Normativa interna para los empleados de Grup Vila Cover Corredoria d'Assegurances S.L.

(mayo 2021 – versión 1.3)

Normativa interna

La Normativa Interna, no es más que la concienciación a los empleados de la importancia del buen uso de los medios informáticos y de telecomunicación que se les proporciona para el desarrollo de sus funciones, de forma que el tratamiento de la información se haga según reglas estrictas que permiten garantizar su seguridad.

Una de las funciones de **Grup Vila Cover Corredoria d'Assegurances S.L.**, en adelante la Correduría, es aprobar, publicar y comunicar a todos sus empleados la normativa interna en materia de protección de datos de carácter personal.
Todas las peticiones y autorizaciones deberán ser por escrito, correo electrónico o documento firmado.

Dicha normativa contiene las exigencias legales establecidas en la normativa vigente en materia de Protección de datos, siendo éstas las siguientes:

A. Relativas al uso de contraseñas

- Las claves de acceso al sistema son de uso **personal e intransferible**. No se debe comunicar la clave personal **a ninguna persona**. Si por causa de fuerza mayor se comunica la clave, ésta debe ser cambiada con la mayor brevedad posible.
- La longitud de las claves de acceso tiene un mínimo de **6 caracteres alfanuméricos**.
- No se debe apuntar la clave en sitios accesibles.
- El sistema le obligará a cambiar, trimestralmente la contraseña de acceso. Igualmente, el sistema no le permitirá repetir contraseñas previamente utilizadas.

B. Relativas a los dispositivos de acceso (PC's)

- El terminal de acceso no se puede dejar desatendido, con la aplicación abierta, en ningún momento. Si debe ausentarse del puesto de trabajo realice la desconexión del sistema, de tal forma que sea necesario volver a facilitar identificación de usuario y clave. Si por operatoria de trabajo no es conveniente desconectarse del sistema, bloquee el acceso al terminal, bien cerrando el despacho, bloqueando el terminal con llave física o mediante salva pantallas con contraseña, o cualquier otra medida que impida el acceso no autorizado al sistema. Ningún PC tendrá configurado el inicio automático.
- Se prohíbe la instalación de software en el puesto de trabajo, sin la correspondiente autorización del Responsable de Seguridad.
- Las aplicaciones necesarias para el desempeño de su trabajo son instaladas únicamente por los Administradores del Sistema.
- Siempre debe estar activado el antivirus. Se revisará periódicamente la versión del programa antivirus instalado.

- No se puede guardar información sensible en el PC. La información sensible estrictamente necesaria se debe guardar en directorios protegidos de los servidores de red. Periódicamente los usuarios deben revisar su PC para detectar información sensible, incluida la papelera de reciclaje. Dicha información será destruida o traspasada al servidor de Red.
- No se puede guardar información sensible en cualquier tipo de soporte (disquetes, CD,…). Si por causa de fuerza mayor se debe guardar información sensible en soportes, se etiquetarán adecuadamente y se guardarán bajo llave. Una vez finalizada la utilidad del soporte, se formateará para asegurar el adecuado borrado del mismo.
- Si por alguna causa un soporte que contenga información sensible se estropea y es imposible formatearlo, hay que destruirlo físicamente (la carcasa y el disco interno en el caso de los disquetes) antes de deshacerse de él, de tal forma que sea imposible recuperar información del mismo.

C. Relativas al soporte papel

- Se almacena únicamente en papel aquella información sensible que sea absolutamente necesaria.
- Se guardan los documentos que contengan información sensible en lugares no accesibles por personas no autorizadas, no encima de la mesa.
- Se destruyen los papeles que contengan información sensible de tal manera que sea imposible recuperar la información que contienen antes de deshacerse de ellos.

D. Relativas a las incidencias

- Los usuarios deben notificar al Administrador aquellas incidencias que detecten en referencia a la seguridad de los datos. A modo de ejemplo se citan las siguientes:

  Claves bloqueadas (alguien ha intentado acceder a la información con su código de usuario)
  Desaparición de listados y/o disquetes y/o cintas de respaldo.
  Virus detectados
  Disquetes que no se pueden leer, etc
- El conocimiento y la no-notificación de una incidencia por parte de un usuario es considerado como una falta contra la seguridad del Sistema por parte de ese usuario.
- Las incidencias se crearán en la aplicación Web "IG Quality", especificando que se trata de una incidencia de protección de datos: LOPD.

