"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN"

CIRCET IBERIA S.L.U.(compuesta por CIRCET INFRAESTRUCTURA DE TELECOMUNICACIONES y SMARTEL) como empresa líder en infraestructuras de telecomunicaciones, ofrecemos a nuestros clientes servicios llave en mano de ingeniería, construcción, puesta en servicio, instalación y mantenimiento de redes de telecomunicaciones fijas y móviles, así como la venta, instalación y mantenimiento de los servicios a clientes finales, por todo somos conscientes de la importancia de cumplir con los requisitos de nuestros clientes para asegurar la plena satisfacción de los mismos, del personal de la organización y demás partes interesadas. Esta Política se establece como marco en el que se deben desarrollar todas las actividades de la organización de manera que se garantice a los clientes y demás partes interesadas el compromiso adquirido por nuestra entidad.

Por ello, asumimos la necesidad de seguir avanzando en el camino de la mejora continua y para ello hemos decidido implantar un Sistema de Gestión de la Seguridad de la Información en base a la norma UNE-EN ISO 27001 y conforme los siguientes principios:

- El cumplimiento de los requisitos exigidos por el cliente, los requisitos legales aplicables y otros requisitos que la organización suscriba en materia de Seguridad de la Información que afecten a nuestra actividad.

- Un esfuerzo para la mejora continua de identificación, evaluación y reducción de los riesgos de Seguridad de la Información que afecten a nuestra actividad.

- La Seguridad de la Información, constituye un elemento fundamental en el desempeño de nuestra actividad empresarial, comprometiéndonos al establecimiento de los mecanismos adecuados para asegurar la Confidencialidad, Integridad y Disponibilidad de los activos y asegurando la continuidad del negocio.

- El desarrollo de planes y programas que establezcan objetivos y metas, para garantizar la Seguridad de la Información, reducir las posibles vulnerabilidades y disminuir los impactos de los riesgos. El desarrollo de auditorías internas que permitan reducir riesgos y minimizar los efectos negativos sobre la Seguridad de la Información y controlar regularmente los avances y la eficacia de las medidas aplicadas, fomentando la mejora continua de los procesos y prácticas de la empresa.

- Establecer las medidas organizativas, técnicas y de control necesarias para el cumplimiento de las directrices de seguridad y evitar violaciones de la política de seguridad.

- Formar a los empleados en materia de Seguridad de la Información desarrollando planes de formación adecuados que garanticen su competencia profesional en el desarrollo de sus funciones.

- Asegurar que todas las actividades, productos y servicios se desarrollen en el marco establecido en la presente Política.

En este sentido, cada integrante de la organización tiene como una condición más de su trabajo el cumplir con los requisitos establecidos en materia de Seguridad de la Información y asegurar la satisfacción de nuestros clientes. Esta Política se encuentra a disposición del público o cualquier otra parte interesada y se revisa y actualiza para su continua adecuación.

Manuel Delgado Godino
Gerente de CIRCET IBERIA S.L.U.
24 de Julio de 2023

Revisión 01

Política de Teletrabajo

CIRCET IBERIA S.L.U. (compuesta por CIRCET INFRAESTRUCTURA DE TELECOMUNICACIONES y SMARTEL) ante el auge del teletrabajo ha decidido establecer una serie de medidas que permitan garantizar la seguridad, confidencialidad, integridad y disponibilidad de la información, activos, procesos, sistemas y redes. Para ello se establece esta Política, que es de obligado cumplimiento para todos los empleados y personal de CIRCET IBERIA, por lo que será comunicada y conocida por aquellas partes pertinentes al sistema y será revisada de forma periódica para verificar su cumplimiento y la efectividad de las medidas en ella indicadas.

- *Control de acceso remoto.*

El trabajador solo tendrá acceso a aquella información estrictamente necesaria para el desempeño de sus funciones. Para ello se controlará:

- Tipo de información que se usa o genera.
- Que trabajador tiene acceso a qué información (autenticación).
- Uso de red privada virtual (VPN).
- Autorización de acceso y uso de equipo.
- Y monitorización del comportamiento de los dispositivos, para determinar si se ajustan a los parámetros establecidos.

