH	I: 3 años
---	Reuniones seguimiento Plan de Igualdad	I: Dir. RRHH	I: 3 años
---	Constitución Comité de Empresa	I: Dir. RRHH	I: 3 años
---	Actas reunión Comité de Empresa	I: Dir. RRHH	I: 3 años
---	Protocolo contra la violencia de género	I: Dir. RRHH	I: 3 años
---	Protocolo contra el acoso sexual	I: Dir. RRHH	I: 3 años
---	Protocolo contra el acoso laboral	I: Dir. RRHH	I: 3 años
---	Protocolo de protección de datos	I: DPD	I: 3 años
---	Código deontológico y ético	I: DPD	I: 3 años

P: Registro en papel **I: Registro Informático**