POLÍTICA SOBRE USO DE SISTEMAS DE INFORMACION

El Consejo de Administración de Barna Steel, S.A., en representación de la totalidad del Grupo Celsa ("**Celsa Group**" o la "**Compañía**"), en el marco de su competencia general e indelegable de determinar las políticas y estrategias generales de Celsa Group, ha aprobado la presente *Política sobre el uso de sistemas de información* (en adelante, la "**Política**").

I. Finalidad

La generalización de la informática y los flujos de información son factores que hacen cada vez más necesario contar con una adecuada red de comunicaciones interna y externa en la empresa, y ello exige establecer medidas para la protección del patrimonio empresarial y el correcto desempeño de la actividad productiva. Las normas de operativa interna de Celsa Group establecen que los medios informáticos y demás medios que la entidad aporta, se facilitan como medios de trabajo. Todo usuario se obliga a utilizar la red corporativa de Celsa Group y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la Compañía o de terceros, o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.

La finalidad de esta Política es asegurar que los medios tecnológicos son utilizados adecuadamente, establecer claras reglas sobre el posible uso para fines personales tanto del correo electrónico, de internet y de otras facilidades como los teléfonos, en la oficina o de forma remota, e informar a los usuarios sobre la monitorización de estas actividades y de las razones para hacerlo. Cualquier violación de la Política podría ser considerada como falta y conducir a la acción disciplinaria correspondiente. Aquel profesional que no esté seguro acerca de si algo que se proponga hacer puede ser susceptible de atentar contra esta Política debería buscar el consejo de su responsable o consultarlo al responsable de IT ServiceDesk o al Comité de Ética y Cumplimiento Normativo.

II. Ámbito de aplicación

Esta Política es de aplicación a Celsa Group y a todas las sociedades que integran su Grupo, atendiendo a sus características propias. Celsa Group promoverá el alineamiento de las políticas de las sociedades que integran su Grupo con la presente Política. En el caso de las actividades que Celsa Group realice fuera de España, esta Política se adaptará a la legislación local más restrictiva que, en su caso, resulte de aplicación.

III. Principios Generales

Mediante esta Política, Celsa Group asume y promueve los siguientes principios generales que deben guiar todas sus actividades:

a) Dirigir nuestros esfuerzos a la prevención de errores, así como a su corrección, control y gestión.

b) Impulsar la formación continua y la concienciación en materia de seguridad de la información.

c) Asegurar que la Compañía cumple con los requisitos establecidos por la legislación en materia de seguridad de la información.

d) Establecer acciones sistemáticas de control, monitorización y prevención de incidentes.

e) Garantizar la confidencialidad y autenticidad de la información, protegiendo los datos y los sistemas de información contra accesos indebidos, ciberataques y modificaciones no autorizadas.

f) Actuar de manera adecuada y conjunta para prevenir, detectar y responder a los ciber incidentes que pudieran afectar a la seguridad de la información.

IV. Contenidos Generales

a) Identificadores de usuario y contraseñas

La mayoría de los sistemas de información de Celsa Group precisan del uso de contraseñas. Todo usuario se compromete a no comunicar a otra persona su identificador y clave de acceso a los sistemas de información de Celsa Group. Si sospechase que otra persona conoce sus datos de identificación y acceso deberá cambiar su contraseña. El usuario será el único responsable de los actos realizados con su identificador de usuario.

IT ServiceDesk prestará la asistencia necesaria para la gestión de sus contraseñas. En este sentido, todo usuario deberá cambiar la contraseña de cualquier equipo informático o dispositivo de telefonía móvil de manera periódica, así como establecer una contraseña suficientemente segura.

b) Uso del ordenador

Los ordenadores de sobremesa o portátiles serán utilizados exclusivamente para fines del negocio, sujeto a las siguientes excepciones:

Los usuarios podrán realizar un uso limitado de los ordenadores de la Compañía para el envío de correos electrónicos de carácter personal, fuera de su jornada laboral o bien durante los periodos de descanso dentro de su jornada y siempre de acuerdo con la Política. En el asunto del mensaje, debe figurar la palabra "Personal".

Los usuarios podrán hacer uso limitado de los ordenadores de la Compañía para la navegación por internet con fines personales, fuera de su jornada laboral o bien durante los periodos de descanso dentro de su jornada y siempre de acuerdo a todos los términos del Reglamento de desarrollo de esta Política.