E. Relativas al acceso a Internet

- Los usuarios son responsables de las sesiones iniciadas de Internet desde sus terminales de trabajo. No olvidar nunca que Internet tiene carácter laboral y no debe usarse con otros fines. Asimismo, se evitará acceder a sitios web de dudosa confianza, o a entidades o empresas desconocidas, para disminuir los riesgos de contagio de programas maliciosos.

- En ningún caso se pueden modificar las configuraciones de los navegadores del equipo, ni la activación de servidores o puertos sin autorización del Responsable de Seguridad.
- Debe evitarse la utilización de imágenes y sonidos para fines distintos e incompatibles a la actividad laboral de la Correduría.
- Se prohíbe expresamente el acceso y/o la descarga y/o almacenamiento en cualquier soporte:
    - de páginas o contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres;
    - de los formatos de imágenes, sonidos o video;
    - de virus y códigos maliciosos;
    - y, en general, de todo tipo de programas sin la expresa autorización del Responsable de Seguridad.
- Queda prohibida toda utilización ajena a las actividades de la Correduría, de los servicios de chat, foros o sitios similares. Tampoco se permite el acceso a páginas de juegos en línea o la descarga de cualquier dispositivo similar, programas como el Messenger o similares.

F. Relativas al uso de correo electrónico

- Los usuarios son responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la Correduría.
- Los usuarios no deberían permitir la utilización de la cuenta y/o el correspondiente buzón, a personas no autorizadas.
- Los usuarios deben ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por la Correduría.
- Los servicios de correo electrónico suministrados deben destinarse a uso estrictamente laboral. Excepcionalmente pueden ser usados para temas personales siempre que no interfieran con el rendimiento del propio servicio, con la labor de los administradores o supongan un coste para la Correduría.
- Cada vez que se tenga que realizar un mailing, a través de correo electrónico, la dirección de los destinatarios de este correo, tendrá que escribirse, obligatoriamente, en la casilla destinada a Copia Oculta (CCo), por motivos de confidencialidad hacia el resto de los destinatarios.
- Está prohibida la utilización, en los equipos informáticos provistos por la Correduría, de buzones de correo electrónico de otros proveedores de Internet.
- No es correcto enviar correo a personas que no desean recibirlo. Si le solicitan detener esta práctica deberá hacerlo. Si la empresa recibe reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas.
- Se prohíbe realizar cualquiera de las siguientes actividades:
    - Utilizar el correo electrónico para cualquier propósito ajeno a las actividades laborales autorizadas por la Correduría;
    - Participar en la propagación de cartas encadenadas, esquemas piramidales o similares, el pasa este correo a tus amigos;
    - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la Correduría;
    - Falsificar las cabeceras de correo electrónico;
    - Recoger correo de buzones de otro proveedor de Internet;

- Difundir contenido ilegal o contrario a la moral y buenas costumbres;
- Enviar correo propio a través de cuentas ajenas sin consentimiento de su titular;
- Efectuar ataques, con objeto de imposibilitar u obstruir sistemas informáticos, dirigidos a un usuario o al propio sistema de correo, así como el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga por objeto la paralización del servicio por saturación de las líneas, de la capacidad de la CPU del servidor, del espacio en disco de servidores o terminales o cualquier otra práctica similar;
- Enviar a foros de discusión, listas de distribución y/o newsgroups, mensajes que comprometan la reputación de la Correduría.

❖ Todos los correos electrónicos incorporaran la siguiente cláusula al pie de los mismos, la cual no debe en ningún caso quitarse.

De conformidad con la normativa vigente en materia de Protección de datos le informamos que en caso de recogida de datos personales a través de este correo electrónico, sus datos serán incorporados a una base de datos de la cual somos Responsables. Usted podrá ejercer sus derechos en cualquier momento y de forma gratuita. Ver Politica de privacidad Completa

GRUP VILA COVER CORREDORIA D'ASSEGURANCES, S.L.U. Registro dirección General de Seguros J00533. Concertado seguro de Responsabilidad Civil profesional según el artículo 157.1g, y acreditada la capacidad financiera según artículo 157.1f, Real Decreto 3/2020, de 4 de febrero, de incorporación de la directiva de la unión europea en el ámbito de seguros privados.

G. Relativas a los soportes

❖ Los soportes que contengan datos del Sistema, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que especifique qué tipo de datos contiene, proceso que los ha originado y fecha de creación.

❖ Los soportes que contengan datos del fichero deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso del mismo.

❖ No se grabarán datos de carácter personal en los soportes sin previa autorización y justificación. Solo el administrador de la base de datos, estará autorizado para hacer este tipo de procesos y será el responsable de su posterior seguimiento.