- *Autorización de uso de dispositivos y aplicaciones.*

Desde CIRCET IBERIA se establece que para la modalidad de teletrabajo solo se emplearán dispositivos corporativos, que contarán con medidas de seguridad que permitirán dar cumplimiento a la política de seguridad de la información establecida.

En caso que no sea posible el uso de dispositivos corporativos y el trabajador debe utilizar sus propios dispositivos se deberá tener en cuenta las siguientes recomendaciones:

- Diferenciar cuestas personales de las profesionales.
- La información generada deberá alojarse de forma compartida en un servidor en la nube.
- Usar contraseñas robustas, (según se establece en el procedimiento PSG-024).
- Sistemas operativos aplicaciones y antivirus actualizados.
- Cifra información.
- Realizar copias de seguridad periódicas.

- Uso de redes seguras.

Desde CIRCET IBERIA solo se permitirá el uso de aplicaciones necesarias para desarrollar sus funciones.

➢ *Copias de seguridad.*

Con objeto de asegurar la información frente a perdidas, robos, extravíos o hackeos se realizarán copias de seguridad diarias, aunque se podrá flexibilizar la frecuencia en función del tipo de información y su criticidad.

➢ *Contraseñas.*

La confidencialidad de las contraseñas será absoluta, evitando dejarlas apuntadas en lugares visibles o accesibles, de manera que puedan ser conocidas por otras personas. Las contraseñas se establecerán según se indica en el PSG-024 Acceso Lógico.

➢ *Uso redes seguras.*

El trabajador se compromete a usar redes seguras para teletrabajar, se prohíbe el uso de redes públicas, que carecen de seguridad y el acceso a la red corporativa desde el exterior podría implicar muchos riesgos. Por ello se usará una conexión privada (VPN), tratando de mantener la seguridad y confidencialidad de nuestra información.

➢ *Cifrado comunicaciones y dispositivos.*

Para proteger nuestra información, las comunicaciones entre los dispositivos empleados por los trabajadores y los servidores corporativos estarán cifradas de extremo a extremo. Cuando se acceda a través de internet se dispone del protocolo de transferencia segura de datos “htpps”.

➢ *Comunicaciones seguras*

Los trabajadores en modalidad de teletrabajo deberán proteger las comunicaciones frente a posibles amenazas, las comunicaciones más utilizadas son:

- Correo electrónico
- Videoconferencias

Correo electrónico:

El empleado se comunicará a través del correo electrónico corporativo por lo que no debe ser descuidado en nuestro perímetro de seguridad.

Además, se permitirá el uso de plataformas de trabajo colaborativo (Microsoft Teams…) que facilitan la comunicación en tiempo real y que permite compartir documentos. Se recomienda el uso de plataformas con medios de acceso seguros.

Durante el uso del correo electrónico corporativo será necesario que el trabajador tenga en cuenta las siguientes medidas de seguridad:

- ✓ Identificar al remitente
- ✓ Inspección de enlaces
- ✓ Activación de spam y antimalware
- ✓ Utilización contraseñas seguras
- ✓ No utilizar redes públicas ni wifi gratuito
- ✓ Utilizar copia oculta en los envíos múltiples

Videoconferencia:

El uso de plataformas de videoconferencias en el teletrabajo será útil y necesarias, pero se deberá tener en cuenta:

- ✓ Aplicaciones de proveedores oficiales, descargar las aplicaciones de proveedores oficiales y mantenerlas actualizadas.
- ✓ Numero participantes, programar las sesiones con el número exacto de participantes y una vez en la sesión cerrar el acceso a otros participantes.
- ✓ Sesiones con identificador único por reunión, evitar el uso de identificadores permanentes.
- ✓ Configurar sesión para aviso de entrada o salida de nuevos usuarios, para saber quiénes están conectados a la sesión, con identificadores o nombres, sobre todo en conexiones solo de audio.
- ✓ Grabación de la sesión, el moderador gestionará si se puede grabar, en tal caso, todos los usuarios deben conocer que está siendo grabada mediante un indicador visual o sonoro.
- ✓ Control del contenido, evitar pinchar en enlaces del chat sobre todo si no se conoce a quien lo comparte.

