POLÍTICA DE SEGURIDAD INFORMÁTICA Y USO DE DISPOSITIVOS DE HOLALUZ

1. Objeto

El objeto del presente documento es regular la Política de Seguridad Informática y Uso de Dispositivos de HOLALUZ-CLIDOM, S.A. (en adelante, Holaluz), a fin de establecer recomendaciones, protocolos, procedimientos de seguridad de la información y datos, control de accesos y encriptado.

2. Ámbito de aplicación

a. Objetivo

La presente política resulta de aplicación a todas las áreas de actividad de Holaluz que hagan uso de dispositivos informáticos.

b. Subjetivo

Esta política resulta aplicable a todas las personas que trabajen o colaboren con Holaluz y hagan uso de dispositivos informáticos y/o accedan de forma autorizada a sus sistemas.

3. Arquitectura del sistema y medidas de protección

Serán explicados en un Anexo al presente documento que será actualizado periódicamente por el CTO de la compañía.

4. Medios y dispositivos

4.1.- Uso

Holaluz pondrá a disposición de los trabajadores que lo requieran los medios e instrumentos informáticos y tecnológicos para el desempeño de las tareas que les hayan sido encomendadas, incluyendo el acceso a Internet y una dirección de correo electrónico, así como, dependiendo de cada caso, un dispositivo de sobremesa (PC), un ordenador portátil, teléfono móvil y/o una *tablet*. Concretamente, Holaluz podrá proporcionar a los trabajadores para el caso de teletrabajo o bien desplazamientos por razones laborales, los medios necesarios para disponer de una conexión a internet móvil. En este mismo sentido también se pondrán a disposición de los trabajadores las herramientas necesarias para poder hacer uso de los recursos privados de la red de Holaluz.

Dichos medios e instrumentos serán utilizados, con carácter general, con una finalidad eminentemente profesional, si bien se autoriza al Trabajador a que pueda hacer uso de dichas herramientas de trabajo para fines personales, siempre que se realice un uso razonable, proporcionado y conforme al principio de la buena fe de dichos medios e instrumentos, y todo ello con pleno respeto de las medidas y directrices de seguridad de esta Política y aquellas que en cada momento se implementaren. Sin embargo, el Trabajador se abstendrá de hacer un uso recreativo de los medios e instrumentos mencionados. Holaluz procederá a la habilitación de una red privada virtual (VPN) para que los trabajadores se puedan conectar entre ellos y puedan comunicarse, así como compartir datos de forma segura. Bajo ningún concepto, se podrán utilizar otras vías de comunicación (como por ejemplo Whatsapp) para enviar y recibir documentación de la empresa. La documentación deberá ser remitida estrictamente por correo Gmail corporativo, Google Drive o Slack.

Los trabajadores evitarán que los familiares y terceras personas accedan a la información de Holaluz y/o utilicen los dispositivos de Holaluz o del perfil laboral en caso de dispositivo particular. Así, no está permitido que personas ajenas al Trabajador, como por ejemplo los hijos, hagan uso de los ordenadores portátiles, PC, *tablets*, teléfonos móviles proporcionados por Holaluz.

Para aquellos trabajadores que no usen el ordenador portátil de empresa ni PC por usar un perfil laboral dentro de un dispositivo propio, será obligatorio bloquear la pantalla de la estación de trabajo cuando no se encuentre delante. El Trabajador será el único que conocerá la clave de desbloqueo. Esta será una contraseña alfanumérica y se deberá modificar periódicamente (cada 3 meses).

Queda prohibido el uso de memorias USB para almacenar información, también por suponer una fuente de entrada de *malware*. A ser posible, se evitará siempre el uso de este tipo de memorias y se deberá usar Google Drive como fuente de almacenamiento.

El Trabajador deberá evitar, en medida de lo posible, navegar por páginas no seguras ("http"), especialmente en aquellos casos en los que se introduzca información sensible.

El uso adecuado de los sistemas y dispositivos, cuya vulneración tendrá la consideración de falta grave, implica, entre otros, evitar el acceso, desde las herramientas informáticas de trabajo, a webs o sistemas que puedan poner en riesgo la seguridad informática de Holaluz.

4.2.- Credenciales de acceso

Los recursos puestos a disposición de los empleados tendrán asociadas credenciales de acceso en forma de cuenta de acceso y/o contraseña asociada.

El usuario se compromete a custodiar diligentemente las credenciales en sitio seguro y a no cederlas o exponerlas a terceros. Asimismo, se compromete a comunicar al Responsable Técnico cualquier anomalía, sustracción o compromiso detectado en el uso de las credenciales.