H. Aspectos relacionados con el Teletrabajo

Las recomendaciones al personal se exponen a continuación y se referencian en el acuerdo de teletrabajo, ajustándose a la situación concreta de las tareas a realizar:

1. Respetar la política de protección de la información en situaciones de movilidad definida por el responsable.
   a. Han de observarse las medidas y recomendaciones recogidas en esta normativa de protección de datos y seguridad de la información, especialmente, en lo que concierne al deber de confidencialidad de la persona trabajadora con relación a los datos personales a los que tuviera acceso en el desempeño de sus funciones laborales.
2. Proteger el dispositivo utilizado en movilidad y el acceso al mismo.

a. La persona empleada debe definir y utilizar contraseñas de acceso robustas y diferentes a las utilizadas para acceder a cuentas de correo personales, redes sociales y otro tipo de aplicaciones utilizadas en el ámbito de su vida personal.
b. No se debe descargar ni instalar aplicaciones o software que no hayan sido previamente autorizados por la organización.

3. Prácticas a tener en cuenta en las fases de inicio, desarrollo, implementación, operación y mantenimiento y retirada de una solución de acceso remoto y teletrabajo.
   a. Es recomendable evitar la conexión de los dispositivos a la red corporativa desde lugares públicos, así como la conexión a redes WIFI abiertas no seguras.
   b. Deben mantenerse protegidos los mecanismos de autenticación definidos (certificados, contraseñas, tokens, sistemas de doble factor, …) para validarse ante los sistemas de control de acceso remoto de la organización.
   c. Si se dispone de un equipo corporativo, no se debe utilizar con fines particulares evitando el acceso a redes sociales, correo electrónico personal, páginas web con reclamos y publicidad impactante, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino.
   d. Si el equipo utilizado para establecer la conexión remota es personal, debe evitarse simultanear la actividad personal con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.
   e. El sistema antivirus instalado en el equipo debe estar operativo y actualizado.
   f. Siempre ha de verificarse la legitimidad de los correos electrónicos recibidos, comprobando que el dominio electrónico del que procede es válido y conocido, y desconfiando de la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces incluidos en el cuerpo del correo que presenten cualquier patrón fuera de lo normal.
   g. Si pueden ser gestionadas por la persona empleada, conviene desactivar las conexiones WIFI, bluetooth y similares que no estén siendo utilizadas.
   h. Una vez concluida la jornada de trabajo en situación de movilidad debe desconectarse la sesión de acceso remoto y apagar o bloquear el acceso al dispositivo.
4. Garantizar la protección de la información que se está manejando
   a. Tanto en lugares públicos como en el entorno domésticos es obligado adoptar las precauciones necesarias para garantizar la confidencialidad de la información que se está gestionando.
   b. Si habitualmente se genera y trabaja con papel, durante situaciones de movilidad es importante minimizar o evitar la entrada y salida de documentación en este soporte y extremar las precauciones para evitar accesos no autorizados por parte de terceros.
   c. La información en soporte papel, incluyendo borradores, no se puede desechar sin garantizar que es adecuadamente destruida. Si es posible, no arrojar papeles enteros o en trozos en papeleras de hoteles, lugares públicos

o en la basura doméstica a los que alguien podría acceder y recuperar información de carácter personal.

d. Conviene extremar las precauciones para evitar el acceso no autorizado a la información personal, propia y de terceros, manejada, no dejando a la vista ningún soporte de información en el lugar donde se desarrolle el teletrabajo y bloqueando las sesiones de los dispositivos cuando estos estén desatendidos.
e. Se debe evitar exponer la pantalla a la mirada de terceros. Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla.
f. En la medida de lo posible es aconsejable prevenir que se puedan escuchar conversaciones por parte de terceros ajenos utilizando, por ejemplo, auriculares o retirándose a un espacio en el que la persona empleada no esté acompañada.

