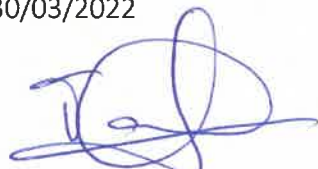


POLITICA DE PRIVACIDAD CORPORATIVA

Edición	Fecha aprobación	Descripción
00	30/03/2022	Edición inicial

ELABORADO: Beatriz Lamenca Responsable de procesos 18/02/2022  FIRMADO	REVISADO: Tanía González 30/03/2022  FIRMADO	APROBADO: Alberto Fernández Cladera Director general 30/03/2022 43158801Z ALBERTO FERNANDEZ (R: A57648388) Firmado digitalmente por 43158801Z ALBERTO FERNANDEZ (R: A57648388) Fecha: 2022.03.30 13:24:21 +02'00' FIRMADO
--	--	--

Contenido

1.	OBJETO.....	2
2.	ALCANCE Y ASPECTOS GENERALES.....	2
3.	DESARROLLO	2
3.1.	Delitos de descubrimiento y revelación de secretos empresariales.....	2
3.2.	Delitos contra la intimidad y allanamiento informático y el delito de daños informáticos.	4
3.3.	Confidencialidad de la información.	5

1. Objeto

En el desarrollo de la implementación del Sistema de Gestión de Cumplimiento Penal (en adelante, el "SGCP") se ha detectado la necesidad de definir y compilar la información referente a la Política de Privacidad Corporativa de la organización, que se encontraba disgregada, y así identificar los requisitos aplicables a la actividad de **GHCM/OPERADORA** y establecer el contenido y metodología aplicables.

2. Alcance y aspectos generales

La política se circunscribe a los empleados y colaboradores de **GHCM/OPERADORA**.

Se considera una violación de secretos empresariales:

- 2.1. La obtención de dichos secretos sin el consentimiento de su titular (acceso, apropiación o copia no autorizada de documentos, objetos, materiales, ficheros u otros soportes).
- 2.2. El incumplimiento del compromiso de confidencialidad adquirido por el trabajador con **GHCM/OPERADORA**.
- 2.3. Cualquier otra actuación que se considere contraria a las prácticas comerciales leales.

El deber de secreto resulta exigible, tanto durante la prestación de los servicios, como con posterioridad a la extinción de su relación con la empresa, ello con independencia de los motivos y forma en que haya tenido lugar dicha extinción.

Por lo tanto, el personal de **GHCM/OPERADORA** está obligado a respetar, en todo momento, tanto la confidencialidad de la información, incluidos los datos personales a los que tienen acceso los empleados en el marco de la relación laboral mantenida con la organización, así como la ley de secretos empresariales. En caso contrario, la organización podrá tomar las medidas legales que considere oportunas, incluyendo la adopción de medidas disciplinarias y, en todo caso, podrá ser causa de reclamación de indemnización por daños y perjuicios, así como, de haber mediado retribución por su revelación, uso o difusión, la exigencia de entrega de la misma, o de su valor equivalente, a la Empresa.

3. Desarrollo

3.1. Delitos de descubrimiento y revelación de secretos empresariales

La Política de privacidad corporativa establece que todas las personas de la organización, independientemente de su puesto de trabajo, están obligadas al secreto profesional en relación con toda la información que conozcan en el desempeño de su trabajo e infringir el deber de secreto, puede tener consecuencias laborales, civiles y penales.

Debe garantizarse la confidencialidad de toda la información que se trata en **GHCM/OPERADORA** por parte de todos sus trabajadores y colaboradores, siendo muy importante tener en cuenta que el deber de secreto se mantiene más allá de la finalización de la relación laboral. Por lo tanto, el deber de secreto no se extingue cuando finaliza la relación con la empresa, si no que se mantiene siempre: no caduca.

Para garantizar el cumplimiento de esta obligación, **GHCM/OPERADORA** como responsable, obtendrá de cada uno de sus empleados y colaboradores, de forma inexcusable, compromiso estricto de confidencialidad (**Cláusula de información y deber de secreto profesional**), que se firma al inicio de la relación laboral del empleado o colaborador de la Sociedad Concesionaria.

