1. Objetivo

El presente documento establece las normas de usos aceptables para los distintos activos que intervienen en los Sistemas de Gestión de la Seguridad de la Información y de Gestión del Servicio, de **QUENTAL**.

2. Definiciones

- **ENS**: Esquema Nacional de Seguridad.
- **SGSI**: Sistema de Gestión de la Seguridad de la Información. **De aquí en adelante, nos referiremos tanto a ISO 27001, como al ENS cuándo tratemos el SGSI**. El alcance de ambos Sistemas es el mismo, están alineados y son equivalentes.
- **SGS**: Sistema de Gestión del Servicio.

3. Uso de Equipos

Los usuarios deben cumplir las siguientes medidas de seguridad para el uso de los ordenadores personales, objeto del alcance:

- No está permitido alterar la configuración física de los equipos, ni conectar otros dispositivos a iniciativa del usuario, así como variar su ubicación.
- Cada usuario será responsable de la información almacenada en el ordenador que tenga asignado, y de su almacenamiento en los sistemas de información corporativos, o en su defecto en las carpetas compartidas.
- Se recomienda encarecidamente y bajo responsabilidad del usuario: NO utilizar, copiar o transmitir información contenida en los sistemas informáticos de su responsabilidad para uso privado, o cualquier otro distinto del servicio al que está destinado.
- El usuario debe bloquear el equipo siempre que se ausente de su puesto de trabajo.
- Los ordenadores portátiles tienen la misma consideración y se rigen por estas mismas normas.

4. Uso de Aplicaciones

Los usuarios deben cumplir las siguientes diligencias:

- Será responsabilidad del usuario la instalación, ejecución o descarga, sin autorización por parte del Responsable del SGSI, de aplicaciones en el ordenador de trabajo asignado, salvo que estén autorizadas expresamente. Quental se reserva el derecho de auditar, eliminar e incluso formatear completamente el equipo, sin previo aviso. Cualquier uso ilegal (copia de software, software malicioso, ficheros indecorosos, incumplimiento de condiciones del proveedor y/o fabricante del software, etc…) será responsabilidad del usuario, pudiendo

Quental tomar todas las medidas oportunas que crea convenientes, sanciones o incluso la imposición de medidas disciplinarias (faltas leves o graves) o de carácter legal que sean aplicables.

- No se borrará o eliminará ninguno de los programas instalados legalmente sin autorización por parte del Responsable del SGSI.
- No se introducirán de forma voluntaria, programas que causen o sean susceptibles de causar cualquier tipo de alteración, en los sistemas informáticos de la entidad o de terceros. Siendo el usuario totalmente responsable del daño, pudiendo Quental aplicar las mismas medidas que en el apartado anterior.
- No se desactivarán los programas antivirus y sus actualizaciones.

5. Uso de Contraseñas

- Las contraseñas de acceso al equipo, sistema y/o a la red, objeto del alcance, son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. No está permitido:
    - Emplear identificadores y contraseñas de otros usuarios para acceder al sistema y a la red corporativa, salvo que por necesidades del puesto así se determine y autorice (vacaciones o ausencias).
    - Intentar modificar o acceder al registro de accesos.
    - Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros
    - En general, el empleo de la red corporativa, sistemas, equipos informáticos y cualquier medio puesto al alcance del usuario, vulnerando el derecho de terceros, los propios de la institución, o bien para la realización de actos que pudieran ser considerados ilícitos.
- En caso de que fuera necesario acceder al sistema, en ausencia de un compañero, se solicitará autorización al Responsable de Seguridad, para que se habilite el acceso eventual. Una vez finalizada la/s tarea/s que motivaron el acceso, deberá ser comunicado, de nuevo, al Responsable de Seguridad para la revocación del acceso.
- Las contraseñas no deben anotarse, deben recordarse, o bien archivarse mediante un gestor de claves legal (KeePass).
- Las contraseñas deben cambiarse periódicamente. Los usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente. Esto garantiza el uso privado de las mismas. Se aplicarán las políticas establecidas por sistema, en la configuración de los equipos windows, establecidas a facilitar y controlar su gestión.