5. Guardar la información en los espacios de red habilitados
   a. Conviene evitar almacenar la información generada durante la situación de movilidad de forma local en el dispositivo utilizado, siendo preferible hacer uso de los recursos de almacenamiento compartidos o en la nube proporcionados por la organización.
   b. Si se permite la utilización de equipos personales, no utilizar bajo ningún concepto aplicaciones no autorizadas en la política de la entidad para compartir información (servicios en nube de alojamiento de archivos, correos personales, mensajería rápida, etc.)
   c. No se debe bloquear o deshabilitar la política de copia de seguridad corporativa definida para cada dispositivo.
   d. Es recomendable revisar y eliminar periódicamente la información residual que pueda quedar almacenadas en el dispositivo, como archivos temporales del navegador o descargas de documentos.
6. Si hay sospecha de que la información ha podido verse comprometida comunicar con carácter inmediato la brecha de seguridad
   a. Cualquier anomalía que pueda afectar a la seguridad de la información y a los datos personales tratados debe notificarse al responsable, sin dilación y a la mayor brevedad posible, a través de los canales definidos al efecto.
   b. Ante cualquier cuestión que pueda suscitarse en el contexto de las situaciones de movilidad y que puedan representar un riesgo para la protección de la información y el acceso a los recursos corporativos el empleado debe consultar con el Responsable de Protección de Datos y con el responsable de seguridad de la información, o los perfiles responsables designados al efecto, trasladándoles toda información de interés de la que tenga constancia.

I. Registro de jornada laboral

ÁMBITO DE APLICACIÓN

Será de aplicación a todos los empleados/as de la CORREDURÍA.

PRINCIPIOS BÁSICOS DEL REGISTRO DIARIO DE JORNADA

Primero. - Obligación de registro

Con la finalidad de cumplir con lo establecido en el apartado 9 del artículo 34 del Estatuto de los Trabajadores, la CORREDURIA garantizará el "registro diario de jornada laboral" que incluye el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora.

Segundo. - Obligación de registrar

El personal laboral de la CORREDURIA tiene la obligación de cumplimentar con responsabilidad y profesionalidad los datos requeridos en el registro, de conformidad con el principio de buena fe contractual.

El "registro diario de la jornada de trabajo" tiene carácter de deber laboral para todo el personal.

Quienes presten servicios en régimen de teletrabajo o bajo cualquier modalidad de flexibilidad de la CORREDURIA, estarán obligados a cumplir y registrar el horario de trabajo que tengan asignado, siendo irrelevante a estos efectos, que el lugar desde el que se prestan sus servicios no sea el centro de trabajo de la CORREDURIA.

En el supuesto de que la persona trabajadora no cumpliese con la obligación de registro de manera reiterada, falsee o induzca a otras personas al falseamiento de dichos datos, evitando así la veracidad de los datos introducidos, la CORREDURIA podrá requerir su cumplimiento, reservándose el derecho a tomar las medidas disciplinarias procedentes conforme a la legislación vigente.

Tercero. – Modelo de registro de jornada

Para los trabajadores que realicen su labor presencialmente se registra la fecha, horario de entrada y salida mediante un lector de huellas.

Para los trabajadores en situación de teletrabajo se registra el día y hora de primera conexión y de la última desconexión al programa de gestión Elevia.

Cuarto. – Datos de carácter personal

Habida cuenta de la necesidad de incorporar datos de carácter personal al sistema de Registro diario de la jornada, la CORREDURIA se compromete a garantizar el cumplimiento de la normativa vigente en materia de Protección de datos personales según se dispone en el artículo 20 bis del Estatuto de los trabajadores, así como las que se establecen en la Ley Orgánica 2/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales. Dicho compromiso se extenderá en los ismos términos descritos en el supuesto que se hiciera uso de sistemas de videovigilancia o geolocalización.

PROCEDIMIENTO DEL REGISTRO DIARIO DE JORNADA

CONCEPTOS BÁSICOS

Jornada máxima de trabajo efectivo anual

- La jornada máxima de trabajo efectivo anual será la que resulte del sumatorio de los horarios establecidos en el convenio interno que realiza cada persona durante cada uno de los días laborables durante el año natural.
- En el caso de horarios distintos al general que contemplen trabajo en días festivos, la jornada máxima de trabajo efectivo anual se considerará realizada siempre y cuando se cumpla con el horario establecido.
- A los efectos del cumplimiento de la jornada máxima de trabajo anual, y para aquellas jornadas diarias continuas superiores a 6 horas, se computarán como tiempo de trabajo efectivo los 15 minutos diarios de descanso obligatorio a los que se tiene derecho.

Hora de inicio de jornada

Se entenderá como la hora concreta de inicio la que el empleado registre una vez se encuentre en su puesto de trabajo (artículo 34.5 del Estatuto de los Trabajadores) o en el lugar acordado o convenido con la CORREDURIA.