- ✓ Acceso a la reunión, será recomendable que los usuarios a la sesión no puedan acceder hasta que no se conecte el moderador y la sesión debe poder cerrarse al salir el moderador.
- ✓ Enlace, se recomienda no compartir el enlace a la reunión de manera pública.

➢ *Almacenamiento en la nube.*

Se fomentará el uso de plataformas de compartición de documentación y almacenamiento de ficheros (Microsoft OneDrive, Google Drive, Dropbox…), que facilitará el acceso, de forma segura y rápida, a la información en la modalidad de teletrabajo y ante casos de pérdida o robo de dispositivos, no implicará la perdida de la información.

Para información confidencial se recomienda cifrarla para evitar el acceso a su contenido, aunque se descargue.

➢ *Actualización de antivirus, aplicaciones y sistema operativos.*

Serán obligatorias las actualizaciones de antivirus o software antimalware, sistema operativo o aplicaciones de uso corporativo, se tendrán en cuenta las notificaciones de los fabricantes, por lo que será necesario tener licencias oficiales de uso.

➢ *Monitorización y accesos autorizados.*

Los trabajadores en situación de teletrabajo serán supervisados para conocer cómo se realiza el trabajo, así como revisar que lo establecido en esta política se cumple por el personal de la organización.

➢ *Derechos de empleados.*

En caso de trabajadores en modalidad de teletrabajo los mecanismos de monitorización tendrán en cuenta y respetarán los derechos digitales establecidos en la LOPDGDD, en particular, el derecho a la intimidad y uso de dispositivos digitales, así como el derecho a la desconexión digital en el ámbito laboral. Derechos de los trabajadores en modalidad de teletrabajo:

- Derecho a la intimidad en el uso de los dispositivos digitales otorgados por la empresa, de acuerdo con los usos sociales y en el marco constitucional.
- Derecho a la desconexión digital al finalizar la jornada laboral, respetando el descanso, permisos y vacaciones.

- Los trabajadores en situación de teletrabajo, tendrán los mismos derechos que los trabajadores presenciales (promoción interna, derechos de salud, seguridad en materia de PRL, … (Art. 13 Estatuto Trabajadores)

➢ *Comunicación de incidentes de seguridad*

Desde CIRCET IBERIA se establecerán los mecanismos que permitan monitorear el comportamiento en la red que se este utilizando para el teletrabajo, de manera que se pueda identificar situaciones anómalas que puedan dar lugar a ataques cibernéticos o incidentes de seguridad. En caso de producirse incidentes en la seguridad se deberá poner en conocimiento del Responsable de Seguridad según se establece en el procedimiento PSG-025 Gestión de Incidencias.

También podrán comunicarse a través de ADCAB (HELPDESK).

Manuel Delgado Godino
Gerente de CIRCET IBERIA S.L.U.
24 de Julio de 2023

Revisión 01

Política de Mesas Limpias

En CIRCET (compuesta por CIRCET INFRAESTRUCTURA DE TELECOMUNICACIONES y SMARTEL) trabajamos a diario con gran cantidad de documentación, la cual es habitual que esté distribuida encima de la mesa para mayor comodidad o porque es necesaria para las tareas diarias.

Sin embargo, al acabar la jornada laboral o en espacios temporales que no vayamos a estar controlando dicha información, debemos guardar la documentación que se encuentre a la vista (información de la empresa, clientes, proveedores, etc.) Esto es especialmente importante en casos en que se pueda atender a personal externo en la propia mesa del trabajador.

