Manual de Usuario de los Sistemas de Información

Índice

1. Introducción

El presente Manual facilita la información necesaria para el **funcionamiento adecuado de los Sistemas de Información** (ordenadores, correo electrónico, Internet, telefonía, TPV's, balanzas, terminales RF picking, etc.) y es una **guía general para el uso eficiente de los recursos y bienes informáticos** por parte de los empleados de Condis Supermercats, S.A. (en adelante, Condis).

Los usuarios de los Sistemas de Información deberán observar todos los aspectos del Manual como **condiciones de uso y medidas de seguridad** del mismo, que son detallados en el presente documento, del mismo modo, las indicaciones **para un manejo eficiente y eficaz.**

Las Políticas y estándares de Seguridad Informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información de Condis.

El Manual describe las Políticas y los estándares de seguridad, para su conocimiento y cumplimiento, que deberán observar de manera **obligatoria todos los usuarios de Sistemas de Información**, para **el buen uso** del equipo, aplicaciones y servicios informáticos de Condis y sirve de **guía operativa** para su acatamiento.

Los Sistemas de Información que Condis pone a disposición de sus empleados, son propiedad de la Compañía. Por ese motivo, Condis se reserva la facultad de supervisar el uso que se realiza de los mismos. No existirá, de manera general, **una expectativa de privacidad en el uso de dichos Sistemas.**

No obstante lo anterior, se respetarán en todo caso los estándares mínimos de protección de datos personales y de la intimidad del personal, de acuerdo con los usos sociales, los derechos reconocidos constitucional y legalmente y, en particular, de conformidad con el artículo 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y de Garantía de los Derechos Digitales ("**LOPDGDD**"), así como en lo que resulte de aplicación el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales ("**RGPD**").

Con el uso de los Sistemas de Información, **el empleado conoce y acepta el derecho de la Compañía a monitorizar y auditar** la utilización de los equipos, aplicaciones y servicios informáticos con el objetivo de asegurar el cumplimiento de las normas contenidas en este manual.

2. Soporte técnico y ayuda

2.1 Servicio de Helpdesk

La División de Organización y Sistemas de Información (DOSI) dispone de un servicio de *Helpdesk para usuarios de oficinas y plataformas.*

Este servicio ofrece soporte en las aplicaciones, equipos, sistemas y comunicaciones de Condis tanto para solicitar ayuda en el uso de las aplicaciones y herramientas informáticas, como para reportar incidencias y realizar peticiones.

En caso de existir alguna incidencia o consulta puedes dirigirte a *Helpdesk*, utilizando su extensión corporativa: 223750 si llamas desde la sede de Montcada, el teléfono directo 935.653.422 si llamas desde otra plataforma o su dirección de correo electrónico: helpdesk@condis.es.

2.2 Servicio de SCC

El Departamento de Soporte y Comunicación al Cliente, en adelante SCC, conjuntamente con la DOSI, ofrece soporte en las aplicaciones, equipos, sistemas y comunicaciones a los usuarios de plantas propias y franquicias de Condis tanto para solicitar ayuda en el uso de las aplicaciones y herramientas informáticas, como para reportar incidencias y realizar peticiones.

En caso de existir alguna incidencia o consulta puedes dirigirte al SCC, utilizando su número de teléfono 931.229.594 o su dirección de correo electrónico: info@condis.es.

3. Seguridad en la red y en los ordenadores

3.1 Seguridad en la red

Mantener segura la red de datos de la Compañía es un elemento esencial para la protección de sus activos.

Todos debemos colaborar en esta tarea cumpliendo con las Políticas de Seguridad detalladas en este Manual.

Comunica inmediatamente a Helpdesk o al SCC cualquier indicio que tengas sobre la falta de seguridad o integridad de los sistemas y/o las redes.

3.2 Configuración inicial

Cualquier cambio en la configuración inicial del ordenador puede vulnerar la seguridad de los datos, dañar el acceso a las comunicaciones y/o alterar su correcto funcionamiento.

Queda, por tanto, prohibido modificar la configuración inicial de los equipos, así como manipular las conexiones eléctricas, cableados de Red y telefonía.

Cualquier cambio debe ser autorizado por el Departamento de Operaciones TI, notificándolo por el canal que corresponda, Helpdesk o SCC.

3.3 Seguridad en ordenadores portátiles

Las siguientes medidas de seguridad en el uso y transporte de ordenadores portátiles son de obligado cumplimiento para todos los empleados:

- El portátil debe mantenerse en todo momento bajo control, siendo obligatorio dejarlo guardado bajo llave si nos separásemos de él.
- Los portátiles deben ser trasladados usando bolsas de protección.
- Protege el portátil del polvo y la suciedad; no lo expongas directamente al sol.
- No se deben tomar alimentos ni bebidas sobre el portátil.
- Evita exponer tu ordenador a cambios bruscos de temperatura. Si el ordenador se ha sometido a una temperatura extrema, espera a que esté a temperatura ambiente antes de volver a encenderlo.
- Mantén tu portátil alejado del agua. No lo enciendas estando mojado y si se moja estando encendido, desconéctalo inmediatamente de la red y de la toma eléctrica.
- No coloques la bolsa del portátil en el suelo de ningún medio de transporte eléctrico (tren, tranvía, etc.). El disco duro se puede dañar debido a los campos magnéticos generados por estos motores. Deja el ordenador en los compartimentos superiores.
- Está prohibido modificar o desactivar la contraseña de arranque de los equipos cuando éstos la tengan activada.
- Los Sistemas anexos proporcionados por el Departamento de Operaciones TI para dotar de mayor seguridad a los equipos portátiles (tarjetas, USB, Tokens, etc.), no se deberán guardar en la bolsa de protección del equipo portátil.

En caso de robo del ordenador portátil, ponte en contacto, de inmediato, con el Departamento de Asesoría Jurídica (Ext. 223700) para que te indiquen los pasos a seguir para realizar la denuncia y notifícalo, también, al Departamento de Operaciones TI mediante Helpdesk.

3.4 Política de contraseñas

Es muy importante el uso de contraseñas para reforzar la seguridad de la información que es propiedad de Condis. Las contraseñas deben cumplir las siguientes normas:

- Las contraseñas deben ser memorizadas. Nunca se deben escribir en el Smartphone, agendas, teléfonos móviles, Post-it, etc. Las contraseñas críticas imprescindibles para el mantenimiento de ciertos sistemas se deben guardar por escrito en lugares seguros. Contacta con Helpdesk para más información.
- Nunca dejes tu contraseña a nadie, incluyendo compañeros de trabajo, familiares, o amigos. Si se hace, debe cambiarse inmediatamente.
- La contraseña se cambiará cada tres meses. Cuando un sistema te sugiera un cambio de contraseña, hazlo lo antes posible, no esperes a que ésta quede caducada.
- Es importante cambiar la contraseña cuando ésta haya sido proporcionada por Helpdesk o SCC, sea para un usuario nuevo, en caso de reseteo de la contraseña, etc.
- Realiza el cambio de contraseña en todos los sistemas y aplicaciones a los que tengas acceso cuando debas de modificar una de ellas, y utilices la misma contraseña para todos.
- La contraseña deberá tener al menos 8 caracteres.
- La contraseña puede contener letras minúsculas, letras mayúsculas, números y caracteres especiales. De los 4 tipos de caracteres mencionados anteriormente, la contraseña debe contener 3 de ellos.
- Los sistemas recordarán un historial de 10 contraseñas, es decir, cuando se haga un cambio de contraseña, no se podrá utilizar ninguna de las 10 contraseñas anteriores.
- La mala introducción de la contraseña en 5 ocasiones supondrá el bloqueo de la cuenta en la mayoría de las aplicaciones.
- La cuenta se desbloquea automáticamente transcurridos 30 minutos. Antes de este periodo, la cuenta solo podrá ser desbloqueada por el Administrador del sistema. Se deberá contactar con el servicio de soporte correspondiente, SCC para el personal de plantas y Helpdesk para el resto de la compañía.