En caso de que un empleado decida, de forma voluntaria, anticipar su entrada al centro de trabajo o se conecte con antelación por los distintos medios habilitados, ya sea por estar en modalidad de teletrabajo o cualquier otra circunstancia, antes del inicio de la jornada que le corresponda, los tiempos anteriores a su hora de inicio de actividad, en ningún caso serán tenidos en cuenta como tiempo de trabajo efectivo. A esto se le añade una excepción, cuando se produzcan circunstancias que precisen del inicio de la jornada anterior al inicio oficial que corresponda, como podría considerarse la preparación de algún evento o actividad puntual que requiera una preparación previa al inicio de jornada establecido.

Hora de finalización de jornada

Se entenderá como la hora concreta de finalización aquella que el empleado indique encontrándose en su puesto de trabajo (artículo 34.5) o en el lugar acordado o convenido por la CORREDURIA.

En todo caso, una vez indicada la hora concreta de finalización, el empleado no podrá realizar ninguna actividad laboral hasta la próxima hora de inicio.

Tiempo de trabajo efectivo

Será aquel que transcurra entre el inicio de la jornada y su finalización, habiendo descontado los tiempos utilizados en pausas o interrupciones de carácter personal, siempre que no tengan la consideración de trabajo efectivo.

A los efectos anteriores, **no se considerará tiempo de trabajo efectivo**, a modo de ejemplo, los tiempos que se utilicen para:

- La pausa de la comida, cuando se presten servicios en régimen de jornada partida y para aquellos horarios que explícitamente lo tengan contemplado. El tiempo mínimo de comida que esté dispuesto para los horarios regulados por la

CORREDURIA será descontado, y cualquier exceso de dicho mínimo deberá ser registrado por el empleado;
- Interrupciones que obedezcan a una razón personal que superen 10 minutos al día (fumar, café, llamadas personales, etc.);
- Las ausencias del centro de trabajo o puesto para resolver asuntos personales, que no estén comprendidas dentro de las licencias retribuidas, que hayan sido debidamente o informadas y/o autorizadas por el responsable.

Por otro lado, **tendrá la consideración de tiempo de trabajo efectivo** los supuestos que se describen a continuación:

- Los 15 minutos diarios de descanso obligatorio siempre que la jornada diaria exceda de 6 horas;
- Tiempo dedicado a la formación obligatoria y a la formación exigible legalmente para el desempeño del puesto de trabajo (presencial y online), tanto dentro como fuera del centro de trabajo;
- La asistencia a reuniones, tanto si el horario de las mismas está dentro como fuera de la jornada laboral;
- Las licencias retribuidas existentes en el convenio colectivo, acuerdo de empresa y legislación vigente;
- Cualquier otro supuesto que tenga consideración de tiempo de trabajo.

Vacaciones

Las vacaciones anuales podrán disfrutarse durante el año natural en que sean devengadas y hasta el día 15 de enero del año natural siguiente, siempre de manera consensuada con el responsable.

METODOLOGIA: REGISTRO DE LA JORNADA DIARIA DE CADA PERSONA

Funcionamiento

El trabajador deberá registrar la hora de inicio de su jornada y la hora de finalización de la misma, según el sistema proporcionado por la CORREDURIA.

Procedimiento de excepción

Se establece un procedimiento de excepción para aquellos casos en los que la persona trabajadora haya olvidado, de forma puntual, registrar su hora de inicio o finalización de la jornada, o no haya sido posible por motivos técnicos o por cualquier otra causa debidamente justificada, siendo necesario cumplimentar el registro lo antes posible y en todo caso dentro del plazo permitido, que es hasta el día 10 del mes siguiente.

Estas circunstancias quedarán asociadas al registro, de forma que, en todo momento, permanezca visible e inalterable la trazabilidad del proceso. La persona trabajadora podrá ver en su registro y resúmenes mensuales, el estado de su registro.

Por otra parte, se establece una flexibilidad de 15 minutos en la hora de entrada, compensable en la hora de salida para todas aquellas jornadas y horarios que actualmente no dispongan de flexibilidad horaria.

Participación en actividades extraordinarias o eventos

En el supuesto de que, puntualmente, por motivo de alguna actividad extraordinaria o evento, deba realizarse el inicio de la jornada antes de la hora ordinaria de cada empleado, se considerará como tiempo de trabajo efectivo. Para que sea así, deberá contar con la validación del responsable directo.

Viajes o desplazamientos

- **Desplazamiento con motivo de visita al centro de trabajo del cliente:**

En el supuesto que el empleado no inicie o finalice su jornada de trabajo desde su de trabajo habitual y se desplace directamente a o desde la empresa del cliente, las horas efectivas de trabajo se iniciarán o finalizarán con referencia al domicilio del empleado descontando 30 minutos por trayecto en concepto de in itinere o 60 minutos si se trata del trayecto ida y vuelta.