- Medidas de seguridad a tomar por parte del empleado.

  - El empleado debe mantener su puesto de trabajo limpio y ordenado, evitando tener aparatos electrónicos y cables que puedan provocar situaciones de peligro.
  - La documentación que no se esté utilizando en un momento determinado debe estar guardada correctamente, especialmente cuando dejamos nuestro puesto de trabajo y al finalizar la jornada.
  - No debe haber usuarios y contraseñas en hojas o post-it visibles en la mesa o pantallas.
  - Debe bloquearse el equipo para evitar accesos no autorizados. De esta manera evitamos miradas indiscretas que puedan derivar en una fuga de información, además del robo de documentos que pueden contener información confidencial.

  - Todos los equipos electrónicos (ordenadores, teléfonos móviles …) deberán estar protegidos por contraseñas robustas.
  - Todo el personal debe de ser cauteloso de cuidar que la información presentada por las aplicaciones no sea visible por personas no autorizadas. Al finalizar la jornada, los ordenadores deben quedar apagados. En el caso de que sea necesario que permanezcan

encendidos, la pantalla debe estar bloqueada. El acceso físico a las instalaciones donde se encuentren ubicados los sistemas de tratamiento de la información queda restringido, salvo al personal autorizado a ello.

- Responsabilidades.

El responsable de cada departamento es responsable de gestionar la implementación y velar por el cumplimiento de la presente política, así como el Resp. de Seguridad es responsable de su revisión periódica, actualización, difusión, concienciación del personal y terceros para su adecuado cumplimiento.

- Conformidad.

Esta Política será mantenida y actualizada y adecuada a los fines de nuestra organización. A este efecto se revisará a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

24/07/2023

Revisión 03

"POLÍTICA DE GESTIÓN DE LA ENERGÍA"

CIRCET IBERIA S.L.U. (compuesta por CIRCET INFRAESTRUCTURAS DE TELECOMUNICACIONES y SMARTEL) como empresa dedicada a la ***Instalación y Mantenimiento de Teléfono, Internet y Televisión por cable*** así como la **ingeniería de telecomunicaciones,** basando su actividad en las instalaciones de telecomunicaciones, la adquisición, legalización e ingeniería, para el despliegue de redes de fijo y móvil, así como la gestión de la red ya existente, es consciente de la importancia de cumplir con los requisitos medioambientales de sus clientes para asegurar la plena satisfacción de los mismos y de que la actividad que desarrolla puede incidir sobre las condiciones ambientales de su entorno.

La Dirección de CIRCET IBERIA S.L. con la visión de constituir la compañía como un referente en el sector de las telecomunicaciones y que aporta soluciones de valor e innovadoras en todos sus servicios asume la necesidad de seguir avanzando en el camino de la mejora continua y ha decidido implantar un Sistema de Gestión de la energía en su actividad en base a la norma UNE-EN ISO 50001 y se compromete a liderar la Gestión del Sistema de gestión de la energía y a facilitar todos los recursos y medios necesarios para garantizar la satisfacción de nuestros clientes y la mejora continua del Sistema, así como la prestación de servicios seguros y fiables cumpliendo con las especificaciones, requisitos legales, normas y códigos aplicables en base a los siguientes principios:

- Mantener, aplicar y revisar periódicamente un Sistema de Gestión Energética conforme con la norma internacional ISO 50001.

- El cumplimiento de los requisitos exigidos por el cliente, a través de un permanente contacto con los mismos, los requisitos legales aplicables y otros requisitos en materia energética que afecten a nuestra actividad y a los que la organización suscriba.

- Un esfuerzo para la mejora continua de identificación, evaluación y reducción de los efectos ambientales derivados de nuestra actividad, mejorando de forma permanente la eficacia del Sistema de Gestión implantado, aplicando las acciones determinadas tras analizar los resultados del desempeño energético y la información obtenida en las auditorías y en las revisiones periódicas.