ATENCIÓN: *Todo documento en papel es un documento NO CONTROLADO y puede estar desactualizado. Los documentos CONTROLADOS se encuentran en el Sistema Integrado de Gestión Avanzada (SIGA), propiedad confidencial de QUENTAL*

5.1 Política de contraseñas

- En general, las contraseñas han de tener una longitud mínima de 8 caracteres y máxima de 15. En el caso particular de los dispositivos móviles, se permite el uso de un PIN de acceso de 4 dígitos.
- No se puede repetir ninguna de las 5 contraseñas anteriores que se hayan usado.
- Se aplicará el sistema de bloqueo de acceso tras 5 veces seguidas de introducción de una contraseña errónea.
- La sintaxis de las contraseñas será la siguiente:
    - No puede contener el nombre de cuenta del usuario, el email, el nombre completo o partes del nombre completo del usuario (nombre o apellidos).
    - Deberá incluir caracteres de tres de las siguientes categorías:
        - Mayúsculas (de la A a la Z)
        - Minúsculas (de la a a la z)
        - Dígitos de base 10 (del 0 al 9)
        - Caracteres no alfanuméricos (Se puede utilizar los siguientes caracteres especiales: ! @ # $ % * ( ) _ + = : , . ? –
    - No se deben utilizar como contraseña:
        - Palabras que se encuentren en el diccionario (español o extranjero).
        - Palabras derivadas del nombre de usuario o del nombre del servicio al que se accede.
        - Palabras de uso común, como por ejemplo, nombres familiares, animales, compañeros de trabajo, amigos, personajes, términos y marcas informáticos, comandos, compañías comerciales, hardware, software, etc.
        - Fechas de nacimiento y cualquier otra información personal, como por ejemplo la dirección o el número de teléfono.
        - Patrones de letras o números o secuencias de teclado, como ‘aaabbb’,’ qwerty’,’ zxywvu’, ‘123321’, etc…
        - Cualquiera de lo anterior escrito al revés o seguido o antecedido por un dígito (por ejemplo ‘secreto1’ o ‘1secreto’).
        - Palabras derivadas de información personal (del número de teléfono, número de identificación, DNI, fecha de nacimiento, etc…).
    - Las contraseñas no se deben almacenar por escrito, y en ningún caso en lugar visible. Tampoco se deben almacenar contraseñas en ficheros de ordenador sin cifrar o desprovisto de algún mecanismo de seguridad.
    - Se intentarán crear contraseñas que se puedan recordar fácilmente (una forma de recordarlo, por ejemplo, es crear una contraseña basada en una frase fácilmente recordable). Se recomienda el uso de aplicaciones para gestión de contraseñas, aprobadas por la organización (KeePass).

ATENCIÓN: *Todo documento en papel es un documento NO CONTROLADO y puede estar desactualizado. Los documentos CONTROLADOS se encuentran en el Sistema Integrado de Gestión Avanzada (SIGA), propiedad confidencial de QUENTAL*

- No debe utilizarse la misma contraseña en dos servicios distintos.
- No se debe hacer uso de la característica de "Recordar Contraseña" existente en algunas aplicaciones o servicios (Outlook, Internet Explorer, Firefox, Chrome, etc.).
- No se debe emplear la misma contraseña que se utiliza para las cuentas de recursos y servicios de QUENTAL en otras cuentas externas a la organización (acceso a proveedores de servicios personales, acceso a servicios de banco, etc…).
- No se deben compartir las cuentas y contraseñas con ninguna otra persona de la organización. Todas las contraseñas deben ser tratadas como información sensible y confidencial, siendo el usuario responsable del uso que se realice de sus credenciales. En casos excepcionales (ausencia por vacaciones, por ejemplo) se podrá comunicar la contraseña a un sustituto (backup) previa autorización del Responsable del SIGA. Finalizada la necesidad, el usuario deberá cambiar la contraseña que hubiera compartido.

- Las cuentas de equipo de usuario y administración, deberán cambiar la contraseña, como mínimo, cada 180 días. Los equipos tienen habilitadas políticas de seguridad que obligan a dicho cambio y es responsabilidad del usuario cumplirlo.
- Las credenciales proporcionadas por **QUENTAL**, solo son válidas en los equipos autorizados ya que se trata de usuarios locales configurados por el Departamento de Sistemas para cada equipo y usuario.
- Las cuentas de correo genéricas y las cuentas de aplicación son responsabilidad de quien las solicita.
- Cuando el responsable de una cuenta de este tipo es trasladado a otro puesto o dado de baja debe notificar, en un periodo máximo de 15 días, un nuevo responsable para la cuenta. Por otro lado y en el mismo periodo, se debe cambiar la contraseña de dicha cuenta. Como medida preventiva, el Responsable de Sistemas notificará este hecho al superior jerárquico del responsable de la cuenta, y a la cuenta genérica, si fuera el caso, para que se actúe en consecuencia. Si antes de terminar el plazo, no se ha hecho el cambio, se desactivará la cuenta.
- La contraseña del usuario no será visible en las pantallas de las aplicaciones y sistemas correspondientes.
- Las contraseñas provisionales se envían por correo electrónico a la cuenta personal (no de empresa), y el sistema obliga a cambiarla en el primer inicio de sesión.