3.5 Gestión segura de contraseñas

Indicaciones a seguir para la creación de contraseñas:

- Nunca debes crear un usuario y contraseña en servidores externos a Condis iguales al usuario y contraseña de acceso a los sistemas de la Compañía.
- Nunca uses una parte o variación del usuario para crear la contraseña.
- Nunca uses una parte o variación de tu nombre o el de algún familiar, ni tu dirección, teléfono, etc.
- Nunca uses datos que se puedan encontrar fácilmente como la matrícula de tu coche, modelo, etc.
- Nunca utilices contraseñas que contengan únicamente números dado que, éstas son más fáciles de descifrar.
- Nunca anotes tu contraseña, ni la escribas en un correo electrónico, ni hables de ella en público.
- Nunca compartas tu contraseña con nadie.

Queda prohibido:

- El acceso a los Sistemas de otro empleado utilizando sus credenciales (usuario y contraseña).
- Facilitar a otro empleado tus credenciales de acceso a los Sistemas.

Para evitar el uso de estas prácticas, deberán seguirse las siguientes recomendaciones:

- Guardar todos los documentos corporativos en las unidades de red (Z, X, etc.) para que los usuarios pertinentes puedan tener acceso a dicha información en el caso que, fuera necesario o en los espacios personales que tengas asignados en la nube (OneDrive).
- La gestión de temas corporativos deberán realizarse utilizando cuentas de correo genéricas.
- Cuando un usuario no pueda atender el correo por motivos de vacaciones, bajas, etc., se deberá activar la opción "Fuera de oficina" para avisar al remitente de los mensajes, tanto de la fecha en la que podrá responder el mensaje, como de a quién contactar en su ausencia. Esta opción se puede activar en el menú "Archivo", "Respuestas Automáticas" del Microsoft Outlook.

3.6 Prevención ante software malicioso

El software malicioso o malware es un tipo de software que está diseñado para infiltrarse o dañar los Sistemas de Información sin el consentimiento de su propietario.

Dicho software puede robar datos confidenciales de tu equipo, ralentizar su rendimiento gradualmente o incluso enviar correos electrónicos falsos desde tu cuenta sin tu conocimiento.

El término software malicioso o malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware entre otros.

El software malicioso puede introducirse en tu ordenador de distintas formas, siendo éstas las más comunes:

- Visitando sitios web.
- Abriendo un correo o un archivo adjunto al correo electrónico que contenga software malicioso.
- Pinchando un pendrive en el ordenador.
- Haciendo clic en una ventana emergente o en un mensaje de error falso que inicia una descarga de software malicioso.
- Descargando software gratuito de Internet que contenga software malicioso.
- Descargando software ilegítimo donde se haya incluido software malicioso.

Para reducir el riesgo de descarga de programas maliciosos es necesario que todos contribuyamos en la protección de los recursos de la Compañía contra estos ataques, por lo que deberás cumplir con la normativa siguiente:

- No cambies la configuración de las funciones de seguridad de tu navegador.
- Presta atención a las advertencias de seguridad de tu navegador.
- En lugar de hacer clic en el enlace de un email, escribe directamente el URL en la barra de tu navegador.
- No abras los archivos adjuntos de los emails a menos que sepas quién te los envió y de qué se trata.

- No descargues ni instales ningún software que no sea el proporcionado por la Compañía. Si existiera la necesidad de instalar nuevo software, se deberá proceder tal y como se explica en el punto 5 de este manual.
- No hagas clic en las ventanas pop-up ni en los carteles de los anuncios con información sobre el rendimiento de tu ordenador.
- Escanea las unidades de memoria USB y demás dispositivos externos antes de usarlos.
- Haz copias de seguridad de tus datos con regularidad.

Controla el funcionamiento de tu ordenador para ver si detectas algo inusual. Si tu ordenador presenta alguno de los siguientes síntomas, podría estar infectado con un software malicioso. En este caso, lo deberías comunicar al Departamento de Operaciones TI por el canal que corresponda, Helpdesk o SCC.

- Funciona lentamente, funciona mal o te aparecen mensajes de error repetidamente.
- No puedes apagarlo o no puedes reiniciarlo.
- Te aparecen en pantalla un montón de ventanas pop-up.
- Te aparecen en pantalla anuncios inapropiados o anuncios que interfieren con el contenido de la página.
- No te permite eliminar un programa indeseado.
- Aparecen anuncios en lugares atípicos.
- Te aparecen páginas web que no tenías la intención de visitar o envía mensajes de correo electrónico que no escribiste.

Otras señales de advertencia de un software malicioso:

- Barras de herramientas nuevas e imprevistas o íconos nuevos e imprevistos en tu escritorio.
- Cambios inesperados en tu navegador, como por ejemplo el uso de un nuevo motor de búsqueda predeterminado o pestañas o etiquetas que no abriste.
- Un cambio repentino o reiterado de la página principal de internet de tu ordenador.
- La batería de tu ordenador portátil se agota más rápido de lo normal.

3.7 Protección de la información para evitar fugas o accesos no autorizados

Para evitar que, en caso de pérdida o robo, haya fugas de información o accesos no autorizados a información de la Compañía, deberás actuar tal y como se detalla a continuación:

- Es obligatorio que los dispositivos móviles (Portátil, Smartphone, tablets, etc.) tengan activado el bloqueo con contraseña. Ello es aplicable a los dispositivos suministrados por la Compañía y a aquellos privados con usos profesionales.
- La información que se grabe en soporte pendrive deberá estar cifrada: se deberá comprimir utilizando WinRar y habilitar una contraseña para poder acceder a dicha información. En el caso de tener dudas al respecto, deberás contactar con Helpdesk.
- No podrá salir de Condis información que haya sido guardada en soporte DVD salvo que, ésta sea pública o esté cifrada.
- Los empleados que utilicen sus dispositivos personales (portátil, Tablet, etc.), podrán utilizarlos para acceder a la información Compañía que se requiera, trabajar con ella, pero no podrán guardarla en dicho dispositivo.
- En el caso que, sea necesario sacar información de Condis en formato papel, serás responsable de su custodia. Deberás ser cuidadoso y velar por su seguridad.

En el caso que, se requiera utilizar otros medios de comunicación vía internet para compartir información (OneDrive, MS Teams, We Transfer, etc.), la información que no sea pública se deberá comprimir y habilitar una contraseña para poder acceder a la misma.

3.8 Datos personales

Es responsabilidad de todos los empleados de Condis que traten y/o tengan acceso a datos personales o de los sistemas que los conservan, cumplir con todas las políticas y leyes aplicables en relación con el tratamiento de los datos personales. Ello se encuentra detallado en el documento "La Protección de Datos en Condis", disponible en la Intranet.

No obstante, consulta con el Departamento de Asesoría Jurídica el modo de proceder en caso de duda o en el caso que, quieras llevar a cabo alguna acción que conlleve recabar datos personales.

Recordarte que, cualquier información (en soporte papel, soporte electrónico o registrada en los Sistemas) que contenga nuevos datos personales debe ser comunicada, antes de su recogida, al Departamento de Asesoría Jurídica) para proceder al cumplimiento de las obligaciones que, en su caso, puedan corresponder de conformidad con la normativa aplicable en materia de protección de datos.

Asimismo, si detectas cualquier suceso esporádico que suponga o pueda suponer un peligro para la seguridad de la información con respecto a datos personales, considerada desde sus tres vertientes de confidencialidad, integridad y disponibilidad, deberás comunicarlo a Helpdesk enviando un correo electrónico a la dirección helpdesk@condis.es.

4. Política de uso de los Sistemas

4.1 Normas generales

Condis pone a tu disposición sistemas de comunicaciones e información en formato electrónico para facilitar las necesidades del negocio de la Compañía y sus intereses. La denominación genérica de Sistemas de Información (los "**Sistemas**") engloba los siguientes componentes: ordenadores personales, conexiones de red, correo electrónico, acceso a Internet y telefonía.

