ANEXO I: POLÍTICA DE PROTECCIÓN DE DATOS APLICABLE AL TRATAMIENTO DE SUS DATOS.

Responsable: GRUPO COSMOS XXI, S.L sita en Pol. Industrial de Aoiz, s/n, con número de Telf.: +34 699 132 896 y dirección de correo electrónico info@gcosmos.com. El Responsable, cuenta con un Delegado de Protección de Datos con el que puede contactar a través de la siguiente dirección de correo electrónico: dpd@gcosmos.com.

Tratamientos: El Responsable tratará los datos de carácter personal que nos facilite con motivo de la Relación que nos une con usted para el control y ejecución de la Relación y en particular para las finalidades que se indican a continuación. En relación con cada tratamiento (uso de datos) le indicamos la base que nos legitima para tratar sus datos y el tiempo durante el que realizaremos el mismo. Asimismo, bajo el epígrafe "comunicaciones" le identificamos aquellos terceros a los que eventualmente podemos comunicar sus datos.

Tratamiento	Base legal	Comunicaciones	Plazo conservación
Control y ejecución de la Relación, inclusive el pago de salarios, evaluación de desempeño, potestad disciplinaria y control de medios digitales.	Obligación legal. Ejecución contrato laboral. Interés legítimo (artículo 20 Estatuto de los Trabajadores)	Otras empresas del Grupo (se recoge información sobre esto más adelante). Agencia Estatal de Administración Tributaria. Instituto Nacional de la Seguridad Social. Bancos y entidades financieras. Tribunales y órganos arbitrales. Representantes de los trabajadores/as - Comité de empresa.	Durante la Relación y finalizada ésta mientras persista responsabilidad para el Responsable.
Prevención de riesgos laborales	Obligación legal (Ley 31/1995, de prevención de Riesgos Laborales) Consentimiento para los reconocimientos voluntarios.	Instituto Nacional de la Seguridad Social. Mutuas Colaboradoras con la Seguridad Social.	
Formación	Ejecución contrato laboral	Fundación tripartita Empresa/personal formador/a	
Control de jornada	Obligación legal. Artículo 34.9 Estatuto de los Trabajadores	Inspección de trabajo. Tribunales y órganos arbitrales.	4 años
Control de accesos; Acceso mediante vector huella dactilar-Acceso	Interés público y en el caso de acceso por huella, consentimiento.	Cuerpos de seguridad del Estado Tribunales y órganos arbitrales Empresa de seguridad	Durante la Relación y finalizada ésta mientras persista responsabilidad para el Responsable.
Gestión y coordinación viajes	Ejecución contrato laboral	Agencia de viajes	

Canales de denuncia	Interés público	Tribunales y órganos arbitrales Cuerpos de seguridad del Estado	3 meses
Videovigilancia	Interés público	Cuerpos de seguridad del Estado Tribunales y órganos arbitrales Empresa de seguridad	30 días
Contratación y gestión seguros fuera convenio	Consentimiento	Correduría de seguros. Aseguradoras.	Durante la Relación y finalizada ésta mientras persista responsabilidad para el Responsable.
Publicación datos intranet y sitio web.	Interés legítimo y en su caso consentimiento.	Personal de la Organización o del Grupo en el caso de la Intranet y público en general en el caso de la web corporativa.	
Eventos	Consentimiento	Personal de la Organización o del Grupo.	Mientras sea necesario para la gestión del evento y una vez finalizado este plazo, mientras persistan responsabilidades para el Responsable.
Uso imagen de la PERSONA.	Consentimiento	Generalidad del público	Mientras se utilice el material en el que aparece la PERSONA. O hasta que retire su consentimiento para el tratamiento de su imagen con esta finalidad.
Envío de comunicaciones internas relacionadas con el trabajo o que afecten directamente al trabajador/a. Podrá realizarse a través de correo electrónico, teléfono móvil, u otro canal que haya facilitado voluntariamente.	Consentimiento	No hay previsión de comunicación/transferencia de estos datos.	Mientras dure la relación laboral o hasta que retire su consentimiento para el tratamiento.

Grupo de empresas: Dado que el Responsable forma parte de un grupo empresarial, sus datos serán cedidos al resto de organizaciones de su grupo sobre la base legal del cumplimiento del contrato e interés legítimo de la empresa en dicha comunicación, todo ello con la finalidad de poder gestionar el talento y capacidades de organización de la fuerza productiva. Se incluyen, a continuación, las empresas que pertenecen al Grupo:

EMPRESA	N.I.F.	LOCALIZACIÓN
Grupo Cosmos XXI, S.L.	B31949696	Carretera aoiz - km 19,5 · 31420, Urroz-villa (Navarra)
Alcalá Industrial, S.A.U.	A28033066	Polígono Industrial S/n · 31430, Aoiz (Navarra)
Navarra de Estampación e Inyección S.A.U.	A31540503	Polígono Industrial S/n · 31430, Aoiz (Navarra)
Estampaciones Guipúzcoa, S.A.U.	A20666475	Polígono Industrial S/n · 31430, Aoiz (Navarra)
Logística y Acabados S.L.	B20998902	Polígono Industrial S/n · 31430, Aoiz (Navarra)
Cosmos Bizkaia, S.L.U.	B71171557	Polígono Industrial S/n · 31430, Aoiz (Navarra)
Cuadro 1.1. Empresas que forman Grupo Cosmos		

Derechos del titular de los datos. Tiene la posibilidad de ejercitar los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición del tratamiento de sus datos. El ejercicio de los citados derechos podrá hacerse mediante solicitud dirigida por escrito al responsable, en los términos que suscribe la legislación vigente. Puede asimismo interponer una reclamación ante Agencia Española de Protección de Datos (www.aepd.es).

ANEXO II: POLÍTICA DE CONFIDENCIALIDAD.

1.- <u>Deber de confidencialidad</u>: la PERSONA estará sujeta al deber de confidencialidad establecido en el Reglamento General de Protección de Datos y en la Ley Orgánica de Protección de Datos de Carácter Personal y garantía de los derechos digitales. Complementariamente con el deber de confidencialidad establecido en la normativa de protección de datos, serán de aplicación las previsiones establecidas al respecto por las Partes en la presente política.

2.- <u>Concepto de Información Confidencial</u>. Tienen el carácter de Información Confidencial todos los datos e informaciones a los que la PERSONA tenga acceso y/o conocimiento con motivo de su Relación con la ORGANIZACIÓN, siendo indiferente (i) la titularidad (ya sean de la propia ORGANIZACIÓN, de algún Cliente, Proveedor, contacto, etc.), (ii) la naturaleza o tipología de dicha información, (iii) el medio empleado para el acceso y conocimiento, incluyendo expresamente la comunicación oral, y (iv) si la misma se encuentra o no, fijada en un soporte o medio de almacenamiento.

Tiene en todo caso carácter de Información Confidencial lo siguiente:

a) Cualquier información que tenga la consideración de "Secreto Empresarial", según la definición establecida en Ley 1/2019, de Secretos Empresariales.

b) Todo el conocimiento que pueda suponer una ventaja competitiva para la ORGANIZACIÓN, incluyendo todos aquellos conocimientos, datos e informaciones económicas, técnicas, tecnológicas, investigaciones I+D, plantillas, procedimientos y procesos, así como los resultados totales y/o parciales de los mismos.

c) Información comercial, relación de clientes y/o fondo de comercio de la ORGANIZACIÓN incluyendo los datos de identificación de dichos contactos, como, por ejemplo, correo electrónico, teléfono, dirección, etc., así como cualesquiera estrategias comerciales, estudios de mercado e información análoga.

d) Información de la ORGANIZACIÓN relativa a las propuestas de servicios, tarifas, forma de confección o criterios de rentabilidad internos usados para llegar a las mismas; todo tipo de información fiscal, contable, financiera y salarial, incluyendo balances, estudios de viabilidad, estructura, y composición organizativa de la ORGANIZACIÓN, así como la existencia por parte de la ORGANIZACIÓN de acuerdos y/o contratos con terceros, siempre que estos datos e informaciones no sean públicos.

e) Los datos de carácter personal que trate la ORGANIZACIÓN o en su caso los que esta tenga acceso como consecuencia de un tratamiento por cuenta de terceros.

f) El código fuente de los programas informáticos, así como sus manuales y comentarios que en su caso le acompañen. Los códigos de activación de los programas informáticos de los que la ORGANIZACIÓN pudiera ser titular o licenciataria.

g) Los datos de acceso a los servicios puestos a disposición de la ORGANIZACIÓN, como, por ejemplo, bases de datos.

h) Cualquier tipo de información y/o dato sobre el que la ORGANIZACIÓN le haya comunicado a la PERSONA su carácter confidencial.

3.- <u>Exclusiones</u>: Queda excluida del concepto de Información Confidencial aquella información que:

a) Hubiera sido bien conocida por la PERSONA con anterioridad a su incorporación a la ORGANIZACIÓN, o bien con posterioridad a dicha incorporación por terceros que no tengan obligación de confidencialidad, en ambos casos por un medio legítimo siempre.

b) Sea de carácter público en el momento de tener acceso o recibirla de la ORGANIZACIÓN, siempre y cuando el carácter público de la información no haya sido provocado por una infracción de las obligaciones contenidas en el presente Contrato.

c) La ORGANIZACIÓN expresamente y por escrito decida dispensar de dicha obligación a la PERSONA.