El Área de Tecnología irá actualizando el sistema de protección de contraseñas, de forma que se asegure que las contraseñas empleadas sean seguras, que se cambien con una determinada frecuencia de forma preventiva, y que se puedan dar órdenes de cambios de contraseña urgentes ante posibles ataques informáticos recibidos.

4.3.- Instalación de Programas

Está prohibido instalar programas software de cualquier tipo, que no sean parte de la configuración inicial, aunque estos cuenten con licencias de uso.

Excepcionalmente, Holaluz podrá autorizar la instalación de cualquier programa, siendo necesario para ello que el CTO de la Compañía, el CEO o la persona que éstos designen, autorice dicha instalación. Para ello, proporcionaran a la persona una contraseña que tendrá que introducir en el sistema para proceder a la instalación. Los ordenadores estarán bloqueados, de forma que ningún trabajador pueda instalar en ellos ningún problema sin la autorización de las personas a cargo de la seguridad informática.

Por ningún motivo deberán instalarse programas informáticos para espiar o dañar informáticamente (programas de hackeo informático) a la empresa o a terceros.

4.4.- Equipos y medios propios

En el caso de que el trabajador emplee equipos propios para el desempeño de sus tareas de forma remota, deberá asegurarse de que dichos equipos también cumplan con la Política de Seguridad y Uso de Dispositivos de Holaluz. Para ello, el CTO dará instrucciones precisas sobre las precauciones a adoptar en los equipos personales desde los que se acceda de forma remota a los servidores de Holaluz.

Se establecen en el Anexo I a la presente Política, los requisitos para poder operar con Holaluz con equipos propios y/o personales.

4.5.- Uso de la información

Queda terminantemente prohibido, y se sancionará como falta muy grave, la copia de archivos de Holaluz para fines personales. En caso de que el trabajador copiara algún archivo de Holaluz por motivos laborales en un ordenador personal, quedará obligado a destruirlo una vez haya finalizado el trabajo que motivó dicha copia.

4.6.- Facultades de control

Las personas que hagan uso de dispositivos de Holaluz o accedan a sus sistemas quedan advertidas de que Holaluz se reserva la facultad de acceder a los dispositivos o sesiones de acceso a sus sistemas para verificar las actividades desarrolladas con o en los mismos, así como a los efectos de ejercer sus facultades de dirección y control. Dicho acceso se realizará siempre únicamente por indicación del CEO y bajo el control del CTO y se documentará debidamente.

5. Data Breach

En caso de *Data Breach*, la persona que lo detecte deberá ponerlo inmediatamente en conocimiento del CTO de la Compañía, que es el responsable último de la seguridad informática y quien dará las instrucciones pertinentes por email sobre cómo reaccionar ante el *Data Breach*, velando siempre por el máximo respeto a la normativa, y en particular, a la de Protección de Datos.

6. Consecuencias del incumplimiento

El incumplimiento de esta política de Holaluz y de sus normas e instrucciones de desarrollo será sancionado como infracción leve, grave o muy grave en función de la conducta y los daños que ésta genere a la Compañía o a terceros y de conformidad con lo previsto en el Convenio Colectivo y/o contrato aplicable.

Las sanciones serán impuestas por el Comité Directivo, a propuesta de la persona responsable de la persona sancionada y/o del Compliance Officer, y previa audiencia al interesado.

7. Dudas y notificación de incumplimientos

La Política de Seguridad Informática y Uso de Dispositivos será supervisada por el Área de Tecnología de Holaluz, a la cual se dirigirán las dudas o propuestas de mejora.

En todo caso, se recuerda que en caso de que existan indicios de una conducta irregular o de una posible conducta delictiva, existe un canal de denuncia específico a través de la dirección de email alertas@holaluz.com.

8. Formación

El Área de Tecnología realizará las formaciones necesarias para garantizar la correcta aplicación de la presente Política. Asimismo, en caso de que existan quiebras potenciales del sistema de seguridad informático de Holaluz, el Área de Tecnología informará lo antes posible por correo electrónico a todos los obligados por la presente política, quienes deberán seguir tales instrucciones, a fin de que no se produzcan daños a la seguridad de los sistemas de Holaluz.

9. Fecha de aprobación de la política y responsables de la supervisión, desarrollo y actualización de la política

Esta política ha sido elaborada por el Área de Tecnología de Holaluz, con la colaboración del Área Legal y su supervisión, desarrollo y actualización queda asignada a la persona responsable del Área de Tecnología o a la que en cada momento se designe.

Esta política ha sido aprobada por el Consejo de Administración en fecha de 14 de marzo de 2018 y actualizada el 12 de agosto de 2020.