6. Uso del Correo Electrónico

- Se considera el correo electrónico, objeto del alcance, como un instrumento básico de trabajo. El acceso al correo se realizará mediante una identificación, consistente en un usuario y una contraseña.

- Los envíos masivos de información, así como los correos que se destinen a gran número de usuarios, serán sólo los estrictamente necesarios, previa autorización formal, para que no puedan provocar un colapso del sistema de correo.
- Sólo podrán enviar correos publicitarios, el personal autorizado para ello, en función de su cargo de la compañía y, en este caso, siempre que se cuente con el consentimiento del destinatario.
- No deberá utilizarse el correo electrónico para envíos de información de carácter personal (esto es, salud, ideología, religión, creencias, origen racial o étnico) o sensible. Este envío, únicamente, podrá realizarse en casos expresamente autorizados y si se adoptan los mecanismos necesarios, para evitar que la información no sea inteligible, ni manipulada por terceros.
- No deberán abrirse anexos de mensajes ni ficheros sospechosos, o de los que no se conozca su procedencia.

7. Uso de Memorias USB

En este caso se atendrán a las siguientes diligencias:

- Los dispositivos de almacenamiento, propiedad de **QUENTAL**, se entregarán en calidad de préstamo y para uso profesional. La organización podrá requerir su devolución en cualquier momento.
- El usuario no alterará ni eliminará la función de cifrado de información que incluye el dispositivo, en caso de disponerla.
- El usuario se asegurará, en la medida de lo posible, de que el equipo al que se conecta el dispositivo dispone de antivirus actualizado y operativo.
- Bajo ningún concepto, se prestará el dispositivo a terceros.
- El dispositivo se mantendrá en todo momento bajo vigilancia y custodia del usuario. Nunca, se dejará desatendido y conectado a un ordenador.
- El usuario es responsable de realizar copia de seguridad de los archivos almacenados en el dispositivo (Ej: GDrive).

8. Uso de Carpetas Compartidas

La documentación de trabajo, objeto del alcance, debe estar almacenada preferentemente en los sistemas de información correspondientes o en su defecto, en las carpetas compartidas dispuestas por **QUENTAL** a este efecto (Gdrive).

El uso de las carpetas compartidas deberá atenerse a las siguientes diligencias:

- No se permite el uso de las carpetas compartidas para el almacenamiento de información privada, ajena al objeto del puesto de trabajo del usuario.
- No se permite la creación de carpetas compartidas, en los ordenadores asignados a los usuarios.

- Debe eliminarse de las carpetas compartidas, toda información que por su obsolescencia u otro motivo, haya dejado de ser relevante o útil para la organización.
- No se almacenarán documentos que contengan datos de carácter personal, que no hayan sido expresamente autorizados por **QUENTAL**.

9. Uso de terminales móviles

En este caso se atendrán a las siguientes diligencias:

- Los dispositivos móviles, propiedad de **QUENTAL**, se entregarán en calidad de préstamo y para uso profesional. La organización podrá requerir su devolución en cualquier momento.
- El usuario no alterará ni eliminará la función de cifrado de información que incluye el dispositivo, en caso de disponerla.
- El usuario se asegurará de que su dispositivo tiene activado un sistema de desbloqueo en cada uso que se haga del dispositivo.
- Bajo ningún concepto, se prestará el dispositivo a terceros.
- El dispositivo se mantendrá en todo momento bajo vigilancia y custodia del usuario. Nunca, se dejará desatendido.