Los Sistemas y toda la información que contienen (incluyendo archivos del disco duro, correos electrónicos, mensajes de voz, logs de acceso a Internet, documentos en la nube, etc.) son propiedad de Condis y su finalidad es el uso profesional. Cada individuo asume la responsabilidad personal de hacer el uso apropiado de los Sistemas, de acuerdo con las Políticas de Condis, y cualquier otra Política de ámbito nacional, comprendidas en los siguientes documentos disponibles en la Intranet.

- ***Política de la Seguridad de la Información.***
- ***Manual de Usuario de los Sistemas de Información* (este mismo documento).**
- ***Manual de Seguridad.***

El personal autorizado por la Compañía puede tener acceso a todos los datos almacenados en los Sistemas, incluyendo los eliminados, respetando en todo momento los periodos de conservación establecidos en el Protocolo de conservación de datos de carácter personal que se encuentra en la Intranet. En cualquier momento, **esta información puede ser monitorizada, revisada o interceptada con intención legítima de la Compañía**; esto incluye lo siguiente:

- por parte del Departamento de Operaciones TI: monitorizar el rendimiento de los Sistemas, prevención del mal uso de los Sistemas, arreglo de incidencias en el software o hardware; y
- por parte de la Dirección de Auditoría Interna: verificar el cumplimiento de las políticas, prevención del mal uso de los Sistemas, cumplir peticiones de información legales o regulatorias e investigar posibles casos de uso indebido de información confidencial de la Compañía, información propiedad de la Compañía o conductas que puedan ser ilegales o influir negativamente en la Compañía o sus miembros.

El uso personal de los Sistemas de Condis se aceptará siempre y cuando sea responsable, moderado, adecuado y no interfiera en el trabajo ni implique la instalación de ningún software ni hardware adicional en el ordenador. Esto podría dañar la configuración del mismo o interferir en el uso de las herramientas profesionales.

En todo caso, debe tenerse en cuenta que, en ningún caso existirá una expectativa de privacidad en el uso personal de los Sistemas, respecto a cualquier uso que no resulte responsable, moderado y adecuado. En este sentido, cualquier acceso a los Sistemas utilizados por los empleados, se realizará de manera justificada y siempre de conformidad con las correspondientes garantías legales, que se exponen en el presente documento.

4.2 Restricciones en el uso de los Sistemas

Los Sistemas facilitan un medio rápido y eficiente de comunicación. Esta facilidad de uso no debe llevar a un uso inapropiado de cualquier tipo de comunicaciones:

- Los Sistemas de la Compañía no se deben usar para enviar / recibir comunicados que contengan material ofensivo, difamatorio y/o amenazante.
- El uso del correo electrónico o cualquier otro medio de comunicación debe estar regido por el buen juicio, buen gusto, sentido común y respeto a la Compañía, sus miembros, clientes, proveedores, etc.
- Los Sistemas no deben utilizarse para enviar o recibir material o imágenes de carácter explícitamente sexual, de discriminación racial o que pueda ser considerado ofensivo, dañino o insultante para cualquier persona basándose en su raza, religión, sexo, nacionalidad, origen, estado civil, edad, discapacidad o aspecto físico.
- Los Sistemas no se pueden utilizar para la distribución de "mensajes en cadena", soportar otro negocio distinto al de Condis, obtener un beneficio personal de algún tipo distinto a los intereses de la Compañía, realizar declaraciones políticas o religiosas, o participar en organizaciones no gubernamentales.
- Actúa con extrema cautela a la hora de suscribirte a listas de distribución de información, "newsletters" o servicios similares dado que, puede provocar una recepción masiva de correos diariamente y es posible que no sea sencillo borrarse de estas listas. Además, esto solo debe realizarse por motivos profesionales. Para otros motivos, utilizar cuentas de correo personales.
- La información almacenada en los servicios de la nube (por ejemplo, OneDrive o MS Teams) **no se puede descargar** fuera de los equipos proporcionados por Condis.

Está prohibido revelar cualquier secreto empresarial de la Compañía, información sujeta a copyright, confidencial o propiedad de la Compañía, clientes o terceras partes, definidos en el "Manual de Seguridad". Esta prohibición también deberá ser estrictamente observada por el empleado en el uso de los Sistemas de Información.

4.3 Restricciones específicas en el uso de Internet

No es posible asegurar una comunicación segura vía Internet si no se usa un sistema de cifrado.

El texto enviado o recibido vía Internet (correo electrónico externo) no debe considerarse privado ni seguro y es susceptible de ser interceptado y manipulado.

La Compañía facilita el acceso a Internet para la comunicación con clientes y otros fines relativos al negocio propio de Condis y para permitir al personal de la Compañía buscar y obtener información para actividades directamente relacionadas con proyectos de la Compañía. Este acceso debe ser autorizado por un Jefe de Departamento, Área o Director y el Director de División correspondiente y debiendo ser justificado, considerando los requerimientos del puesto.

El uso personal de Internet se aceptará siempre y cuando no interfiera en el trabajo ni penalice el rendimiento de la red y además se haga un uso responsable, moderado y adecuado.

Asimismo, está prohibido el uso de Internet para:

- Acciones ilegales.
- Gestionar negocios independientes diferentes a los gestionados por Condis.

- Hablar o escribir en foros de noticias o chats, sea en nombre propio o en nombre de la Compañía sin autorización expresa de la Dirección.
- Participar en actividades externas a la Compañía, como juegos, apuestas, subastas, etc.
- Apoyar o instar al apoyo de causas políticas, comerciales u otras organizaciones "paralelas".
- Actuar como "Hacker" de cualquier tipo, incluyendo el uso de FTP, TELNET o cualquier otro acceso aleatorio a sistemas externos.
- Desarrollar o propagar cualquier tipo de virus informáticos.
- Modificar o evitar el paso por los controles de seguridad de acceso remoto instalados en la Compañía o en cualquier cliente.
- Descargar o recibir por correo electrónico cualquier software que no sea autorizado.
- Obtener o distribuir material de carácter sexual, juegos on-line.

Recordar que, en ningún caso existirá una expectativa de privacidad en el uso de Internet, respecto a cualquier uso que contravenga las prohibiciones o los usos permitidos que se contemplan en este manual.

En este sentido, Condis se reserva el derecho de acceder, monitorizar, auditar, interceptar o revisar cualquier fichero almacenado en un ordenador personal, en la red o la nube, correo electrónico o accesos a Internet, con o sin aviso previo. En concreto, la infraestructura de conexión a Internet pertenece a la Compañía y ésta se reserva el derecho de monitorizar todas las conexiones entre la red e Internet por usuario, sitio accedido y tiempo de conexión.

El Departamento de Operaciones TI puede bloquear, dentro de la red de Condis, el acceso a determinadas páginas cuyo contenido no se considere adecuado.

Con el uso de los Sistemas y conocimiento del presente Manual, todo el personal de Condis conoce y acepta el derecho de la Compañía a realizar los controles descritos en los párrafos precedentes.

En este sentido, en caso de llevar a cabo tales controles con la finalidad de verificar el cumplimiento por el empleado de sus obligaciones y deberes laborales, así como para proteger el patrimonio empresarial y el de los demás empleados, éstos se realizarán únicamente cuando se cumplan los siguientes aspectos:

- El empleado ha sido informado y notificado previamente sobre la existencia de medidas para supervisar su conexión a Internet.
- El acceso que se llevará a cabo se efectuará sobre las conexiones entre la red e Internet por usuario, sitio accedido y tiempo de conexión.
- Condis cuenta con argumentos legítimos para justificar el acceso a las conexiones entre la red e Internet.
- El acceso efectuado cumple siempre con el máximo respeto a la dignidad e intimidad del empleado.

En el marco de una investigación, Condis contará con el soporte externo de expertos terceros a los fines de asesorarse en la ejecución de cualquier actuación necesaria, incluido el acceso a cuentas personales no corporativas de los empleados.