ANEXO I. Requisitos en equipos para operar con Holaluz

● Sistema Operativo	Mínimo: **Windows 10** actualizado hasta la fecha **Actualizaciones** automáticas activadas	Mínimo: macOS Mojave Deseado: **macOS Catalina** **Actualizaciones** automáticas activadas	<u>Linux debian Based</u> Mínimo: Ubuntu 18.04 Deseado: **Ubuntu 20.04** **Actualizaciones** automáticas activadas
● Hardware	**CPU** Mínimo: Intel i5 2,5 GHz Deseado: Intel i7 2,4 Ghz **RAM** Mínimo: 8 Gb Deseado: 16 Gb **RED** Mínimo: conexión de 100 Mbps (4g) Deseado: conexión de 300 Mbps (Adsl / Fibra)	**CPU** Mínimo: Intel i5 2,5 GHz Deseado: Intel i7 2,4 Ghz **RAM** Mínimo: 8 Gb Deseado: 16 Gb **RED** Mínimo: conexión de 100 Mbps (4g) Deseado: conexión de 300 Mbps (Adsl / Fibra)	**CPU** Mínimo: Intel i5 2,5 GHz Deseado: Intel i7 2,4 Ghz **RAM** Mínimo: 8 Gb Deseado: 16 Gb **RED** Mínimo: conexión de 100 Mbps (4g) Deseado: conexión de 300 Mbps (Adsl / Fibra)
● Software	**-Antivirus** instalado, actualizado y activado. (Gratis o de Pago) **-Navegador**, preferiblemente Google Chrome -Recomendado: **Tener acceso a una**	-Navegador, preferiblemente Google Chrome -Recomendado: **Tener acceso a una cuenta en Google** (gratis) y hacer uso de sus aplicaciones: Mail, Calendar, Meets, Drive, Docs, Sheets, Hangouts,	**-Navegador**, preferiblemente Google Chrome -Recomendado: **Tener acceso a una cuenta en Google** (gratis) y hacer uso de sus aplicaciones: Mail, Calendar, Meets,

	cuenta en Google (gratis) y hacer uso de sus aplicaciones: Mail, Calendar, Meets, Drive, Docs, Sheets, Hangouts, Keep, etc. -**Java Actualizado**	Keep, etc. -J**ava Actualizado**	Drive, Docs, Sheets, Hangouts, Keep, etc. -J**ava Actualizado**
• Configuración • Seguridad	-**Usuario separado** de la vida personal, perfil laboral **-BitLocker** activado **-Firewall** activado -Configuración de la conexión de red: como **red de trabajo** -**Bloqueo del usuario** por inactividad a los 10 minutos -Usuario con **contraseña**	-**Usuario separado** de la vida personal, perfil laboral -**FileVault** activado -**Bloqueo del usuario** por inactividad a los 10 minutos -Usuario con **contraseña**	-**Usuario separado** de la vida personal, perfil laboral -**Home encriptada,** preferible con eCryptfs -**Bloqueo del usuario** por inactividad a los 10 minutos -Usuario con **contraseña**
• Política de contraseñas	-Cambio cada **90 días** -**6 caracteres** (como mínimo) -**Complejidad**: 1 mayuscula, 1 minúscula, 1 número y 1 carácter especial (como mínimo) -6 o más, recordadas (no repetir las	- Cambio cada **90 días** - **6 caracteres** (como mínimo) - **Complejidad**: 1 mayuscula, 1 minúscula, 1 número y 1 carácter especial (como mínimo) - 6 o más, recordadas (no repetir las	- Cambio cada **90 días** - **6 caracteres** (como mínimo) - **Complejidad**: 1 mayuscula, 1 minúscula, 1 número y 1 carácter especial (como mínimo) - 6 o más, recordadas (no repetir las

	últimas 6)	últimas 6)	últimas 6)
• Otros	**-MFA** activado para acceder a la VPN, al mail de holaluz y a los servicios que lo permitan. -En caso de usar WIFI, debe tener encriptación **WPA2** -**Usar gestor de contraseñas,** (LastPass, bitwarden, etc.) -**No guardar información sensible** en el ordenador (vaciar papelera de reciclaje)	**-MFA** activado para acceder a la VPN, al mail de holaluz y a los servicios que lo permitan. -En caso de usar WIFI, debe tener encriptación **WPA2** -**Usar gestor de contraseñas** (LastPass, bitwarden, etc.) -**No guardar información sensible** en el ordenador (vaciar papelera de reciclaje)	**-MFA** activado para acceder a la VPN, al mail de holaluz y a los servicios que lo permitan. -En caso de usar WIFI, debe tener encriptación **WPA2** -**Usar gestor de contraseñas** (LastPass, bitwarden, etc.) -**No guardar información sensible** en el ordenador