El mal uso de internet y de correo electrónico puede acarrear serios riesgos para las compañías de Celsa Group como la introducción de virus, infracción de leyes sobre copyright o imputación o difamación de terceros. Por otra parte, el correo electrónico, frecuentemente visto como un método informal de comunicación, debe ser considerado de forma equivalente a una carta en papel oficial de la Compañía. El uso descuidado del correo electrónico de la Compañía o de internet pueden tener serias consecuencias y por ello, la Compañía impone estrictos límites en relación al uso profesional o personal.

La Compañía se reserva el derecho de denegar este permiso de uso para fines personales en casos particulares si así lo considera oportuno.

c) Virus

El usuario está obligado a permitir la actualización por parte del Servicio Técnico (IT ServiceDesk) de cualquier sistema antivirus, a colaborar en su mantenimiento y actualización para prevenir la entrada de cualquier elemento que pueda destruir o corromper la información o datos de la red de Celsa Group.

El usuario no debe conectar ningún ordenador o portátil de la Compañía en redes claramente no seguras, ni debe instalar dispositivos 4G de acceso a internet sin autorización pues se podría causar una brecha en la seguridad de los sistemas con el riesgo de la introducción de virus y otros tipos de malware. La vulneración de esta regla podría llegar a considerarse como falta grave.

d) Correo electrónico

Todas las comunicaciones que se realicen por los profesionales de Celsa Group en el ámbito de su responsabilidad por cualquier medio deberán respetar los principios éticos establecidos por Celsa

Group, incluyendo por supuesto las comunicaciones realizadas vía correo electrónico.

Los usuarios no deben enviar, reenviar, distribuir o retener mensajes de correo electrónico que contengan un lenguaje abusivo, agresivo u ofensivo. Cuando redacte un correo, el usuario se compromete a no hacer uso de expresiones que se consideren inapropiadas en referencia a cuestiones de carácter personal y en especial sobre raza, color, religión, creencias, género, edad, nacionalidad, orientación sexual o discapacidad, ni tampoco los que contengan o impliquen actitudes de acoso laboral o sexual. De la misma manera, no debe reenviar o distribuir aquellos que las contengan.

El rendimiento de las redes de Celsa Group puede verse afectado por el envío de grandes ficheros adjuntos en los correos electrónicos como videoclips, imágenes de gran tamaño o en gran cantidad, por correos basura o spam, por falsas alarmas sobre virus (hoax), por mensajes en cadena o piramidales, y por otros tipos de mensajes que se envían y reciben que no atienden a la operativa propia del negocio.

En este sentido, los usuarios deberán borrar sus comunicaciones electrónicas y archivos adjuntos una vez transcurrido un tiempo prudencial y constatada, bien su nula utilidad, bien la innecesaridad de su almacenamiento en los equipos de la Compañía. Celsa Group se reserva el derecho de monitorizar el rendimiento de sus redes, pudiendo eliminar aquellos elementos cuyo almacenamiento no se repute necesario o pudiendo recuperar aquellos archivos incorrectamente eliminados, en el caso de que cualquiera de ambas actuaciones se considere pertinente.

Los usuarios no deben generar ni enviar correos que no estén relacionados con su actividad profesional en la Compañía y deben exigir a su vez a todos los demás usuarios ese mismo comportamiento.

Los usuarios no podrán utilizar cuentas de correo electrónico con nombres de dominio propiedad de Celsa Group en sus actividades personales en la red, así como tampoco registrarse en redes sociales, servicios online u otros recursos no profesionales con estos usuarios.

Los usuarios no podrán utilizar contraseñas utilizadas previamente en Celsa Group en sus actividades personales en la red, así como tampoco en redes sociales, servicios online u otros recursos no profesionales

e) Navegación por Internet

Los usuarios no deben, bajo ninguna circunstancia, acceder a contenidos web de carácter inapropiado u ofensivo, ni almacenar o distribuir semejante material hacia internet o por correo electrónico utilizando los ordenadores de la Compañía. Como ejemplo de contenido inapropiado u ofensivo se incluye material sobre racismo, pornografía, imágenes de todo tipo con contenido explícitamente sexual, así como textos y otros materiales relacionados, promoción de actividades ilegales, de intolerancia con

otros, de juegos o apuestas en la red.

f) Uso de dispositivos de telefonía de empresa para uso particular

Esta Política es de aplicación tanto a las líneas fijas como a los móviles o dispositivos 4G. Los usuarios pueden utilizar los teléfonos de la Compañía a modo particular sólo en caso de emergencia o para llamadas esenciales cuya autorización se debería solicitar en primera instancia a su mando inmediato superior.