4.- <u>Obligaciones de la PERSONA respecto a la Información Confidencial:</u>

a) Guardar absoluto y total secreto sobre la misma, no procediendo a su comunicación en todo o en parte a terceros. La PERSONA únicamente podrá comunicar Información Confidencial, siempre y cuando dicha comunicación sea necesaria para el correcto cumplimiento y desarrollo de las funciones que le hayan sido encomendadas por la ORGANIZACIÓN y dicha comunicación no vulnere ninguna obligación legal ni contractual de confidencialidad.

b) Utilizar la Información Confidencial única y exclusivamente en el marco de la Relación existente con la ORGANIZACIÓN, y una vez finalice ésta, a devolver toda la Información Confidencial que en su caso albergue ya sea en formato papel o electrónico y en todo caso, antes de su salida efectiva de la ORGANIZACIÓN, y si ello no fuera posible, a la mayor brevedad posible desde que conozca la extinción de la Relación.

c) Cumplir las medidas de seguridad técnicas, legales y organizativas que la ORGANIZACIÓN haya dispuesto y le haya comunicado para evitar la alteración y pérdida de la Información Confidencial, así como aquellas que en su caso sean razonables y oportunas para garantizar la confidencialidad y el acceso no autorizado por terceros, en especial cuando (i) la información esté bajo su custodia fuera de las instalaciones de la ORGANIZACIÓN y/o (ii) acceda remotamente por medios telemáticos a la misma.

5.- <u>Duración</u>: El presente compromiso de confidencialidad se mantendrá en vigor durante toda la vigencia de la Relación que une a las partes, así como de manera indefinida una vez sea extinguida dicha Relación por cualquiera de las partes, cualquiera que sea la causa que la motive.

ANEXO III

POLÍTICA DE DISPOSITIVOS DIGITALES
| NORMAS DE USO E INDICACIONES DE SEGURIDAD |

1.-ÁMBITO DE APLICACIÓN.

La presente Política de uso de dispositivos digitales comprende las normas y condiciones de utilización de los servicios, recursos, dispositivos y medios digitales contratados, propiedad o en posesión de la ORGANIZACIÓN, que le hubieran sido facilitados o puestos a disposición de la PERSONA en el marco de la Relación que une a las Partes.

Sin ánimo limitativo, por "Medios Digitales" se entenderá tanto los recursos de tipo hardware (ordenadores, portátiles, impresoras, elementos de red, discos duros etc.), software (sistemas operativos, cliente de correo, navegador, etc.) como servicios (compartición de ficheros, redes sociales, correo, comunicaciones, etc).

2.-PROHIBICIÓN DE USO PRIVADO SALVO AUTORIZACIÓN EXPRESA.

2.1.- La totalidad de los Medios Digitales tienen la consideración de recursos de trabajo. La PERSONA queda advertida de la prohibición expresa de utilización de tales Medios Digitales **para fines ajenos al cumplimiento de sus obligaciones y funciones, no pudiendo en consecuencia utilizar los Medios Digitales para un uso personal o privado, salvo que dicha posibilidad esté prevista en la presente política.**

2.2. Se entenderá que una utilización de los recursos es contraria a la presente política cuando dicho uso:

- pueda contemplar un riesgo para la seguridad informática de la ORGANIZACIÓN en especial si pudiera afectar a la integridad, disponibilidad y confidencialidad.
- afecte, limite o altere el uso de otros usuarios, por ejemplo, mediante el consumo del ancho de banda.

2.3. La PERSONA no podrá poner a disposición o dar acceso a ningún tercero ajeno a la ORGANIZACIÓN a los recursos o informaciones ubicados en los Medios Digitales.

2.4. Queda terminantemente prohibido la detención, des habilitación, desinstalación o bloqueo de servicios y/o programas con los que la ORGANIZACIÓN haya equipado los Medios Digitales, en especial, software de antivirus, firewall, contraseñas y programas o servicios de monitorización y seguimiento de la actividad en el sistema.

2.5.- Los fallos o vulnerabilidades que puedan existir tanto en el hardware como en el software, incluyendo al respecto la ausencia o deficiente configuración de los mismos, no podrán servir de base para una utilización contraria a las presentes directrices, quedando por tanto prohibido su aprovechamiento.

3.-INDICACIONES DE SEGURIDAD.

3.1- SISTEMAS DE IDENTIFICACIÓN: NOMBRE DE USUARIO Y CONTRASEÑA.

- Los sistemas de identificación en los sistemas y servicios son de carácter personal e intransferible.
- En el caso de que el sistema esté basado en un nombre de usuario y contraseña, la PERSONA deberá elegir una contraseña (y en su caso un nombre de usuario) que sea compatible con los requisitos de seguridad establecidos.
- Queda prohibido que la PERSONA utilice la dirección de correo electrónica corporativa para darse de alta en cualquier servicio o portal ajeno a la ORGANIZACIÓN y a la reutilización de las contraseñas en otro tipo de sistemas, páginas web, servicios, etc. ya sean personales, de la propia ORGANIZACIÓN, como de terceros.