- Determinar los medios adecuados para garantizar la eficaz comunicación interna y externa sobre el Sistema de Gestión y el desempeño energético.

- Establecer, planificar y revisar objetivos coherentes con la presente Política y realizar el seguimiento de las acciones que se determinen para su consecución.

- Respeto al medio ambiente mediante el uso sostenible de recursos naturales, así como la prevención la contaminación, con el deseo de convivir en armonía con el entorno que nos rodea.

El desarrollo de planes y programas que establezcan objetivos y metas, para garantizar la calidad de los servicios prestados, reducir los posibles impactos sobre el medio ambiente y el desarrollo de auditorías internas que permitan reducir riesgos y los productos no conformes, minimizar los efectos ambientales negativos y controlar regularmente los avances y la eficacia de las medidas aplicadas, fomentando la mejora continua de los procesos y prácticas de la empresa.

Fomentar la eficiencia energética mediante el desarrollo y mantenimiento de programas de formación e información sobre el uso de las energías. Formar a cada empleado en materia

de gestión energética desarrollando planes de formación adecuados que garanticen su competencia profesional en el desarrollo de sus funciones.

- Asegurar la disponibilidad de la información. Proporcionarlos medios, infraestructuras y recursos humanos necesarios para conseguir la conformidad de los requisitos aplicables al uso y consumo de la energía, el control energético y los objetivos y metas.

- Mejorar el desempeño energético tanto en instalaciones como en equipos, teniendo en cuenta oportunidades de mejora en el diseño y la adquisición de productos y servicios energéticamente eficientes.

- Asegurar que todas sus actividades, productos y servicios se desarrollen en el marco establecido en la presente Política.

En este sentido, cada integrante de la empresa tiene como una condición más de su trabajo el cumplir con los requisitos establecidos en materia de gestión de la energía y asegurar la satisfacción de nuestros clientes. Esta Política se encuentra a disposición del público o cualquier otra parte interesada y se revisa y actualiza para su continua adecuación.

Manuel Delgado Godino
Gerente de CIRCET CABLEVEN S.L.U.
24 de julio de 2023

Edición inicial 01

Política de Dispositivos Móviles

Este es un documento elaborado debido al Sistema de Gestión de Seguridad de la Información, para su cumplimiento por parte de todo el personal de CIRCET IBERIA S.L.U. (compuesta por CIRCET INFRAESTRUCTURA DE TELECOMUNICACIONES y SMARTEL) al que se le haya proporcionado un dispositivo móvil, considerado como un activo dentro del sistema y que permite garantizar y regular el uso y administración de los dispositivos móviles.

- Entrega de dispositivos móviles.

En el momento de entrega de dispositivos móviles, los empleados que reciban el dispositivo deben firmar un compromiso de aceptación y buen uso de activos en referencia al que vaya a recibir en ese momento

- Responsabilidades.

El Departamento de Informática es responsable de gestionar la implementación y velar por el cumplimiento de la presente política, así como el Responsable de Seguridad es responsable de su revisión periódica, actualización, difusión, concienciación del personal y terceros para su adecuado cumplimiento.

- Conformidad.

Esta política de Seguridad será mantenida y actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos estratégica de la organización. A este efecto se revisará a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Manuel Delgado Godino
Gerente de CIRCET IBERIA S.L.U.
24 de Julio de 2023

Revisión 01

"POLÍTICA DE CALIDAD, AMBIELTAL Y DE LA SEGURIDAD Y SALUD LABORAL"

CIRCET IBERIA S.L.U. (compuesta por CIRCET INFRAESTRUCTURAS DE TELECOMUNICACIONES y SMARTEL) como empresa dedicada a la ***Instalación y Mantenimiento de Teléfono, Internet y Televisión por cable*** así como la **ingeniería de telecomunicaciones,** basando su actividad en las instalaciones de telecomunicaciones, la adquisición, legalización e ingeniería, para el despliegue de redes de fijo y móvil, así como la gestión de la red ya existente, somos conscientes de la importancia de cumplir con los requisitos de nuestros clientes para asegurar la plena satisfacción de los mismos, del personal de la organización y demás partes interesadas, de que la actividad que desarrollamos puede incidir sobre las condiciones ambientales de nuestro entorno y de prevenir los daños a la seguridad y salud de los trabajadores y la de terceras personas que puedan permanecer en nuestras instalaciones o zonas cercanas a nuestros lugares de trabajo.