El acceso a tales cuentas personales tendrá lugar con la única finalidad de proteger el patrimonio de la empresa, así como el de sus empleados y con las garantías previstas en el artículo 18 del ET. En consecuencia, dicho acceso se realizará, en caso de ser necesario:

- Dentro del centro de trabajo.
- En horario laboral.
- Con el máximo respeto a la dignidad e intimidad del empleado.
- Con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro empleado de la empresa, siempre que ello fuera posible.

4.4 Restricciones en el uso de Redes Sociales

El uso personal de las Redes Sociales se aceptará siempre y cuando no interfiera en el trabajo ni penalice el rendimiento de la red y además se acceda de forma responsable, moderada y adecuada. No obstante, recordar que, en ningún caso existirá una expectativa de privacidad en el uso de Internet, incluyendo los accesos a Internet para el uso de las Redes Sociales, respecto a cualquier uso que contravenga las prohibiciones o los usos permitidos que se contemplan en este manual.

El Departamento de Operaciones TI puede bloquear, dentro de la red de Condis, el acceso a determinadas Redes Sociales cuyo contenido no se considere adecuado.

En cuanto a la comunicación en Redes Sociales:

- La comunicación corporativa se realizará a través de los perfiles que Condis tiene en las distintas redes sociales y por los empleados autorizados para ello.
- En las comunicaciones personales te animamos a actuar conforme a las "Recomendaciones de uso de las Redes Sociales" disponible en la Intranet con el objetivo de que las utilices protegiendo tu reputación y la de Condis.

5. Software

5.1 Instalación de software

Cuando se entrega un ordenador corporativo, éste ya lleva instalado todo el software estándar para su práctica y especialidad, así como el requerido para el puesto de trabajo específico.

Las instalaciones de nuevo software en ordenadores corporativos deben canalizarse a través de Helpdesk o SCC según corresponda, tanto la compra, como la homologación y la solicitud de instalación de software ya homologado. Debe autorizarlo y solicitarlo un Jefe de Departamento, Área o Director. No está permitida ninguna otra instalación de software por parte del resto del personal de Condis. Sólo está permitida la instalación de software autorizado y proporcionado por la Compañía (Departamento de Operaciones TI).

Mencionar que, la Compañía ofrece la posibilidad de que los empleados instalen el office 365 desktop en equipos particulares.

5.2 Compra de software

El software instalado en los ordenadores de la Compañía es un activo de Condis. Todo el software que se necesite debe ser adquirido por el Departamento de Operaciones TI. Se realizará la petición a Helpdesk o SCC (para tiendas) y éste aplicará el procedimiento establecido.

5.3 Actualizaciones

El Departamento de Operaciones TI, como responsable del buen funcionamiento del Software de la Compañía, puede requerir tu colaboración para actualizar alguno de los Sistemas o parámetros por correo electrónico. Es importante que sigas detalladamente las instrucciones y se realicen en el plazo establecido. Muchas de estas actualizaciones son impuestas por motivos de seguridad y son de obligado cumplimiento para todo el personal.

No está permitido copiar ningún software propiedad de Condis sin tener el consentimiento expreso del Departamento de Operaciones TI.

5.4 Software personal

No está permitido instalar ningún software personal, con o sin licencia de uso, en el ordenador de la Compañía, salvo autorización expresa y previa del Director de División correspondiente y del Jefe del Departamento de Operaciones TI, aplicando los criterios de legalidad, que no interfiera en el rendimiento de los Sistemas ni en la productividad del empleado.

6. Hardware

6.1 Instalación de hardware

Las instalaciones de nuevo hardware deben canalizarse a través de Helpdesk o SCC, que se encargará de registrar la solicitud a la atención del Departamento de Operaciones TI, el cual procederá a homologarlo, inventariarlo y a su instalación. Debe autorizarlo y solicitarlo un Jefe de Departamento, Área o Director. No está permitida ninguna otra instalación por parte del resto del personal de Condis.

No se debe cambiar, manipular, modificar o realizar intercambios entre ordenadores, ni de cualquiera de sus componentes: disquetera, lectora/grabadora de CD-ROM y DVD, la tarjeta de red, etc.

Cuando se realiza un préstamo de un ordenador, periféricos (impresora, escáner, ratón, etc.) o componentes (adaptadores digitales, hubs, cables, adaptadores eléctricos, adaptadores telefónicos, etc.) se especificará una fecha prevista de devolución; en caso de necesitar una ampliación del plazo se deberá informar al Departamento de Operaciones TI.

La sustitución de componentes averiados se realizará previa entrega del componente averiado (cable de módem, teclado, ratón externo, etc.) al Departamento de Operaciones TI.

6.2 Compra de hardware

Todo el hardware es un activo de Condis y debe ser adquirido por el Departamento de Operaciones TI. Se realizará la petición a Helpdesk o SCC y éste aplicará el procedimiento establecido.

6.3 Mantenimiento del disco duro

Para conseguir que tu ordenador funcione correctamente es necesario realizar una "limpieza" periódica del disco duro. Del mantenimiento adecuado de tu ordenador depende, en gran medida, su rendimiento. Esta "limpieza" consiste en borrar el contenido de la carpeta "Temp" y vaciar la papelera, borrar los archivos temporales de Internet.

Además los usuarios de oficinas y plataformas deben apagar el ordenador todos los días no debiéndolo dejar encendido de un día para otro. Si necesitas ayuda para realizar estas tareas, contacta con Helpdesk.

6.4 Política de asignación de ordenadores

La asignación del tipo de ordenador (sobremesa o portátil) va en función de la práctica y especialidad del empleado. No se autorizará el cambio de tipo de ordenador excepto en casos puntuales, debidamente justificados y autorizados por un Jefe de Departamento, Área o Director y el Director de División correspondiente y previa valoración técnica por el Departamento de Operaciones TI. Cualquier cambio de hardware entre usuarios debe ser notificado y autorizado por el Departamento de Operaciones TI.

7. Accesos remotos a Condis

7.1 Generalidades accesos remotos y tele-trabajo

Para evitar multitud de riesgos asociados a esta actividad, se priorizará este tipo de acceso utilizando equipos propiedad de Condis y configurado a tal efecto por el Departamento de Operaciones TI.

Los colectivos que no dispongan de equipos proporcionados por Condis, como pueden ser proveedores y empleados, se realizará la petición al Departamento de Operaciones TI según procedimiento establecido.

Estos equipos deberán disponer como mínimo, de software antivirus actualizado para poder utilizar este tipo de acceso.

Todos los usuarios que dispongan de esta funcionalidad deben estar adecuadamente autorizados por el Jefe de Departamento, Área o Director y el Director de División correspondiente y quedar adecuadamente registrado. El criterio de asignación se realizará atendiendo a la existencia de una necesidad del puesto de trabajo.

El colectivo de usuarios que pueden solicitar un acceso remoto, siempre y cuando aplique el criterio de asignación y la autorización correspondiente, son:

- Propiedad
- Equipo Directivo
- Jefes de Área y Departamento
- Personal de Ventas que realiza sus funciones mayoritariamente fuera de las instalaciones de Condis
- Personal que debe dar soporte fuera del horario laboral.
- Personal que realice tele-trabajo.

7.2 Acceso al correo mediante cliente Web

Todos los empleados con cuentas de correo de Condis, tienen la posibilidad de acceder al correo mediante cliente Web, en la dirección http://mail.condis.es, siendo esta dirección visible tanto en la red local de Condis como desde Internet.

7.3 Conexión a través de Internet y Cliente VPN (Extranet)

Existe la posibilidad de acceder remotamente a la red corporativa de Condis mediante una conexión VPN (Red Privada Virtual).

Esta opción conecta a la red corporativa desde cualquier conexión de Internet, sea esta mediante la tarjeta de comunicación 4G proporcionada con el portátil a los empleados, o con un acceso ADSL-FTTH que pueda disponer en su domicilio o cualquier otra ubicación con acceso a Internet.

Este tipo de acceso es de uso restringido, y lo utilizaran empleados que requieran movilidad, disponibilidad o teletrabajen, así como proveedores que deban dar soporte de forma remota y clientes que lo requieran para acceder a sus tiendas.