Las horas que puedan exceder de la jornada diaria deberán registrarse como "viaje de trabajo".

- **Viajes nacionales**

En el supuesto que el empleado tenga que realizar un desplazamiento a nivel nacional en el que se requiera utilizar un medio de locomoción (tren, avión, etc), el cómputo de horas efectivas de trabajo se considerará tomando la hora de inicio y regreso de dicho medio, descontando 30 minutos por trayecto en concepto de in itineri o 60 minutos si se trata del trayecto de ida y vuelta.

Las horas que puedan exceder de la jornada diaria deberán registrarse como "viaje de trabajo".

- **Viajes internacionales**

Los viajes internacionales serán registrados como "viaje internacional", no computándose el tiempo del desplazamiento por estar comprendida su realización dentro de las funciones, responsabilidades y retribución de las personas trabajadoras que los realizan.

HORAS EXTRAORDINARIAS

Consideración de horas extraordinarias

Tendrán la consideración de horas extraordinarias aquellas que se realicen a instancias o con autorización expresa del responsable y sobrepasen la jornada diaria de cada persona trabajadora.

Se establece un margen de referencia de hasta quince minutos de exceso de la jornada diaria, a contar a partir de la hora de salida que corresponda por el horario legal y contractual, que no tendrá la consideración de prolongación de la jornada, y para lo cual se necesitará la autorización del responsable. Este margen de tiempo no será exigible por parte de la empresa ni acumulable de ningún modo por parte de la misma.

Con carácter general no se deberán realizar horas extraordinarias, ni prolongaciones de jornada de trabajo, únicamente de manera excepcional y en momentos puntuales, por necesidades el servicio.

La realización de horas extraordinarias tiene carácter voluntario. Por tanto, es potestad de la persona trabajadora la realización de las mismas.

De realizarse horas extraordinarias, éstas quedan sujetas a los límites y condiciones establecidas en el artículo 35 del Estatuto de los Trabajadores.

Compensación

En el supuesto de que, con la autorización expresa del responsable, se produjesen prolongaciones de jornada, estos excesos se compensarán con tiempos equivalentes de descanso retribuido a disfrutar en las franjas horarias o jornadas completas previamente consensuadas con el responsable.

ACCESIBILIDAD DE LOS DATOS DEL REGISTRO
Conservación de la información del Registro

La información relativa al registro diario de la jornada será conservada por la CORREDURIA durante un plazo de 4 años, estando a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social.

Accesibilidad de los datos del Registro

Por parte del empleado: cualquier empleado podrá acceder en tiempo real a los datos de su registro diario de jornada. No podrá ver el registro de otro empleado.

Datos del registro que las personas trabajadoras podrán visualizar sin menoscabo de que se puedan añadir nuevos en función de la experiencia

- Identificación del empleado
- Fecha
- Centro de trabajo
- Hora de entrada
- Hora de salida
- Marca manual si el dato se ha introducido en un momento diferente a la hora registrada
- Registro preliminar
- Tiempo de prolongación de jornada enviado al responsable para autorizar (bolsa de horas)
- Estado de la autorización de la prolongación de jornada.

J. Desconexión digital

ÁMBITO DE APLICACIÓN

Será de aplicación a todos los empleados/as de la CORREDURÍA.

MEDIDAS

PRIMERA. – Comunicaciones por diferentes medios (correo electrónico, WhatsApp, teléfono, etc.), realizadas fuera de la jornada laboral.

Con el fin de promover un equilibrio entre la vida personal, familiar y laboral, la CORREDURÍA garantizará a sus personas trabajadoras el derecho a la desconexión digital una vez finalizada la jornada laboral. Las personas trabajadoras de la CORREDURÍA tendrán derecho a no responder a ninguna comunicación, fuere cual fuere el medio utilizado (correo electrónico, WhatsApp, teléfono, etc.), una vez finalizada su jornada laboral, salvo que concurran las circunstancias señaladas en la medida QUINTA de este documento.

En este sentido, para hacer un uso más eficiente de la jornada laboral y respetar el tiempo de descanso, no se enviarán comunicaciones por cualquier medio, desde las 18:00h hasta las 8:00h del día siguiente, ni durante los fines de semana, días festivos o víspera de festivo.

SEGUNDA. – Vacaciones, tiempos de descanso, libranzas…

Para garantizar el tiempo de descanso, permisos y vacaciones de las personas trabajadoras, la CORREDURIA garantizará su derecho a la desconexión digital durante el periodo que duren las mismas, en los términos previstos en el apartado anterior.