- Queda prohibida la revelación de la/s contraseña/s a cualquier tercero, sea personal de la ORGANIZACIÓN o no, sin la autorización expresa de la ORGANIZACIÓN. En el caso de que la contraseña sea conocida fortuita o fraudulentamente por terceros no autorizados, la PERSONA deberá comunicarlo de manera inmediata a la ORGANIZACIÓN para proceder a su cambio y para que se adopten las medidas de seguridad oportunas.

- La PERSONA no podrá en ningún caso autenticarse en el sistema con credenciales de otro usuario salvo que esté expresamente autorizada por la ORGANIZACIÓN o sea personal informático realizando funciones de mantenimiento, supervisión, configuración o similares de la infraestructura.

- Las contraseñas o sistemas de cifrado que la PERSONA pueda utilizar para el acceso y/o utilización de los Medios Digitales, no están implementadas para garantizar la privacidad de la utilización y acceso a los Medios Digitales ni de la información personal o profesional que pueda ser albergada en dichos Medios Digitales, sino como una garantía de seguridad informática.

3.2 ACCESO A LA INFORMACIÓN.

La PERSONA deberá acceder únicamente a la información que sea necesaria para el desarrollo de las funciones encomendadas. La mera posibilidad técnica de acceso a más información de la que pueda necesitar, no legitima dicho acceso. A los efectos oportunos se informa de la monitorización y registro de todos los accesos y usos que pudieran realizarse de la información.

3.3. EXTRACCIÓN DE INFORMACIÓN Y SALIDA DE SOPORTES.

La PERSONA deberá solicitar autorización para cualquier extracción de información o recurso (memoria USB, portátil, etc.) de la ORGANIZACIÓN. En el caso de que se le conceda dicha autorización, la PERSONA deberá extremar las medidas de seguridad y vigilancia fuera de las instalaciones y en caso de pérdida o sustracción del recurso, deberá ponerlo inmediatamente en conocimiento de la ORGANIZACIÓN.

3.4. UTILIZACIÓN DE RECURSOS AJENOS A LA ORGANIZACIÓN.

La PERSONA deberá solicitar autorización para la utilización o conexión de cualquier recurso o medio informático ajeno a la ORGANIZACIÓN. En especial, deberá abstenerse de conectar equipos ajenos a la red interna y/o conectar los recursos de la ORGANIZACIÓN a redes inalámbricas públicas o con una seguridad deficiente.

3.5. INCIDENTES DE SEGURIDAD: BRECHAS DE SEGURIDAD.

La PERSONA deberá notificar a la ORGANIZACIÓN cualquier incidente de seguridad del que pueda tener conocimiento que tenga relación con los Medios Digitales de la ORGANIZACIÓN.

4.-NORMAS DE USO DE DETERMINADOS RECURSOS

4.1.- SERVICIO DE CORREO ELECTRÓNICO.

4.1.1.-GENERALIDADES.

El correo electrónico y los servicios dependientes de éste, como calendario, contactos, y en su caso almacenamiento asociados, **tienen la consideración de un medio de trabajo y en ningún caso se facilitan para fines particulares**, debiendo destinarse por tanto a un uso profesional en el marco de la Relación existente.

4.1.2.-CORREO EN MOVILIDAD/DESDE EL EXTERIOR.

Será necesaria autorización expresa de la ORGANIZACIÓN para la descarga y/o sincronización del correo en dispositivos móviles, tales como, portátiles, tablets o teléfonos móviles con independencia de la titularidad de los mismos.

4.1.3.- ACCESOS AL BUZÓN.

La ORGANIZACIÓN, en el caso de (i) ausencia, (ii) baja laboral, (iii) vacaciones o (iv) negativa de la PERSONA a dar acceso al buzón, podrá en los casos en los que legalmente proceda:

- Insertar un mensaje de autorrespuesta, en el caso de que no lo haya hecho la PERSONA, o el que haya insertado no se ajuste al modelo y/o instrucciones establecidas por la ORGANIZACIÓN. El mensaje a insertar informará de que la cuenta de correo no va a ser atendida, según modelo establecido por la ORGANIZACIÓN.

- Acceder a buzón de correo asignado a la PERSONA, incluyendo los mensajes de correo electrónico almacenados, o no leídos que sean profesionales, contactos, etc. en el caso de que la PERSONA no esté atendiendo la cuenta de correo durante su ausencia o sea necesario acceder a determinada información a juicio de la ORGANIZACIÓN para seguir prestando los servicios, realizar labores de mantenimiento informático y finalmente, verificar el cumplimiento de la presente política de uso de medios digitales, acuerdo de confidencialidad y/o desempeño en el trabajo.

Una vez finalizada la Relación existente entre la ORGANIZACIÓN y la PERSONA, la ORGANIZACIÓN entre otras acciones podrá, respetando los límites marcados por la normativa :

a) Acceder al contenido del buzón, en los casos que legalmente proceda.

b) Eliminar cuando lo estime oportuno el buzón.

4.1.4.-FIRMA CORPORATIVA EN LOS CORREOS.