La petición para este tipo de acceso debe ser siempre solicitada por un Jefe de Departamento, Área o Director a Helpdesk previa autorización del Director de División correspondiente.

Si el acceso es temporal, se deben realizar la petición con fecha de alta y baja del servicio.

8. Almacenamiento de datos

8.1 Normas de archivado de datos

Toda la información de proyectos y clientes es propiedad de Condis y constituye un activo vital para la Compañía que, en caso de pérdida o robo, se considera un alto riesgo de seguridad. Por ello, es obligatorio que los usuarios mantengan el número mínimo de ficheros en los ordenadores corporativos asignados, es decir, únicamente lo estrictamente necesario para el trabajo diario. El objetivo de esta norma es minimizar el riesgo de la perdida accidental de datos, cumplir la normativa en materia de datos personales, así como asegurar una correcta retención de la información esencial.

Normas de Archivado de Ficheros Profesionales:

- Siempre que nos encontremos conectados a la red de la oficina o los servicios de la nube (por ejemplo, OneDrive o MS Teams), los documentos generados por cada empleado deben guardarse en las carpetas de red o espacios en la nube destinadas a tal efecto. No es necesario hacer copias de seguridad de las carpetas de red ni espacios en la nube ya que son salvaguardados diariamente.
- Dado que, la capacidad de las unidades de red y o espacios en la nube es limitada, cada responsable de Departamento, Área y/o División deben responsabilizarse de la depuración de ficheros duplicados u obsoletos.
- El conjunto de carpetas de red departamentales y espacios en la nube es responsabilidad de cada Departamento, Área y División.
- Las carpetas de red son de uso exclusivo profesional, estando prohibido el almacenamiento de archivos personales y expresamente, videos, música, juegos, software, etc. que estén dentro del ámbito personal / familiar del empleado. Los ficheros de tipo personal podrán guardarse en local aplicando los criterios de legalidad, que no interfiera en el rendimiento de los Sistemas ni en la productividad del empleado.

  Los empleados podrán realizar un uso personal de OneDrive, siempre que esta utilización se base en criterios de eficiencia, prudencia y racionalidad y se realice en los términos previstos en este manual.
- Asimismo, es obligatorio almacenar los ficheros profesionales que contengan datos personales en las unidades de red o espacios en la nube.
- Se recomienda salvar los documentos activos cada 5 ó 10 minutos.
- La información almacenada en los servicios de Condis en la nube, como OneDrive, tanto en unidades corporativas como personales, no deberá extraerse fuera del entorno corporativo de Condis. En ningún caso está permitido la descarga de dicha información en sistemas externos a la Organización (ordenadores personales, dominios externos, etc.).

8.2 Archivo de datos históricos

Los archivos guardados con carácter permanente o histórico, que no se utilicen habitualmente, deben almacenarse comprimidos para minimizar el espacio ocupado; esto se hace utilizando la herramienta WinRar. Si necesitas información acerca de la utilización de esta herramienta, contacta con Helpdesk.

Recordamos que debes dar cumplimiento a la política de conservación de datos de Condis, y no almacenar datos personales por más tiempo del necesario para los fines del tratamiento de esos datos personales.

8.3 Destrucción de soportes

Los soportes que dejen de utilizarse como DVD, Discos, Pendrive, etc. que contengan información y sobre todo datos personales, deben pasar por un proceso que garantice la destrucción de dicha información. Para ello, dichos soportes deben depositarse en el contenedor ubicado en la sala de Sistemas para tal fin, donde se procederá a su destrucción de forma periódica.

9. Correo electrónico

9.1 Cuentas de correo

El sistema de correo electrónico de la Compañía es Microsoft.

La creación de nuestra cuenta de correo electrónico, la realiza el Departamento de Operaciones TI con el nombre y apellidos completos facilitados por el responsable superior del empleado.

La creación se realiza de acuerdo a los estándares de Condis, nombre_apellido@condis.es. o el código de la tienda para las plantas c0001@condis.es.

En el caso que, exista duplicidad, se añadirá el segundo apellido. En el caso de que el primer apellido sea "de + Apellido", el "de" se pondrá junto al apellido.

Se consideran direcciones excesivamente largas aquellas donde nombre_apellido supere los 32 caracteres; solamente en este caso se podrá solicitar el cambio de la misma.

Aunque no es recomendable, se podrá utilizar el correo corporativo para uso personal excepto si:

a) Interfiere con el rendimiento del propio servicio de correo o supone un alto coste para la empresa.
b) Interfiere en las labores propias del usuario o de los gestores del servicio.
c) Supone un riesgo de Imagen para la Empresa.

No obstante, recordar que, las comunicaciones que se realicen a través del correo electrónico corporativo, en ningún caso se considerarán privadas o confidenciales. Consiguientemente, no existirá una expectativa de privacidad o secreto en las comunicaciones enviadas / recibidas por correo electrónico desde y en las direcciones profesionales de correo electrónico.

En este sentido, en caso de detectar un uso indebido de las cuentas de correo corporativo, y resulte necesario examinar su contenido en el marco de una investigación; el acceso podrá hacerse con la finalidad de verificar el cumplimiento por el empleado de sus obligaciones y deberes laborales, así como para proteger el patrimonio empresarial y el de los demás empleados. A tales efectos, en caso de llevar a cabo dicho acceso, éste se realizará únicamente cuando se cumplan los siguientes aspectos:

- El empleado ha sido informado y notificado previamente sobre la existencia de medidas para supervisar su correspondencia y otras comunicaciones.
- El acceso que se llevará a cabo se efectuará sobre los correos recibidos y leídos y sobre aquellos que hayan sido enviados.
- El acceso implicará la aplicación de parámetros de búsqueda informática orientados a limitar la invasión en la intimidad, esto es, no se examinará el contenido del correo electrónico de las cuentas corporativas de modo genérico e indiscriminado, sino que se tratará de encontrar elementos que permitan seleccionar qué correos examinar, utilizando para ello palabras clave que puedan inferir en qué correos podría existir información relevante para la investigación.
- Condis cuenta con argumentos legítimos para justificar el acceso a las cuentas de correo corporativo del empleado.
- El acceso efectuado cumple siempre con el máximo respeto a la dignidad e intimidad del empleado.

Asimismo, además, dicho acceso deberá realizarse:

- Dentro del centro de trabajo.
- En horario laboral.
- Con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro empleado de la empresa, siempre que ello fuera posible.

9.2 Buen uso del E-mail

Deben seguirse las siguientes recomendaciones en cumplimiento del "Manual de Seguridad" así como del uso relativo al correo electrónico:

Recomendaciones de Uso:

- Incluir una frase descriptiva en el campo "asunto" del correo. Esto ayuda tanto al remitente como al destinatario a identificar mensajes sin abrirlos.
- Evitar correos largos, utilizar un lenguaje concreto, preciso y claro. Realizar un breve resumen para ayudar a la compresión y agilidad en la gestión al principio del correo.
- Indicar al destinatario qué quieres. Una vez informes de qué se trata, explica lo que esperas que el destinatario haga, indicando la fecha en la que esperas respuesta.
- Como norma, el correo no debe ser respondido por las personas que están en copia "CC", debe ser respondido por las personas a que va dirigido "Para".
- Limitar el uso de Copia (CC) y Copia oculta (CCO). Usar siempre la lista más pequeña que sea posible.
- Utilizar el campo CCO, cuando se envíe o se responda un mensaje al exterior que incluya muchas personas o grupos corporativos, con el fin de no publicar las direcciones.
- Cuando el mensaje sea informativo, añadir en el encabezado algunos de los acrónimos que indican "para tu o vuestra información", como PVI, FYI, PLTI, PTI, etc.
- Limitar la escritura en MAYUSCULAS. Los textos escritos en mayúsculas dan la impresión de estar gritando y son más difíciles de leer; para resaltar un texto, utiliza el estilo negrita, itálica o distinto color. Se debe tener en cuenta que, al enviar mensajes por Internet, los formatos aplicados al texto se pueden perder.
- Al reenviar un correo externo, es recomendable borrar antes todas las direcciones que aparecen en el cuerpo del correo.
- Para la realización de envíos masivos dentro de la Corporación para informar de situaciones personales o efemérides (p.e. felicitaciones de Navidad, despedidas, etc.), deberá solicitarse la autorización previa del superior inmediato (el Jefe de Departamento, Área o Director, en su caso).