Las personas trabajadoras tendrán la obligación de dejar un mensaje de aviso en el correo electrónico con la mención de "ausente", indicando los datos de contacto de la persona trabajadora que hubiera sido designada por la empresa para su reemplazo, así como las fechas de duración de los periodos antes referidos.

TERCERA. – Convocatoria y asistencia a reuniones y cursos de formación

A efectos de garantizar el derecho a la desconexión digital en relación con la efectiva conciliación de la vida personal, familiar y laboral, la convocatoria de ***reuniones de trabajo***, presenciales o telemáticas, tanto a nivel interno como las que se lleven a cabo con clientes, así como la ***formación obligatoria***, se realizarán teniendo en cuenta el tiempo aproximado de duración y, preferiblemente, no se extenderán hasta más tarde de la finalización de la jornada ordinaria de trabajo, a fin de que no se vea afectado el tiempo de descanso de las personas trabajadoras. Con carácter excepcional, y siempre que concurran las circunstancias establecidas en la medida Quinta, el apartado anterior no será de aplicación.

CUARTA. – Trabajo presencial/Teletrabajo

La CORREDURIA garantizará el derecho a la desconexión digital tanto a las personas trabajadoras que realicen su jornada de forma presencial como a las que presten servicios mediante nuevas formas de trabajo: Teletrabajo, medidas de flexibilidad.

QUINTA. – Excepciones

No serán de aplicación las medidas que garantizan el derecho a la desconexión digital en los casos en que concurran circunstancias de causa de fuerza mayor o que supongan un grave, inminente o evidente perjuicio empresarial o del negocio, cuya urgencia temporal necesita indubitadamente de una respuesta inmediata. En dichos supuestos, la Compañía que requiera una respuesta de la persona trabajadora, una vez finalizada su jornada laboral, contactará con aquella preferiblemente por teléfono para comunicarle la situación de urgencia que motiva dicha situación. De esta forma, el tiempo de trabajo así

requerido podría calificarse como hora extraordinaria, de conformidad con lo establecido en cuanto a jornada y/o política de horas extraordinarias en el marco laboral de la empresa propia de la persona trabajadora.

SEXTA. – Acciones de formación y sensibilización

La CORREDURIA implementará las medidas de sensibilización sobre las que se ampara el derecho a la desconexión digital. Para lo cual se informará y/o formará a las personas trabajadoras sobre la necesaria protección de este derecho, teniendo en cuenta las circunstancias, tanto laborales como personales de todas las personas trabajadoras, y para ello se pondrá a disposición de las mismas, toda la información y/o formación que precisen para la comprensión y posterior aplicación de las mencionadas medidas protectoras del derecho a la desconexión digital.

Corresponde a quienes tengan la responsabilidad sobre un equipo y/o superiores jerárquicos de las personas trabajadoras, fomentar y educar mediante la práctica responsable de las tecnologías y con el propósito de dar cumplimiento al derecho a la desconexión digital.

SÉPTIMA. – Compromisos

Las personas trabajadoras se comprometen al uso adecuado de los medios informáticos y tecnológicos puestos a disposición por la CORREDURÍA, evitando en la medida de lo posible su empleo fuera de la jornada estipulada. Quienes tengan la responsabilidad sobre un equipo de personas deben cumplir especialmente las políticas de desconexión digital, al ser una posición referente respecto a los equipos que coordinan. Por lo tanto, los superiores jerárquicos se abstendrán de requerir respuesta en las comunicaciones enviadas a las personas trabajadoras fuera de horario de trabajo o próximo a su finalización, siempre que pudieran suponer para los destinatarios de las mismas la realización de un trabajo efectivo que previsiblemente pueda prolongarse e invadir su tiempo de descanso. Por ello, las personas destinarias de la comunicación tendrán derecho a no responder a la misiva hasta el inicio de la siguiente jornada laboral. En este sentido, en caso de enviar una comunicación que pueda suponer respuesta fuera del horario establecido al efecto, el remitente asumirá expresamente que la respuesta podrá esperar a la jornada laboral siguiente.

OCTAVA. – Derecho a la desconexión digital

La CORREDURIA reconoce y formaliza el derecho a la desconexión digital como un derecho, no como una obligación, aplicable a todas las personas trabajadoras. Esto implica expresamente que, aquellas personas trabajadoras que realicen comunicaciones fuera del horario establecido en esta política podrán hacerlo con total libertad; sin embargo, deben asumir que no tendrán respuesta alguna hasta el día hábil posterior. Las únicas excepciones serían las reconocidas en la medida QUINTA de esta política, por lo que, para procurar la intervención o respuesta de alguna persona trabajadora, deberían aplicarse los mecanismos previstos en dicha medida.