La PERSONA deberá utilizar la firma o firmas de correo facilitadas por la ORGANIZACIÓN.

4.1.6.- MENSAJES NO SOLICITADOS.

Queda prohibido el envío de mensajes de correo electrónico de forma masiva y/o con fines comerciales o publicitarios**.**

4.3.7.- ACCESO CORREO ELECTRÓNICO DE TERCEROS.

Queda prohibido intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios. Sin perjuicio de las consecuencias que en el orden laboral pueda tener esta conducta, la PERSONA queda advertida de que dichas acciones pueden ser constitutivas de un delito contra la intimidad del artículo 197 del Código Penal.

4.2.-NAVEGACIÓN.

4.2.1.-La navegación web deberá emplearse única y exclusivamente en el ámbito de las funciones y tareas a desarrollar por la PERSONA en la ORGANIZACIÓN. La navegación no amparada en alguno de los casos descritos en los apartados anteriores, será considerada contraria a la presente política y por tanto no autorizada.

4.3.-TELÉFONOS MÓVILES.

El teléfono móvil deberá emplearse única y exclusivamente en el ámbito de las funciones y tareas a desarrollar. No se permite la realización de llamadas telefónicas personales desde el terminal proporcionado por la ORGANIZACIÓN siendo la PERSONA responsable del costo que la utilización de los servicios de datos o llamadas desde el extranjero se puedan generar.

La PERSONA deberá tener el software del terminal totalmente actualizado, debiendo instalar a la mayor brevedad las actualizaciones tanto del sistema operativo como de las aplicaciones que se vayan liberando por los diferentes fabricantes.

La PERSONA deberá establecer una contraseña de acceso al terminal, que deberá cambiar regularmente, al menos una vez cada trimestre.

4.4.-CERTIFICADOS DIGITALES.

La PERSONA debe utilizar el certificado electrónico que en su caso sea proporcionado por la ORGANIZACIÓN única y exclusivamente para el cumplimiento de sus obligaciones laborales. En ese sentido no podrá emplear el mismo para acceder a servicios, páginas web, firmar documentos, cifrar información, etc., que no guarden relación con las funciones.

5.- SISTEMAS DE CONTROL.

5.1.- La PERSONA queda advertida de la existencia de sistemas que registran de manera automática y en algunos casos de manera imprescindible gran parte de la actividad generada por los Medios Digitales, como por ejemplo, el proxy, controlador de dominio, servidor de impresión e impresoras, servidor de DNS, servicio de correo, sistema de filtrado antispam y antivirus, firewall perimetral, etc. que pueden registrar la actividad y usos de las herramientas informáticas empleadas por la PERSONA, como por ejemplo:

- Detalles de la navegación (como por ejemplo páginas visitadas, frecuencia, tiempo de permanencia…)
- Detalles de impresión de ficheros (fecha, nombre del fichero…)
- Uso de la red: ip origen/destino y protocolo empleado para la comunicación de información.

- Flujo de envío y recepción de los correos electrónicos; detalles de la comunicación, tales como destinatario, asunto…
- Inicio, tiempo de sesión, recursos accedidos.
- Detalles de los ficheros accedidos en los servidores, como, por ejemplo, número de ficheros, acciones realizadas sobre los mismos (como copia, lectura, modificación etc.)
- Detalle de las llamadas efectuadas desde terminales de la ORGANIZACIÓN (datos de origen-destino de las llamadas, así como su duración).

El listado anteriormente facilitado no es exclusivo y pueden existir otro tipo de registros automáticos no programados que registren la actividad de los Sistemas Informáticos.

5.2.- Duración de la conservación de los registros: los registros indicados en el punto anterior se mantendrán almacenados hasta la expiración de la prescripción de las acciones que pudieran existir derivadas de la Relación.

6.- SUPUESTOS QUE LEGITIMAN EL ACCESO.

6.2.-La ORGANIZACIÓN podrá controlar y/o acceder a los Medios Digitales que utilice la PERSONA por ejemplo mediante (i) el acceso a los registros generados por los servicios, servidores o programas; y/o (ii) el acceso a dichos recursos o la información que tratan en los siguientes supuestos:

- Cuando la ORGANIZACIÓN tenga indicios de cualquier ilícito, transgresión de la buena fe contractual del contrato que une a las Partes o de la presente política de uso de Medios Digitales.

- Cuando se presente cualquier tipo de problema o incidencia de tipo de informático, ya sea a nivel de software o de hardware cuya solución precise dicho acceso o control, específicamente en caso de existencia de virus, troyanos o gusanos informáticos.

- Para la realización de operaciones de mantenimiento, configuración, instalación de nuevas aplicaciones, etc., que la ORGANIZACIÓN estime como oportunas de cara a la finalidad de las herramientas y servicios regulados en las presentes directrices.