10. Acceso Remoto

- Las conexiones remotas a los sistemas de información de **QUENTAL**, objeto del alcance, suponen un riesgo especial para la seguridad de la información transmitida. Por ello, estos accesos deberán estar controlados adecuadamente, con el fin de asegurar la autenticación de los usuarios que acceden, así como la confidencialidad, la integridad y disponibilidad de la información transmitida.
- La posibilidad de acceder remotamente a la red y sistemas de información de **QUENTAL**, objeto del alcance, es una opción y no un derecho. Todas las conexiones externas, de personal de la organización o de terceros, deberán estar debidamente justificadas y contar con la autorización del Responsable de Seguridad.
- Las conexiones remotas a los sistemas de **QUENTAL** requerirán, al menos, el mismo nivel de seguridad exigido para el acceso local o a través de la red de área local.
- Cualquier acceso a Datos de Carácter Personal a través de redes de comunicaciones, deberá estar sujeto a las mismas medidas de seguridad exigibles a los accesos en modo local, de forma que se garantice el mismo nivel de seguridad (Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre).
- Se accederá a los recursos estrictamente autorizados y durante el periodo de tiempo establecido.
- El acceso se realizará a través de la VPN de **QUENTAL** con el cliente OpenVPN con doble factor de seguridad, que requiere además del usuario y contraseña, la instalación de un certificado personalizado**.** Cada usuario autorizado, dispondrá de sus correspondientes

credenciales de acceso. El uso de contraseñas debe cumplir con lo descrito en el apartado *5 Uso de Contraseñas*.

10. Eliminación de Metadatos e Información Oculta de documentos

Para el borrado de Metadatos e Información Oculta de los documentos que se compartan y se transfieran a otras personas, y en especial cuando se publiquen en un servidor web u otro tipo de repositorio de información, realizaremos el borrado con la herramienta PDFelement:

1. Deberá generarse un fichero PDF del documento a compartir.
2. Desde la herramienta vigente, Wondershare PdfElement, se podrá eliminar dicha información (metadatos), a través de la utilidad de “Eliminar Información oculta”.
3. Antes de nada, debe ser usada con minuciosidad, ya que puede también eliminar cualquier otro objeto adjunto al documento, como pueden ser firmas digitales, información añadida a través de plugins y aplicaciones de terceras partes o características especiales de Acrobat Reader, a través de las cuales los usuarios revisan, firman y rellenan documentos PDF.
4. El funcionamiento de “Eliminar Metadatos” con PdfElement:
    - Abre un documento PDF en PDFelement, ve a la pestaña "Archivo" y elige la opción "Propiedades"> "Descripción", luego podrás ver los metadatos del documento PDF.
    - Con el ícono del lápiz se pueden editar y eliminar como lo deseas. Selecciona la información que deseas eliminar y utiliza el botón "Retroceso" o "Eliminar" en el teclado para eliminar la información de metadatos

    La herramienta permite previsualizar los ítems de metadatos e información oculta previamente a seleccionarlos para su borrado. De esta forma podemos acceder a los ítems para modificarlos (por ejemplo, en el caso de metadatos), y desactivarlos en caso de que una vez modificados ya no nos interese eliminarlos.

11. Incumplimiento

QUENTAL podrá suspender el uso de estos recursos, objeto del alcance, a aquellos usuarios que contravengan la presente normativa y en los casos en los que cualquier circunstancia sobrevenida lo aconseje.

Si el posible trastorno causado a otros usuarios o al servicio, por un usuario, se entiende que no afecta de forma inmediata al buen funcionamiento del servicio, se le notificará su mal proceder mediante correo electrónico u ordinario. Si por el contrario, se entendiera que el trastorno producido altera el buen funcionamiento del servicio, objeto del alcance, el Responsable de Seguridad, a través del personal del área de sistemas, tendrá la facultad de tomar las medidas necesarias para restaurar de forma inmediata el correcto servicio. Entre otras medidas a aplicar, se contempla la desconexión o inhabilitación de las cuentas en los servidores, objeto del alcance, e inhabilitar el acceso a la red, del ordenador/usuario o grupo de ordenadores/usuarios, objeto del alcance, que están generando el mal funcionamiento.

Asimismo, en caso de que el incumplimiento de esta norma, conlleve alguna de las faltas recogidas, en el régimen disciplinario contemplado en el Convenio Colectivo, vigente en **QUENTAL**, se aplicarán las sanciones correspondientes.

ATENCIÓN: *Todo documento en papel es un documento NO CONTROLADO y puede estar desactualizado. Los documentos CONTROLADOS se encuentran en el Sistema Integrado de Gestión Avanzada (SIGA), propiedad confidencial de QUENTAL*