Recomendaciones para una gestión eficaz:

- Es fundamental para el negocio la respuesta a tiempo de todos los correos electrónicos recibidos. Por esta razón se debe consultar la entrada de correo todos los días laborables y de forma periódica.
- La firma automática deberá ser la corporativa. Dicha firma solo debe utilizarse para los correos externos. Para los correos internos, deberá obviarse la firma o, en el caso de requerirse, únicamente se firmará con el nombre y el cargo, sin incluir imágenes o información adicional innecesaria.
- No emplear estilos de fondos de mensajes ya que recargan el correo y pueden provocar problemas al destinatario.
- Limitar el uso de mensajes en formato HTML y los adornos innecesarios.
- Evitar incluir anexos o gráficos de gran tamaño en la medida de lo posible. Incluye preferentemente un enlace a un documento. Esto es especialmente importante al enviar mensajes a usuarios que suelen conectarse de forma remota.

- Evitar la marca de "Importancia Alta" en los correos.
- Desactivar la función de "vista previa" en el Outlook para evitar la intrusión de virus.
- No reenviar alertas de virus, la mayoría son falsas.
- Evitar el reenvío de correo no solicitado (rumores, publicidad, etc.).
- Está prohibido el envío o reenvío de mensajes en cadena.
- Activar la opción "Fuera de oficina" para avisar al remitente de los mensajes, tanto de la fecha en la que podrás responder el mensaje, como de a quién contactar en tu ausencia. Esta opción se puede activar en el menú "Archivo", "Respuestas Automáticas" del Microsoft Outlook.
- El correo no sirve para suplir las reuniones. Hay que evitar utilizarlo para resolver temas complejos evitando las preguntas / respuestas en cadena.

9.3 Correos "Basura" o Spam

Llamamos Correos Basura a los correos no deseados que pueden contener archivos anexos con virus, gusanos, etc. Aunque Condis cuenta con un sistema anti-spam para mejorar la recepción de correos desde Internet, que busca, identifica, analiza y finalmente etiqueta correos electrónicos no deseados, debemos colaborar con el mismo adoptando las siguientes acciones preventivas:

- No uses tu dirección de correo de Condis en Internet para compras on-line, foros de noticias, solicitudes de información en Internet, etc. Usa otra dirección de correo particular siempre que no esté vinculada al ejercicio de tu profesión.
- Lee las cláusulas de privacidad, en cada sitio Web, antes de realizar alguna transacción. La cláusula de privacidad indica si tus datos se pueden compartir con terceras partes.
- Al introducir tus datos en un sitio Web, marca o desmarca (según el caso) las casillas de envío futuro de información.
- Si recibes algún correo basura, no lo contestes nunca. A menudo este tipo de correo incluye instrucciones para no continuar recibiendo información; siguiendo estas instrucciones únicamente confirmas al remitente que la dirección usada es válida y lo que se consigue es la recepción de más correos.
- Se deberá aplicar el procedimiento definido por el Departamento de Operaciones TI para la gestión del Spam, según la solución implementada en cada momento.

9.4 Tamaño del archivo de correo

El correo tiene numerosas funcionalidades relativas al envío y recepción del correo, pero no es un sistema de almacenamiento de información a largo plazo.

El servicio de correo puede estar externalizado mediante el servicio Office 365 o en los servidores de Condis. En ambos casos, el buzón de correo tiene un determinado tamaño aunque éste es mayor cuando el buzón está externalizado.

A continuación tienes unos consejos que te pueden ayudar a la mejor utilización del espacio del correo:

- Borrar, cuando sea preciso por motivos de capacidad, los mensajes que no sean necesarios y archivar, de forma excepcional, los mensajes que se desee conservar en fichero.pst en los espacios de la nube siempre y cuando éstos no contengan datos personales y/o confidenciales.
- Desanexar los ficheros que queramos conservar y borrarlos del contenido del correo.
- No guardar sistemáticamente copia de todos los correos enviados ni recibidos.

9.5 Ficheros adjuntos en el correo electrónico

Una funcionalidad del correo electrónico es la posibilidad de enviar y recibir ficheros adjuntos. El tránsito de estos archivos, tanto en la red como en los enlaces con el exterior (Internet, etc.), ralentizan significativamente estos servicios y el envío y recepción de correos.

Para prevenir esta degradación del servicio, los archivos adjuntos deben ser comprimidos (utilizando WinRar) antes de enviarse y habilitar una contraseña en el caso que aplique. No se recomienda enviar ficheros adjuntos con más de 15 Mb, sobre todo, cuando los destinatarios son Puntos de Venta debido a la restricción de las comunicaciones.

Los correos con ficheros adjuntos mayores de estos tamaños son enviados de forma diferida, enviándose, de forma prioritaria, los de tamaño inferior o rechazados cuando se supere la limitación de los buzones receptores.

Los correos externos deberán firmarse utilizando la firma corporativa. Para los correos internos, se recomienda no utilizar ninguna firma. En el caso que, se necesite, se firmará únicamente con el nombre y cargo, evitando el uso de imágenes, logos, banner, etc. dado que, aumentan el tamaño de dichos correos sin ninguna aportación.

9.6 Correos masivos

Una de las ventajas de nuestro sistema de correo electrónico es la posibilidad de enviar el mismo mensaje a una amplia lista de distribución. Pero, el uso inapropiado de esta funcionalidad puede dañar el rendimiento del sistema. Si tienes que enviar un correo a más de 25 personas, no debe marcarse la opción de acuse de recibo o confirmación de entrega; tampoco debe contener ficheros adjuntos ni gráficos de demasiado tamaño. Se recomienda verificar el tamaño del correo antes de ser enviado.

Contacta con Helpdesk para que te aconsejen acerca de la mejor alternativa.

9.7 Acuse de recibo

Es aconsejable utilizar la opción de "Acuse de Recibo" para los correos enviados fuera del dominio @condis.es, en ningún caso para el envío dentro de la Compañía.

Esta opción genera tráfico y puede tener repercusión en el rendimiento del sistema de correo.

9.8 Información confidencial de clientes o terceros

Ningún comunicado que comprometa o pueda comprometer responsabilidad para Condis debe ser enviado sin la revisión del Director correspondiente.

Se recomienda, así mismo, que ninguna información confidencial propiedad de terceros (clientes, proveedores, etc.) se envíe por correo electrónico externo (Internet) sin que el cliente o tercero haya aceptado, por anticipado, a Condis el uso de Internet como vía de comunicación para información confidencial.

9.9 Contactos

En el caso de tener contactos, en el Outlook, tanto personales como profesionales, se recomienda clasificarlos en carpetas separadas y claramente identificadas atendiendo al tipo de contacto (personal / profesional).

10. Normas para minimizar el tráfico de la red

Para tener acceso a los recursos de red como, e-mail, servidores de archivos, Intranet e Internet es muy importante tu colaboración para minimizar el tráfico en la red, para lo cual se deben seguir las siguientes indicaciones:

- Evita el envío de grandes archivos anexos en los correos electrónicos. Utiliza la compresión de archivos (WinRar).
- Los correos externos deberán firmarse, utilizando la firma corporativa. Para los correos internos, se recomienda no utilizar ninguna firma. En el caso que, se necesite, se recomienda firmar únicamente con el nombre y cargo, evitando el uso de imágenes, logos, banner, etc.
- No se deben descargar ficheros grandes de Internet en horas laborales de mayor tránsito.
- Para evitar la caída del rendimiento de las comunicaciones entre oficinas, plataformas y sobre todo tiendas, para realizar transferencias de ficheros entre equipos de diferentes sedes, se deberá consultar con *Helpdesk*, que valorará el impacto en el rendimiento de la red de datos, y en su caso, planificará la transferencia en el momento de menor tránsito.
- Seguir las recomendaciones del uso de correo electrónico expuestas anteriormente, por el gran volumen de tráfico que genera el correo.