- Con ocasión de la aplicación de la normativa de protección de datos y en concreto, con la aplicación de las medidas de seguridad que se puedan definir por parte de la ORGANIZACIÓN en base al análisis de riesgo.

7.-AUTORIZACIONES Y PERMISOS.

7.1.- Las autorizaciones y permisos a las que hacen referencia la presente Política de Medios Digitales podrán ser otorgadas por cualesquiera miembros de (i) Dirección de la ORGANIZACIÓN o del (ii) Departamento de Informática de la ORGANIZACIÓN.

8.-CONSECUENCIAS DE LA VIOLACIÓN DE LAS NORMAS.

8.1.- La violación de las presentes directrices será considerada una utilización fraudulenta de los medios de trabajo que quiebra la buena fe y la diligencia exigible, por lo que puede ser sancionada con las medidas disciplinarias establecidas en el Convenio Colectivo y Estatuto de los Trabajadores, pudiendo incluso ser causa de rescisión del contrato de trabajo, así como la responsabilidad civil y penal que pudiera derivarse de ese incorrecto uso.

ANEXO IV: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección del Grupo Cosmos XXI ha establecido los principios y directrices con los que Grupo Cosmos XXI protegerá su información, de conformidad con la normativa aplicable y con sus valores éticos, así como con lo previsto en el Reglamento del Comité de Seguridad de la Información y en otra normativa interna que resulte de aplicación.

PRINCIPIOS GENERALES

- Clasificación de la Información. La Información se clasificará en función a su valor, importancia y criticidad para el negocio, de forma que las medidas de protección se adecúen al nivel de clasificación de cada activo de información. Del mismo modo, la clasificación de los activos de Información se realizará tomando en consideración los requisitos legales, operacionales y las buenas prácticas y estándares al respecto.
- Uso de los Sistemas de Información. El uso de los Sistemas estará limitado a fines lícitos y exclusivamente profesionales, para la realización de tareas relacionadas con el puesto de trabajo. En consecuencia, estos medios y sistemas no están destinados para uso personal ni podrán utilizarse para ninguna finalidad ilícita.
- Segregación de funciones. Se deberán evitar las concentraciones de riesgos derivados de la ausencia de segregación de funciones y la dependencia unipersonal de funciones críticas para el negocio.

  En este sentido, se deberán establecer procedimientos formales para controlar la asignación de privilegios a los Sistemas de Información, de forma que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.
- Retención de la Información. Se establecerán, cuando resulte necesario o conveniente, períodos de retención de la Información por categorías atendiendo a las necesidades operativas o de cumplimiento regulatorio, así como los correspondientes procedimientos de destrucción de la Información.
- Acceso a la Información por parte de terceros. Se desarrollarán los procedimientos de control de la puesta a disposición y acceso por terceros a la Información relativa a Grupo Cosmos XXI o de cualesquiera otros terceros relacionados con el Grupo.
- Seguridad de la Información en los Sistemas. Los entornos de desarrollo y producción se mantendrán en Sistemas independientes. Igualmente, el desarrollo y mantenimiento de los Sistemas de Información deben incluir los controles y registros necesarios para garantizar la correcta implementación de las especificaciones de seguridad.
- Continuidad. Se establecerá un proceso de gestión de continuidad que permita garantizar la recuperación de la Información crítica para el Grupo en caso de desastre, reduciendo el tiempo de indisponibilidad a niveles aceptables.
- Cumplimiento. Los Sistemas de Información y comunicaciones del Grupo deberán estar adecuados de forma permanente a las exigencias de la legislación vigente en todas las jurisdicciones en las que opera, así como a la normativa interna de desarrollo que resulte de aplicación.

La responsabilidad de la protección de la Información y de los Sistemas que la tratan, almacenan o transmiten se extiende a todos los niveles organizativos y funcionales de Grupo Cosmos XXI.

ANEXO V: GESTIÓN DE CONSENTIMIENTOS DE LA PERSONA.

SOLICITUD ENVÍO NÓMINAS POR CORREO ELECTRÓNICO

Don/Doña , NIF número , solicito que a partir de este momento se me remita la nómina a la siguiente cuenta de correo electrónico personal que he facilitado a la empresa (ACTUALIZACION DATOS PERSONALES) , a la que manifiesto tener acceso.

Política de Privacidad aplicable:

Responsable del tratamiento GRUPO COSMOS XXI, S,L sita en Pol. Industrial de Aoiz, s/n , con número de Telf.: +34 699 132 896 y dirección de correo electrónico info@gcosmos.com. El Responsable, cuenta con un Delegado de Protección de Datos con el que puede contactar a través de la siguiente dirección de correo electrónico: dpd@gcosmos.com.

Finalidad del tratamiento. Gestionar el envío de su nómina.

Legitimación legal del tratamiento. Consentimiento. Podrá retíralo si lo desea, momento en el cual la nómina le será remitida por un método alternativo. La retirada en ningún caso afectará a la licitud del tratamiento basado en el consentimiento previo a la retirada.