La Dirección de CIRCET IBERIA S.L.U. con la visión de constituir la compañía como un referente en el sector de las telecomunicaciones y que aporta soluciones de valor e innovadoras en todos sus servicios asume la necesidad de seguir avanzando en el camino de la mejora continua y ha decidido implantar un Sistema de Gestión Integrado de Calidad, Ambiental y de la Seguridad y Salud Laboral en su actividad en base a las normas UNE-EN ISO 9001, UNE-EN ISO 14001 e ISO 45001. Por ello, nos comprometemos a liderar la Gestión del Sistema Integrado y a facilitar todos los recursos y medios necesarios para garantizar la satisfacción de nuestros clientes y la mejora continua del Sistema, así como la prestación de servicios seguros y fiables cumpliendo con las especificaciones, requisitos legales, normas y códigos aplicables en base a los siguientes principios:

- El cumplimiento de los requisitos exigidos por el cliente, a través de un permanente contacto con los mismos, los requisitos legales aplicables y otros requisitos en materia de prevención de riesgos laborales y medio ambiente que afecten a nuestra actividad y a los que la organización suscriba.

- Potenciar el trabajo en equipo y realizar grupos de trabajo con un enfoque a la innovación de servicios con los que apoyar a nuestros clientes.

- Un esfuerzo para la mejora continua de identificación, evaluación y reducción de los efectos ambientales y riesgos laborales derivados de nuestra actividad, así como la obtención de beneficios en la empresa.

- La salud y seguridad de los trabajadores y el respeto al medio ambiente mediante el uso sostenible de recursos naturales, así como la prevención la contaminación, con el deseo de convivir en armonía con el entorno que nos rodea y las condiciones de trabajo seguras y saludables para la prevención de lesiones y deterioro de la salud dirigida a obtener el nivel adecuado de protección de los trabajadores así los daños materiales y reducir el absentismo laboral, buscado el compromiso y bienestar del personal en el ámbito de la seguridad y la salud laboral, así como la consulta y participación de los trabajadores, incluyendo estos compromisos dentro de su estrategia empresarial.

- El desarrollo de planes y programas que establezcan objetivos y metas, para garantizar la calidad de los servicios prestados, reducir los posibles impactos sobre el medio ambiente y disminuir la importancia de los riesgos laborales de los puestos de trabajo. La actualización de planes de emergencia y el desarrollo de auditorías internas que permitan reducir riesgos y los productos no conformes, minimizar los efectos sobre la calidad, ambientales y de seguridad y salud laboral negativos y controlar regularmente los avances y la eficacia de las medidas aplicadas, fomentando la mejora continua de los procesos y prácticas de la empresa.

- Formar a cada empleado en materia preventiva, de gestión ambiental y de la calidad, desarrollando planes de formación adecuados que garanticen su competencia profesional en el desarrollo de sus funciones.

- Asegurar que todas sus actividades, productos y servicios se desarrollen en el marco establecido en la presente Política.

En este sentido, cada integrante de la empresa tiene como una condición más de su trabajo el cumplir con los requisitos establecidos en materia de Seguridad y Salud Laboral, respetar el Medio Ambiente y asegurar la satisfacción de nuestros clientes. Esta Política se encuentra a disposición del público o cualquier otra parte interesada y se revisa y actualiza para su continua adecuación.

Manuel Delgado Godino
Gerente de CIRCET IBERIA S.L.U.
24 de julio de 2023

Edición inicial 01