11. Uso de OneDrive y MS Teams

OneDrive es la herramienta de almacenamiento de archivos en la nube adoptada por Condis para la gestión de la información de sus empleados y MS Teams es la herramienta de comunicación corporativa, como tal no solo permite el intercambio de mensajes entre usuarios, sino que también funciona como herramienta de gestión documental, intercambio de ficheros y edición.

Estas herramientas cuentan con el respaldo de Microsoft y son unas de las herramientas más robustas en el mercado no solo a nivel de usabilidad, sino también a nivel de seguridad. No obstante, existen recomendaciones de seguridad y buenas prácticas que se deben seguir para evitar que la información pueda verse en riesgo.

¿Qué se puede hacer con la herramienta?

- Guardar los documentos corporativos para acceder remotamente desde los dispositivos corporativos o mediante la visualización web en equipos personales.
- Compartir información con terceros fuera del entorno de Condis, siempre que los documentos estén protegidos por contraseña.
- Las copias de seguridad de los documentos almacenados en OneDrive se realizan de forma automática, por lo tanto, su uso es muy recomendable.
- Se podrá realizar un uso personal de OneDrive y MS Teams, siempre que su utilización se base en criterios de eficiencia, prudencia y racionalidad y se realice en los términos previstos en este Manual.
- Usar MS Teams como herramienta de comunicación interna con los empleados de Condis para el intercambio de mensajes y documentación.

¿Qué <u>no</u> se puede hacer con la herramienta?

- No se debe compartir información con terceros que no pertenezcan a Condis sin proteger los documentos con contraseña. Y en caso de ser necesario, serás responsable de su custodia. Deberás ser cuidadoso y velar por su seguridad.
- La información almacenada en ellos, no deben ser descargada fuera de los equipos proporcionados por Condis. Es posible acceder a ellos a través del navegador web pero nunca descargar o sincronizar con el equipo.
- Se debe cerrar la sesión de OneDrive siempre que se termine de trabajar para evitar el acceso de terceros a la información de Condis.
- Se debe revisar periódicamente quien tiene acceso a los documentos y revocar los permisos si es necesario.

Recordarte que las herramientas OneDrive y MS Teams son propiedad de Condis por lo que, en ningún caso existirá una expectativa de privacidad respecto a cualquier uso que contravenga lo contemplado en este Manual. En este sentido, cualquier acceso a las mismos, se realizará de manera justificada y siempre de conformidad con las mismas garantías legales establecidas para el acceso a dispositivos móviles.

En caso de resultar necesario examinar el contenido almacenado en dichas herramientas en el marco de una investigación; el acceso podrá tener lugar con la única finalidad de proteger el patrimonio de la empresa, así como el de sus empleados y con las garantías previstas en el artículo 18 del ET. En consecuencia, dicho acceso se realizará estableciendo las mismas garantías para el acceso por Condis a dispositivos móviles (Apartado 11.5 del Manual).

Asimismo, en caso de detectar un uso indebido de la funcionalidad de mensajería de Teams, el acceso podrá hacerse con la finalidad de verificar el cumplimiento por el empleado de sus obligaciones y deberes laborales, así como para proteger el patrimonio empresarial y el de los demás empleados. En este sentido, dicho acceso se realizará estableciendo las mismas garantías para el acceso por Condis a cuentas de correo corporativas (Apartado 9.1 del Manual).

IMPORTANTE: Ante cualquier duda o sospecha sobre la exposición de información o cualquier otro riesgo debes contactar con Helpdesk.

12. Política referente a la telefonía fija, móvil y Smartphone

12.1 Consideraciones generales

Es importante homogeneizar las comunicaciones y la imagen de la empresa al contestar al teléfono, por ello se adjuntan las siguientes recomendaciones:

- Descolgar el teléfono cuando empiece a sonar, evitar esperas al que está llamando.
- Para llamadas externas, identificarse con el nombre de la Empresa, "Condis Supermercats, Buenos días/Buenas Tardes/Buenas Noches".
- Responder inmediatamente después de descolgar sin hacer esperar a nuestro interlocutor.
- Escuchar a nuestro interlocutor hasta que haya terminado de hablar sin interrumpirlo.
- Evitar hablar con los compañeros con el auricular tapado, ya que posiblemente te oirán.
- En las llamadas internas, identificarse al descolgar con el nombre de la persona o con el nombre del Departamento o División.
- Existe la opción de activar el buzón para mensajes de voz en el sistema de Telefonía de Montcada.
- Realizar un uso prudente y racional de la telefonía sea ésta fija o móvil.

En el campo de la seguridad informática, existe una práctica conocida como ingeniería social que consiste en obtener información confidencial a través de la manipulación de usuarios legítimos. Un hacker, mediante ingeniería social, usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible o bien a violar las políticas de seguridad. En ese sentido:

- Nunca se informará del identificador de usuario (userid) a una persona externa a la Compañía ni por supuesto la contraseña aunque sea solicitado por personal de la propia compañía.
- Se debe evitar la difusión de información de cualquier tipo. No se debe difundir información por teléfono salvo con terceros siempre y cuando exista una relación contractual.
- Los terminales de telefonía móvil y Smartphone, son activos de la compañía. Debe realizarse un uso responsable y adecuado del mismo para evitar daños y pérdidas.
- En caso de robo de un terminal móvil o Smartphone, se procederá a realizar la denuncia correspondiente y se solicitará a Helpdesk o SCC la cancelación de la tarjeta SIM. En caso de ocurrir fuera de horario laboral, se debe llamar al teléfono móvil 609 069 967 (Ext. 422750).

12.2 Telefonía móvil y Smartphone: criterios de asignación

A. Todos los empleados integrados en los siguientes colectivos disfrutan de una línea móvil y un Smartphone (modelo de gama alta) por el cargo de responsabilidad y disponibilidad que ocupan en el organigrama de la Compañía:
   i. Miembros de la Propiedad
   ii. Equipo Directivo

B. Todos los empleados que ocupen puestos de trabajo que, en el desempeño de sus funciones, deban permanecer más del 35% de su tiempo laboral fuera de su centro de trabajo, con necesidad de ser localizados, pueden tener derecho al uso del teléfono móvil o Smartphone.

C. Todos los empleados que ocupen puestos de trabajo, que en el desempeño de sus funciones, deban permanecer localizables fuera de su horario laboral deberán tener asignado una línea móvil y Smartphone en el caso de ser necesario.

12.3 Autorización de la entrega del teléfono móvil o Smartphone

Para los supuestos B y C del apartado anterior, el Director del empleado afectado deberá autorizar la asignación y el tipo de dispositivo, realizando la petición correspondiente vía Helpdesk. En estos casos, el dispositivo será de gama media.

12.4 Autorización de la contratación de Roaming / cambio de tarifas de datos

Los empleados que, por motivos de trabajo, requieran la activación del servicio de Roaming si viajan al extranjero (fuera de la UE) o cambiar la tarifa de datos nacional, requerirán la autorización de su Director.

Cuando se realice la activación del Roaming se contratará, en cada caso, la tarifa más adecuada atendiendo a los días de estancia en el extranjero (fuera de la UE) y la necesidad de utilización de los datos que indique el empleado o su Director.

Las líneas tendrán activado un límite de consumo. En el caso de llegar al límite y requerir su ampliación, esta ampliación deberá solicitarse a Helpdesk. En caso de necesitar dicha ampliación fuera de horario laboral, se deberá llamar al teléfono móvil 609 069 967 (Ext. 422750).

El empleado deberá adoptar las medidas necesarias para evitar los excesos de consumo de datos involuntarios que puedan generar las distintas App's instaladas en el Smartphone así como mantener desactivada la "itinerancia de datos" o "datos móviles" en el terminal cuando no se utilice o se pueda acceder vía wifi.