Plazo conservación. Mientras dure la relación laboral y una vez finalizada ésta mientras exista responsabilidad legal para Responsable en relación con el tratamiento.

Comunicaciones y/o transferencias. Salvo obligación legal, sus datos no serán comunicados a ningún tercero.

Derechos del titular de los datos. Tiene la posibilidad de ejercitar los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición. El ejercicio de los citados derechos podrá hacerse mediante solicitud dirigida por escrito al responsable en la dirección de correo electrónico info@gcosmos.com, en los términos que suscribe la legislación vigente. Asimismo, podrá presentar una reclamación ante la autoridad de control competente ejerciendo esa función en España la Agencia Española de Protección de Datos (www.aepd.es).

AUTORIZACIÓN PARA LA CAPTACIÓN DE DATOS BIOMÉTRICOS

Don/Doña , NIF número , informa que,

Habiendo sido informado/a de la posibilidad de acceder a las instalaciones a través de un sistema de datos biométricos (huella dactilar), solicito poder acceder a las instalaciones a través del mismo y, los efectos oportunos, presto mi consentimiento expreso para el tratamiento de mis datos con la finalidad recogida en la presente solicitud.

Que, en relación con los datos dactiloscópicos me han indicado que no será almacenada ni conservada una imagen de la huella, sino la captura digital de la misma basándose en sus características físicas, las cuales serán transformadas en un algoritmo que se asociará con mi persona. Siendo este algoritmo el que se conserve en las bases de datos.

Política protección de datos:

Responsable del tratamiento GRUPO COSMOS XXI, S,L sita en Pol. Industrial de Aoiz, s/n, con número de Telf.: +34 699 132 896 y dirección de correo electrónico info@gcosmos.com. El Responsable, cuenta con un Delegado de Protección de Datos con el que puede contactar a través de la siguiente dirección de correo electrónico: dpd@gcosmos.com.

Finalidad del tratamiento. Generar un perfil biométrico e incorporarlo a las bases de datos del sistema para permitir la identificación y el acceso a las instalaciones por parte del personal, así como para controlar el cumplimiento de las obligaciones derivadas de la relación laboral como la asistencia, los horarios, el absentismo laboral o la puntualidad del trabajador entre otros.
Legitimación legal del tratamiento. Consentimiento. Puede retirar el mismo en cualquier momento. La retirada en ningún caso afectará a la licitud del tratamiento basado en el consentimiento previo a la retirada.
Plazo conservación: Mientras dure la relación laboral y una vez finalizada ésta mientras exista responsabilidad legal para Responsable en relación con el tratamiento.
Comunicaciones y/o transferencias: Salvo obligación legal sus datos no serán comunicados y/o transferidos a ningún tercero.
Derechos del titular de los datos. Tiene la posibilidad de ejercitar los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición. El ejercicio de los citados derechos podrá hacerse mediante solicitud dirigida por escrito al responsable en la dirección de correo electrónico info@gcosmos.com, en los términos que suscribe la legislación vigente. Asimismo, podrá presentar una reclamación ante la autoridad de control competente ejerciendo esa función en España la Agencia Española de Protección de Datos (www.aepd.es).

UTILIZACIÓN IMAGEN DEL TRABAJADOR

Don/Doña , en nombre propio y con DNI , por la presente, autorizo a la empresa al registro de mi imagen por fotografía o vídeo y su uso para la siguiente finalidad:

☐ Publicación en la página web y Redes sociales.

☐ Noticias y actualidad de la Organización en medios informativos.

☐ Formaciones/charlas, etc., en las que pueda participar como ponente o público.

La autorización tendrá validez hasta que la persona firmante desee revocarla por escrito.

Política de Protección de Datos:

Responsable del tratamiento. GRUPO COSMOS XXI, S,L sita en Pol. Industrial de Aoiz, s/n, con número de Telf.: +34 699 132 896 y dirección de correo electrónico info@gcosmos.com. El Responsable, cuenta con un Delegado de Protección de Datos con el que puede contactar a través de la siguiente dirección de correo electrónico: dpd@gcosmos.com.

Finalidad del tratamiento. Gestión de la autorización y utilización de la imagen y/o voz en relación con las finalidades que se indican en el cuerpo de la autorización.

Legitimación legal del tratamiento. Consentimiento. Podrá retirar el consentimiento en cualquier momento sin que eso afecte a la legalidad del tratamiento anterior a la retirada del consentimiento.

Comunicaciones y/o transferencias: Sus datos personales (su imagen y/o voz) pueden ser compartidos con la generalidad del público tanto interno como externo mediante diversos medios.

Plazo conservación: Mientras se utilice el material en el que aparece el trabajador. O hasta que retire su consentimiento para el tratamiento de su imagen con esta finalidad.