Para uso particular, no está permitido el uso de servicios que generen un coste adicional para la Compañía, como llamadas a líneas de chat, suscripciones por SMS, etc., así como la utilización de servicios con coste asociado a través de los dispositivos 4G de la Compañía.

El uso de los dispositivos de telefonía de empresa tiene, además de las limitaciones expuestas en este apartado, todas la que les sean de aplicación referidas a las funciones similares que se pueden ejecutar en teléfonos "Smart" y que asimilan los mismos a ordenadores y pcs, así como las relativas a virus informáticos, correo electrónico y cualquier otra que sea asimilable por su naturaleza.

g) Protección de dispositivos portátiles de empresa; ordenadores, smartphones, tablets u otros

Con el fin de proteger la información y dispositivos propiedad de Celsa Group, todos los dispositivos móviles tendrán implantado un sistema de gestión en remoto (MDM) que permite entre otras cosas; protegerlos de ataques externos, en particular ciberataques, instalar aplicaciones de trabajo en remoto, dar soporte en remoto y aplicar configuraciones automáticas como el correo electrónico corporativo. En cualquier caso, la gestión y tratamiento de la herramienta MDM será controlada por el departamento de IT para las finalidades anteriormente descritas, conforme a las disposiciones legales en vigor.

h) Geolocalización de dispositivos

Los usuarios son conscientes de que los dispositivos de titularidad de la empresa pueden estar dotados de sistemas de geolocalización. La instalación de estos dispositivos tiene como finalidad primordial su utilización en casos de emergencia del usuario, tales como accidentes, así como su recuperación en casos de extravío o sustracción de los equipos. La activación del protocolo de actuación en estos casos será autorizada expresamente por el Chief People & Organisation Officer.

i) Uso de teléfono móvil particular en horario de trabajo

El uso del teléfono particular durante las horas de trabajo ha de ser lo mínimo posible, la regulación detallada de su uso se establecerá en el Reglamento de desarrollo de esta Política.

j) Monitorización de las comunicaciones

La Compañía puede guardar registro y auditar el uso de los teléfonos, fijos y móviles, máquinas de fax, ordenadores u otros dispositivos propiedad de la Compañía, incluyendo los sistemas de correo electrónico, internet y otros sistemas, fijándose su regulación en el Reglamento de desarrollo de la presente Política.

En el supuesto hecho de existir suficientes indicios o sospechas sobre la comisión de un ilícito o conductas contrarias a las normas, principios o Código Ético y de Conducta Profesional de Celsa Group, la Compañía podrá guardar registro y monitorizar las llamadas de teléfono, faxes, ficheros de ordenador y uso de internet así como correos electrónicos enviados, recibidos y almacenados, todo ello con las limitaciones y salvaguardas legales que prevea la normativa aplicable, previa autorización del Chief People & Organisation Officer.

Todos los usuarios serán informados del contenido de esta Política y de su Reglamento de desarrollo a fin de que sean conocedores de estas posibilidades de monitorización.

k) Redes Sociales

Las normas de la presente Política y de su Reglamento referidas al uso de los equipos informáticos, correos y navegación por internet son plenamente aplicables al acceso de los usuarios a las redes sociales en tiempo de trabajo y/o con los medios o equipos de titularidad de la empresa.

V. Contenidos Específicos contrarios a esta Política

Las siguientes practicas se considerarán contrarias a la presente Política y su Reglamento de desarrollo atendiendo a la peligrosidad de las mismas para la integridad de la seguridad de los sistemas de información de Celsa Group. Siendo tales prácticas consideradas como faltas graves o muy graves en atención al alcance de las mismas.

1. Permitir el uso de un ordenador de la Compañía a alguien ajeno a la misma, es decir, que no sea profesional directa o indirectamente de alguna empresa de Celsa Group.
2. Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la entidad o de terceros.

3. Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otro usuario.
4. Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Celsa Group.
5. Intentar aumentar el nivel de sus privilegios o de otro usuario en el sistema.
6. Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de Celsa Group.
7. El acceso a debates en tiempo real (Chat/IRC) por ser especialmente peligrosos, pues se facilita la instalación de utilidades que permiten accesos no autorizados al sistema.
8. Utilizar receptores de radio/TV en los ordenadores de la Compañía. El uso de receptores de TV es ilegal sin una licencia de TV en algunos países.
9. Introducir datos en los ordenadores de la Compañía desde dispositivos personales como "USB memory sticks", "pen drives", tarjetas SD o similares, especialmente en los entornos industriales.
10. Introducir voluntariamente programas, virus, macros, applets, controles Active X o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros.
11. Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por IT Celsa Group, o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
12. Introducir contenidos obscenos, inmorales, ofensivos, racistas o discriminatorios, de acuerdo a las leyes vigentes en los países en los que Celsa Group está presente.
13. Borrar cualquiera de los programas instalados legalmente.
14. Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de Celsa Group, o de terceros.
15. Intentar distorsionar o falsear registros "LOG" del sistema.

VI. Confidencialidad de la información

Queda prohibido enviar información confidencial de Celsa Group al exterior, mediante soportes materiales, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.

El profesional, usuario de los sistemas de información corporativos, deberá guardar por tiempo indefinido la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con Celsa Group, tanto en soporte material como electrónico.

Ningún colaborador deberá poseer, para usos no propios de su responsabilidad, ningún material o información propiedad de Celsa Group.

El Reglamento de desarrollo de la presente Política regulará el detalle de la posesión temporal, uso y devolución de cualquier clase de información propiedad de Celsa Group y/o calificada como de confidencial.

La duración de las obligaciones de confidencialidad establecidas en el presente documento será indefinida, manteniéndose en vigor durante la vigencia de la relación laboral o contractual con Celsa Group y con posterioridad a su finalización.

El incumplimiento de esta obligación puede constituir un delito de revelación de secretos y dará derecho a Celsa Group a exigir al profesional una indemnización económica.

VII. Propiedad y Seguridad de la información

Las compañías de Celsa Group son las propietarias de la información y de los derechos de uso y explotación de programas de software y sistemas, equipos, manuales, informes y todos los documentos instalados en los equipos y dispositivos de su propiedad.

En ese sentido, todos los correos electrónicos, mensajes y documentos enviados y / o recibidos por los profesionales que usen el sistema de correo electrónico de la Compañía son considerados como propiedad de la Compañía. En el mismo sentido la totalidad de los archivos de cualquier índole que se encuentren alojados en su sistema informático y en su sistema de archivos.

Los profesionales no deben operar, reproducir, replicar o transferir los sistemas o aplicaciones que se utilizan en la organización para propósitos no relacionados con la Compañía. Además, están obligados a cumplir con todas las medidas y protocolos establecidos para el mantenimiento de la seguridad, control, acceso y uso de los sistemas establecidos en Celsa Group.

El puesto de trabajo estará bajo la responsabilidad del profesional autorizado, quien además garantizará que la información confidencial no pueda ser visible por personas no autorizadas. El Reglamento de desarrollo establecerá las medidas particulares en materia de uso de pantallas e impresoras a estos efectos.

VIII. Sistema de Gobierno de los sistemas de información

a) Comunicación de infracciones

El personal tanto interno como externo que por cualquier medio tenga conocimiento de la comisión de infracciones a lo dispuesto en la presente Política, así como de cualquier conducta que pueda infringir las normas legales y/o las normas éticas establecidas por Celsa Group deberá poner las mismas en conocimiento de los responsables a través de los canales de comunicación y denuncia puestos a su disposición en la intranet corporativa.

b) Protección de datos de carácter personal

Los profesionales usuarios de los servicios de información de Celsa Group deberán respetar en todo momento la Política de Protección de Datos. El Reglamento en desarrollo de esta Política, establecerá las obligaciones y responsabilidades que afectan a todo el personal que tenga a acceso a los sistemas de información y en particular a datos de carácter personal.

Especial mención a la prohibición expresa de:

1) Crear ficheros que contengan datos personales sin la autorización expresa del responsable del fichero.
2) Alterar la finalidad de cualquier fichero que contenga datos personales.

Esta Política sobre usos de Sistemas de Información ha sido aprobada por el Consejo de Administración de Barna Steel, S.A., en representación de la totalidad del Grupo Celsa el día 13 de Julio de 2023.