La CORREDURIA no podrá sancionar disciplinariamente a las personas trabajadoras con ocasión del ejercicio por parte de estas últimas de su derecho a desconexión digital en los términos establecidos en esta política. El ejercicio del derecho a desconexión digital no repercutirá negativamente en el desarrollo profesional de las personas trabajadoras.

NOVENA. - Vigencia

La vigencia de esta política se iniciará con la comunicación formal por parte de la CORREDURIA a sus empleados, a través del correo electrónico.

Esta política se incorpora a la Normativa interna ya existente en la CORREDURÍA, normativa que el empleado se compromete a cumplir y hacer cumplir con la firma del Acuerdo de confidencialidad.
Cada vez que haya una modificación, ésta será incorporada a la Normativa interna existente, comunicándoselo nuevamente a los empleados.

K. Relativas al canal de comunicación del empleado

Informar al empleado de la existencia del siguiente procedimiento para la comunicación interna de infracciones sobre la normativa de distribución de seguros:

- Todo empleado dispone de un Canal de Denuncia de infracciones sobre la normativa de distribución de seguros cometidas dentro de La Correduría.
- Dicho Canal está accesible a través del dominio: www.canaldenunciasmediadores.com
- La Correduría ha suscrito un acuerdo con la entidad SOLVENTO CONSULTING PARTNER, S.L., para adherirse a su Canal de Denuncias internas (regulado en el art. 199 del RDL 3/2020, de 4 de febrero), y cuyas características se detallan a continuación:
    - **Finalidad**: Este canal tiene por objeto que los empleados de La Correduría dispongan de procedimientos adecuados para notificar infracciones a nivel interno sobre la normativa de distribución de seguros. Estas infracciones se regulan en el artículo 192 del RDL 3/2020, de 4 de febrero.
    - **Confidencialidad del procedimiento**: El procedimiento establecido en el Canal de Denuncias garantiza la confidencialidad tanto de la persona que informa de las infracciones como de las personas físicas presuntamente responsables de la infracción.
    - **Ausencia de represalias contra los denunciantes**: Conforme a lo establecido en el apartado 3 del artículo 199 del RDL 3/2020, de 4 de febrero, La Correduría adherida se compromete a garantizar que los empelados que informen de las infracciones cometidas en la entidad sean protegidos frente a represalias, discriminaciones y cualquier otro tipo de trato injusto.
    - Procedimiento de denuncia: Para conocer en detalle el procedimiento de denuncia vigente puede acceder a la sección "¿Cómo funciona? De la página web www.canaldenunciasmediadores.com.
    - Presentar una denuncia: En la sección "Denunciar" de la página web www.canaldenunciasmediadores.com se ha habilitado un formulario para la presentación de denuncias.

L. Relativas a la propiedad Intelectual e Industrial

- ❖ Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de programa informático protegidos por los derechos de propiedad intelectual o industrial.
- ❖ Se prevén severas sanciones a los usuarios que lleven a cabo la instalación de dichos programas, debido a que su acción podría ocasionar serias responsabilidades civiles y/o penales a la Correduría.

M. Relativas a aspectos generales

- Se informa al trabajador que todas las conversaciones telefónicas son grabadas por motivos de calidad, pudiendo servir como prueba tanto por parte del trabajador como por parte de la Correduría, en caso de conflicto.
- Se prohíbe revelar a persona alguna ajena a la Correduría, información a la que hayan tenido acceso en el desempeño de sus funciones, sin la debida autorización.
- Se prohíbe utilizar cualquier información que hubiese podido ser obtenida por su condición de empleado de la Correduría, con cualquier otro fin que no sea el estrictamente necesario para el desempeño de sus funciones en la propia la Correduría.
- Es obligación de los usuarios cumplir la normativa vigente y lo dispuesto en el Documento de Seguridad, en relación a la protección de los datos de carácter personal.
- Los usuarios deberán cumplir con los compromisos anteriores, incluso después de extinguida la relación laboral con la Correduría.
- El trabajador será responsable frente a la Correduría y frente a terceros de cualquier daño que pudiera derivarse del incumplimiento de los compromisos anteriores, y resarcirá a la Correduría por las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Aprobado por

La Dirección: Angel Vila	***Responsable de RRHH: Nombre persona***
Firma	***Firma***