Derechos del titular de los datos. Tiene la posibilidad de ejercitar los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición. El ejercicio de los citados derechos podrá hacerse mediante solicitud dirigida por escrito al responsable en la dirección de correo electrónico info@gcosmos.com, en los términos que suscribe la legislación vigente. Asimismo, podrá presentar una reclamación ante la autoridad de control competente ejerciendo esa función en España la Agencia Española de Protección de Datos (www.aepd.es).

ENVÍO DE COMUNICACIONES AL PERSONAL INTERNO

Don/ Doña , NIF número informo,

Que la empresa me ha informado de la posibilidad de que las comunicaciones internas relacionadas con mi trabajo dentro de la Organización o que me afecten como trabajador/a pueden ser enviadas a través del correo electrónico o el teléfono.

En este sentido, solicito que a partir de este momento las comunicaciones internas sobre mi trabajo o que me afecten como trabajador/a de la Organización (a modo de ejemplo: envío de la nómina, comunicación de eventos o envío de los planes y material formativo, etc.,) se realicen a través del correo electrónico personal facilitado a la empresa, medio al que manifiesto tener acceso.

Política de Protección de Datos:
Responsable del tratamiento. GRUPO COSMOS XXI, S,L sita en Pol. Industrial de Aoiz, s/n, con número de Telf.: +34 699 132 896 y dirección de correo electrónico info@gcosmos.com. El Responsable, cuenta con un Delegado de Protección de Datos con el que puede contactar a través de la siguiente dirección de correo electrónico: dpd@gcosmos.com.
Finalidad del tratamiento. Gestión de la autorización y utilización de la imagen y/o voz en relación con las finalidades que se indican en el cuerpo de la autorización.
Legitimación legal del tratamiento. Consentimiento. Podrá retirar el consentimiento en cualquier momento sin que eso afecte a la legalidad del tratamiento anterior a la retirada del consentimiento.
Comunicaciones y/o transferencias: Sus datos personales (su imagen y/o voz) pueden ser compartidos con la generalidad del público tanto interno como externo mediante diversos medios.
Plazo conservación: Mientras se utilice el material en el que aparece el trabajador. O hasta que retire su consentimiento para el tratamiento de su imagen con esta finalidad.
Derechos del titular de los datos. Tiene la posibilidad de ejercitar los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición. El ejercicio de los citados derechos podrá hacerse mediante solicitud dirigida por escrito al responsable en la dirección de correo electrónico info@gcosmos.com, en los términos que suscribe la legislación vigente. Asimismo, podrá presentar una reclamación ante la autoridad de control competente ejerciendo esa función en España la Agencia Española de Protección de Datos (www.aepd.es).

CONSENTIMIENTO VIGILANCIA DE LA SALUD

Don/Doña , con D.N.I. , trabajador de la empresa GRUPO COSMOS XXI, S.L, tras ser informado/a del derecho a la participación en la vigilancia periódica de mi estado de salud, de acuerdo con el Artículo 22.1 de la Ley de Prevención de Riesgos Laborales 31/1995, de 8 de noviembre, manifiesto mi consentimiento para la realización del examen de salud específico de Vigilancia de la Salud.

En la medida en que para la realización de dicho examen es necesario que se traten mis datos de carácter personal, autorizo y consiento a la empresa para el tratamiento de mis datos con la finalidad especificada, sin que en este sentido la empresa pueda acceder o tratar mis datos de salud, estando únicamente legitimado para dicho tratamiento la empresa encargada de las labores de vigilancia de la salud.

Política de Protección de Datos:

Responsable del tratamiento. GRUPO COSMOS XXI, S,L sita en Pol. Industrial de Aoiz, s/n, con número de Telf.: +34 699 132 896 y dirección de correo electrónico info@gcosmos.com. El Responsable, cuenta con un Delegado de Protección de Datos con el que puede contactar a través de la siguiente dirección de correo electrónico: dpd@gcosmos.com.

Finalidad del tratamiento. Gestión de la autorización y utilización de la imagen y/o voz en relación con las finalidades que se indican en el cuerpo de la autorización.

Legitimación legal del tratamiento. Consentimiento. Podrá retirar el consentimiento en cualquier momento sin que eso afecte a la legalidad del tratamiento anterior a la retirada del consentimiento.

Comunicaciones y/o transferencias: Sus datos personales (su imagen y/o voz) pueden ser compartidos con la generalidad del público tanto interno como externo mediante diversos medios.

Plazo conservación: Mientras se utilice el material en el que aparece el trabajador. O hasta que retire su consentimiento para el tratamiento de su imagen con esta finalidad.

Derechos del titular de los datos. Tiene la posibilidad de ejercitar los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición. El ejercicio de los citados derechos podrá hacerse mediante solicitud dirigida por escrito al responsable en la dirección de correo electrónico info@gcosmos.com, en los términos que suscribe la legislación vigente. Asimismo, podrá presentar una reclamación ante la autoridad de control competente ejerciendo esa función en España la Agencia Española de Protección de Datos (www.aepd.es).