En el caso que, se detecte un consumo excesivo por uso inadecuado del Smartphone o terminal, este exceso podrá ser facturado al empleado.

12.5 Uso personal de la línea y/o dispositivos móviles

Los empleados que dispongan de línea y/o dispositivo móvil (teléfono móvil o Smartphone) a cargo de la Compañía podrán realizar un uso personal de los mismos, siempre que esta utilización se base en criterios de eficiencia, prudencia y racionalidad y se realice en los términos previstos en este Manual.

No obstante, recordar que, las líneas y dispositivos móviles son propiedad de Condis por lo que, en ningún caso existirá una expectativa de privacidad respecto a cualquier uso que contravenga lo contemplado en este Manual. En este sentido, cualquier acceso a los mismos, se realizará de manera justificada y siempre de conformidad con las correspondientes garantías legales, que se exponen en el presente documento.

En caso de resultar necesario examinar el contenido de dichos dispositivos en el marco de una investigación; el acceso podrá tener lugar con la única finalidad de proteger el patrimonio de la empresa, así como el de sus empleados y con las garantías previstas en el artículo 18 del ET. En consecuencia, dicho acceso deberá realizarse:

- Dentro del centro de trabajo
- En horario laboral
- Con el máximo respeto a la dignidad e intimidad del empleado.
- Con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro empleado de la empresa, siempre que ello fuera posible

12.6 Renovación del teléfono móvil o Smartphone

El tiempo de renovación de un dispositivo móvil estará fijada en cada caso según su utilización y función.

Cuando se renueve el dispositivo móvil, el empleado puede optar por quedarse con el antiguo. En este caso, el empleado deberá llevarlo, previamente, al Departamento de Operaciones TI para que sea reseteado.

12.7 Retirada de la línea y/o dispositivos móviles

La Dirección de la Compañía se reserva el derecho de retirar la línea y/o dispositivo móvil (teléfono móvil o Smartphone) asignado a un empleado en los siguientes casos, pudiéndole cargar el importe del consumo en voz y/o datos si se considera pertinente:

- Abuso en el consumo personal en voz y/o datos.
- Llamadas a números de teléfono de contenido ilegal o con motivos que atenten contra las buenas costumbres.
- Desaparición de la causa laboral que ha originado la entrega del teléfono.
- Incumpla el presente manual o cualquiera de las políticas de la empresa.

12.8 Uso de dispositivos móviles personales para usos profesionales (BYOD – bring your own device)

Cualquier empleado que disponga de dispositivos móviles personales que contengan o accedan a información corporativa deben aplicar las medidas de seguridad contempladas en el punto 11.9.

Indicar que, estos dispositivos solo deberán tener acceso al correo electrónico y a la Intranet / Extranet y servicios en la nube, no debiéndose descargar, en dichos dispositivos, información de la Compañía.

No obstante, tras la finalización de la relación laboral, se deberá proceder a la eliminación de cualquier información Compañía que contenga o a la que acceda.

Asimismo, si se considera necesario acceder al contenido de estos dispositivos para la protección del patrimonio empresarial y del de los demás empleados de la empresa (i.e.: sospechas y/o indicios de revelación de información confidencial), se podrá requerir al empleado que facilite el dispositivo en cuestión para poder examinarlo a estos fines. Este control se practicará en horas de trabajo en el centro laboral, y ante la presencia de un representante de los trabajadores o, en su ausencia, de otro empleado de Condis.

12.9 Seguridad

Es obligatorio tener el bloqueo del terminal activado con contraseña para evitar fugas de información de la compañía o accesos no autorizados a recursos corporativos que se puedan producir en caso de pérdida o robo del dispositivo.

El backup de los datos de los dispositivos es responsabilidad del empleado.

En caso de sospecha de infección del dispositivo, acceso no autorizado, pérdida o robo se deberá notificar a Helpdesk.

Queda prohibido realizar Jailbreak o rooteo de los dispositivos (hackear el dispositivo).

Esta política es aplicable a todos los dispositivos corporativos o particulares (BYOD) que puedan contener o acceder a información o recursos de la Compañía.

13. Finalización de la relación laboral

Los empleados podrán utilizar y acceder a los Sistemas puestos a su disposición mientras dure la relación con la Compañía y en los términos previstos en el presente Manual.

En consecuencia, el empleado es conocedor y acepta que, en el momento de la finalización de su relación laboral, dejará de tener acceso a su buzón de correo electrónico y a los medios y equipos informáticos de la Compañía, a los servicios en la nube y, consiguientemente, a los archivos incluidos en los mismos.

En este sentido, cabe indicar que:

- El Departamento de Operaciones TI podrá acceder al buzón de correo electrónico del empleado que ha causado baja. Para los correos electrónicos que puedan recibirse con posterioridad a la baja del empleado, se creará (en el caso que aplique) un "automensaje" de respuesta que se enviará de forma automática al remitente del correo electrónico. En dicho "automensaje" se indicarán los siguientes aspectos: i) que el empleado al que ha enviado el correo electrónico ha causado baja en la Empresa y, ii) de a quién contactar a partir de ese momento.
- El empleado tendrá que devolver los equipos (ordenador portátil, teléfono móvil, etc.), que tenga a su disposición. En el caso que, no se produjera tal devolución o al producirse se detectasen desperfectos derivados de un mal uso, la Compañía se reserva el derecho a tomar las medidas que considere necesarias para cubrir los daños ocasionados.
- El empleado deberá dejar intactos todos los archivos y documentos que hayan tenido un fin profesional o productivo y, a partir de ese momento, no estará autorizado para acceder a los mismos. En el supuesto de que existan archivos de carácter personal, él mismo deberá eliminarlos bajo la supervisión del Departamento de Operaciones TI. Asimismo, no mantendrá en su poder copias de documentos de la Compañía.

Los medios informáticos que el empleado tuviese a su disposición en el momento de la finalización de su relación profesional con Condis, serán custodiados por el Departamento de Operaciones TI hasta que su contenido haya sido copiado y, en su caso, almacenado. En este sentido, cabe indicar que, el contenido de los equipos informáticos y del correo electrónico del empleado únicamente podrá ser revisado, copiado y almacenado por los profesionales del Departamento de Operaciones TI.

Tras la finalización de la relación laboral con la Compañía, ésta última se reserva la facultad de revisar el contenido de:

- Los documentos de trabajo;
- Los discos duros de los ordenadores o sistemas de almacenamiento de información;
- Los datos de las conexiones a la red de Internet;
- La bandeja de salida del correo electrónico;
- La bandeja de entrada del correo electrónico, excepto aquellos correos electrónicos recibidos y no leídos, conforme a lo dispuesto en la ley.

14. Incumplimiento del manual

El contenido del presente Manual es de obligado cumplimiento para todos los empleados de Condis a los que les aplique.

Cualquier incumplimiento de las políticas y normas de uso recogidas en este Manual constituye un incumplimiento del contrato de trabajo, hecho que puede conllevar la adopción de las acciones disciplinarias que, en su caso, procedan conforme a la naturaleza y circunstancias de cada supuesto y en los términos previstos en la Ley y en el Convenio Colectivo que resulte de aplicación. Asimismo, el empleado será responsable frente a Condis y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores.

Con independencia de las medidas que pudieran aplicarse, los costes derivados de un mal uso o del incumplimiento de las normas y recomendaciones de este Manual, como por ejemplo las rupturas y pérdidas de material informático (ordenadores, portátiles, telefonía, Smartphone, etc.), podrán ser facturados al empleado.


PASIÓN
TRANSPARENCIA
RESPETO
CALIDAD
SERVICIO
COLABORACIÓN
HONESTIDAD
AYUDA
DIVERSIÓN
ESFUERZO
INTEGRIDAD
EFICIENCIA
PROXIMIDAD
COMPROMISO
RESPONSABILIDAD
RIGOR
PRECIO
ORGULLO
OPTIMISMO
EXCELENCIA
COMPETITIVIDAD