Se define como secreto empresarial, cualquier información o conocimiento (tecnológico, científico, industrial, comercial, organizativo o financiero), cualquiera que sea su soporte:

- Sea secreto, por lo tanto, no sea fácilmente accesible ni conocido.
- Tenga un valor empresarial real o comercial, por su carácter secreto.
- Ser objeto de medidas razonables para mantener su carácter secreto.

Desde listados de precios a tarifas, a listados de proveedores o clientes, a estrategias comerciales, protocolos, manuales e instrucciones técnicas, correspondencia, documentación o comunicaciones con los clientes, organigramas o funcionamiento interno de la empresa, datos financieros, presupuestos, la lista de información y documentación confidencial es extensa.

Por ello, la información que se entiende como secreto empresarial en la organización no puede ser copiada, entregada, revelada o facilitada por los empleados o directivos de **GHCM/OPERADORA** fuera de los cometidos propios de su actividad de trabajo y para los objetivos que se le hayan establecido o autorizado.

Actualmente, está en vigor la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, que protege el secreto empresarial y establece un régimen de penalizaciones por no respetar el secreto empresarial por parte de los trabajadores. Queda al margen de la protección de esta ley, la información de escasa importancia, la experiencia y las competencias adquiridas por los trabajadores durante el normal transcurso de su carrera profesional y la información que es de conocimiento general o fácilmente accesible es los círculos en que normalmente se utilice el tipo de información en cuestión.

Se considera una violación de secretos empresariales la obtención de dichos secretos sin el consentimiento de su titular (acceso, apropiación o copia no autorizada de documentos, objetos, materiales, ficheros u otros soportes), el incumplimiento del compromiso de confidencialidad adquirido por el trabajador con la Sociedad Concesionaria o cualquier otra actuación que se considere contraria a las prácticas comerciales leales. Por lo tanto, los trabajadores de **GHCM/OPERADORA** están obligados a respetar la cláusula de confidencialidad, así como la ley de secretos empresariales. En caso contrario, la concesionaria podrá tomar las medidas legales oportunas, aplicar las sanciones disciplinarias pertinentes que pudieran corresponder de conformidad con la legislación vigente, sino también a reclamar al usuario los daños y perjuicios que la vulneración de este deber de confidencialidad pueda producir o que se deriven de ella.

Por lo que, tras la finalización de la relación profesional con la empresa por cualquier causa, el empleado deberá devolver todos los documentos, archivos y materiales que contengan información confidencial, incluidas las herramientas telemáticas que tengan en su poder, dispositivos digitales, sin poder reservarse para sí copia alguna ni extracto de los mismos. Asimismo, en caso de suspensión de la relación laboral, la empresa se reserva la facultad de solicitar a la persona trabajadora la devolución de los archivos, documentos, materiales y herramientas telemáticas que tenga en su poder.

3.2. Delitos contra la intimidad y allanamiento informático y el delito de daños informáticos.

GHCM/OPERADORA dispone de una serie de **Políticas de Seguridad de la información**, en las que se define el buen uso de los activos de la organización y del tratamiento de la información asociadas, incluyendo los datos de carácter personal.

Estas políticas son de aplicación general y nos remitimos a ellas, para su conocimiento en profundidad. Todo el personal de **GHCM/OPERADORA** debe conocer esa normativa interna ya que afecta a los distintos recursos de la organización, como pueden ser:

- Los puestos de trabajo y sistemas de informáticos o aplicaciones establecidos para acceder a la información.
- Los servidores y entorno del sistema operativo en el que se encuentran los ficheros.
- La documentación impresa.

Para evitar comprometer las medidas de seguridad establecidas, no se podrán realizar las siguientes prácticas, salvo autorización del responsable de Sistemas de Información:

- a) Cualquier uso para fines personales.
- b) Instalar o modificar la configuración de software de los equipos (sistema operativo, programas instalados, etc.)
- c) Realizar conexiones a redes o sistemas externos a la red propia.
- d) Trasladar fuera de las instalaciones habituales de trabajo, equipos, información confidencial o datos de carácter personal, sea en formato automatizado o no; sin la correspondiente autorización y sin garantizar el nivel de seguridad correspondiente con anterioridad a la extracción.
- e) Modificar o desactivar los mecanismos de seguridad para la protección de los recursos informáticos y de los sistemas de información de la organización.

El equipo informático, o estación de trabajo de cada usuario, tendrá una configuración fija en sus sistemas operativos y aplicaciones que, solamente, podrá ser cambiada bajo la autorización de la Dirección de la empresa y por el Departamento de informática. Igualmente, está absolutamente prohibida la instalación de cualquier programa, aplicación o utilidad informática o su supresión sin el consentimiento expreso o escrito de la Dirección o del área informática.

La instalación de dichos programas, aplicaciones o utilidades o su supresión deberá, una vez autorizada, ser llevada a cabo por el Departamento de informática.

- Se ha inhabilitado la instalación de programas informáticos por parte del usuario. La instalación debe siempre realizarse por el Departamento de informática, para asegurarse que se cumple con las medidas de seguridad requeridas y se cuenta con las garantías de soporte correspondientes. Su instalación y uso estará en función de las licencias adquiridas.
- El acceso a Internet debe responder únicamente a fines profesionales. Las conexiones que se produzcan a través de la red deben obedecer a fines propios del puesto de trabajo, con el propósito de obtener el mayor aprovechamiento de los recursos informáticos. El personal debe saber que en el ejercicio de sus funciones laborales representa a la organización por lo que su conducta debe reflejar la ética, profesionalidad, cortesía y responsabilidad correspondiente.
- Por motivos de seguridad y rendimiento, se informa que el Departamento de informática puede monitorizar el uso de Internet, tal y como se recoge en el artículo 20.3 del Estatuto de los Trabajadores.
- Las direcciones de correo electrónico con el dominio **GHCM/OPERADORA** son propiedad de la empresa y se considera un instrumento/herramienta de trabajo que debe ser utilizado sólo con fines relacionados con las funciones del trabajador. Por lo tanto, son herramientas de uso profesional y los usuarios autorizados son responsables del uso que se haga de los mismo. Se debe evitar cualquier práctica que pueda poner en riesgo el funcionamiento y buen uso del sistema.

3.3. Confidencialidad de la información.

Como ya se ha indicado anteriormente, tanto durante la vigencia de la relación laboral como después, el usuario se obliga a mantener la más estricta confidencialidad sobre cualquier información o datos a los que haya tenido acceso durante la vigencia de su relación laboral con la empresa, y que se refieran o estén relacionados en cualquier forma con la tecnología, cuentas, clientes, derechos de propiedad intelectual e industrial, "know-how", métodos, organización, datos personales, contratos o actividades de la empresa, o de cualquier persona o entidad que hubiera tenido contacto con las mismas (la "Información Confidencial").

En orden a garantizar dicha confidencialidad, el usuario únicamente tendrá acceso a la información confidencial que resulte necesaria para el desempeño de sus funciones, mediante la creación y asignación de perfiles de usuario, con sus correspondientes contraseñas de acceso.

- Es responsabilidad de cada usuario evitar que personas no autorizadas, inclusive compañeros de trabajo, tengan acceso a través del equipo informático asignado a la información contenida en el mismo o en la red, al que estas personas no tengan acceso autorizado. A tal efecto, al abandonar el puesto de trabajo (final de la jornada laboral, salida, pausa, descanso, reuniones...) el usuario



deberá apagar el equipo o bloquearlo, de forma que solamente pueda reanudarse la sesión mediante la introducción nuevamente de usuario y contraseña personal:

- Para una mejor conservación, organización, control y protección, todo documento informático relativo a la empresa deberá guardarse en el servidor, en el directorio designado por el departamento de informática, no pudiendo almacenarse en las unidades de disco duro u otro dispositivo, salvo que exista autorización expresa por parte de la dirección de la empresa.
- Con carácter general, el uso de memorias USB, discos duros externos, no está autorizado. Por ello, aunque no están deshabilitados los puertos USB de los equipos informáticos, se limita su uso por parte de los usuarios a requerimiento específicos de comunicaciones con las partes interesadas, en concreto, con el IbSalut.
- No está permitido almacenar datos de carácter personal de los empleados en los ordenadores que la empresa les facilite, ni en ningún otro al que tengan acceso por su actividad profesional.

Todos los empleados de la Sociedad Concesionaria y demás personas obligadas respetarán de forma rigurosa las normas sobre protección de datos que se comunican en el Plan o Manual de Acogida.