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. y sus filiales (en adelante, "**Holaluz**"), persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, que constituyen componentes básicos de la seguridad de la información, y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos así como para garantizar la prestación continua de los servicios.

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. Principios

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a Holaluz.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la Compañía que debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual

borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

1. **Principio de cumplimiento normativo**: todos los sistemas de información se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, datos, comunicaciones y servicios electrónicos.
2. **Principio de mejora continua**: se revisará de manera recurrente el grado de eficacia de los controles de seguridad implantados para para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
3. **Principio de gestión del riesgo**: se deben minimizar los riesgos hasta niveles aceptables y buscar el equilibrio entre los controles de seguridad y la naturaleza de la información. Los objetivos de seguridad deben ser establecidos, ser revisados y coherentes con los aspectos de seguridad de la información.
4. **Principio de concienciación y formación**: se articularán programas de formación, sensibilización y campañas de concienciación para todas las personas usuarias con acceso a la información, en materia de seguridad de la información.
5. **Principios de confidencialidad, integridad y disponibilidad**:
    a. Se debe garantizar la **confidencialidad de la información**, de tal manera que solo tengan acceso a la misma las personas autorizadas.
    b. Deberá asegurarse la **integridad de la información** con la que se trabaja, de modo que sea concisa y precisa, incidiéndose en la exactitud, tanto de su contenido como de los procesos involucrados.
    c. Se debe garantizar la **disponibilidad de la información**, asegurándose la continuidad del negocio soportado por los servicios de la información mediante planes de contingencias.
6. **Principio de proporcionalidad**: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
7. **Principio de responsabilidad**: todas las personas que trabajen o colaboren con Holaluz y hagan uso de dispositivos informáticos y/o accedan de forma autorizada a sus sistemas, deben ser responsables en su conducta en cuanto a la seguridad de la información, cumpliendo con las normas y controles establecidos.

4. Arquitectura del sistema y medidas de protección

Serán explicados en un Anexo al presente documento que será actualizado periódicamente por la Dirección de Infraestructura y Seguridad de la compañía.

5. Medios y dispositivos

4.1.- Uso

Holaluz pondrá a disposición de las personas trabajadoras 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 ordenador portátil, teléfono móvil y/o una *tablet*. Concretamente, Holaluz podrá proporcionar a las personas trabajadoras 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 las personas trabajadoras 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. En cualquier caso, la persona trabajadora 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 las personas trabajadoras se puedan conectar entre ellas 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.

Las personas trabajadoras 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 a la persona trabajadora, como por ejemplo los/las hijos/as, hagan uso de los ordenadores portátiles, PC, *tablets*, teléfonos móviles proporcionados por Holaluz.

Para aquellas personas trabajadoras 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. La persona trabajadora será la única 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.

La persona trabajadora 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 inadecuado 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 las personas trabajadoras tendrán asociadas credenciales de acceso en forma de cuenta de acceso y/o contraseña asociada y en el proceso de autenticación deberá utilizar el sistema de doble factor (MFA).

La persona usuaria 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 Equipo 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. Asimismo el Equipo de Tecnología irá actualizando periódicamente la Política de Contraseñas, y que su cumplimiento es aplicable a todo el personal que tenga o sea responsable de una cuenta (o cualquier forma de acceso que admita o requiera una contraseña o clave) en cualquier sistema que se utilice para las actividades de Holaluz.

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/la Director/a de Infraestructura y Seguridad de la Compañía, el/la CEO o la persona que éstos designen, autorice dicha instalación. Para ello, proporcionarán 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 programa 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 la persona trabajadora 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 así como el Procedimiento de uso profesional de dispositivos personales (Bring Your Own Device, “BYOD”). Para ello, el/la Director/a de Infraestructura y Seguridad 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.

En este caso, es de carácter obligatorio la instalación del agente del sistema de gestión de dispositivos (MDM) y el antivirus corporativo para tener una gestión básica y segura de los dispositivos.

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 la persona trabajadora 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 Director de Infraestructura y Seguridad y se documentará debidamente.

6. Data Breach

En caso de *Data Breach*, la persona que lo detecte deberá ponerlo inmediatamente en conocimiento del Director de Infraestructura y Seguridad 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.

El canal para comunicar un Data Breach es el correo electrónico security@holaluz.com o el canal de slack #eng-security.

7. 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 a la persona interesada.

8. Dudas y notificación de incumplimientos

La Política de Seguridad Informática y Uso de Dispositivos será supervisada por el Equipo de Tecnología de Holaluz, al 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 o del siguiente formulario.

9. Formación

El Área de Tecnología realizará las formaciones necesarias para garantizar la correcta aplicación de la presente Política. Asimismo, en caso de que existan

brechas o vulnerabilidades potenciales del sistema de seguridad informático de Holaluz, el Equipo 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.

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

Esta política ha sido elaborada por el Equipo de Tecnología de Holaluz, con la colaboración del Equipo Legal y su supervisión, desarrollo y actualización queda asignada a la persona responsable del Equipo 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 15 de noviembre de 2023.

holaluz

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	Linux debian Based Mínimo: Ubuntu 20.04 Deseado: **Ubuntu 22.04** **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) -**Sistema de Gestión de Dispositivos (MDM)** -**Navegador**, preferiblemente Google	-Navegador, preferiblemente Google Chrome -**Sistema de Gestión de Dispositivos (MDM)** -Recomendado: **Tener acceso a una**	-**Navegador**, preferiblemente Google Chrome -**Sistema de Gestión de Dispositivos (MDM)** -Recomendado: **Tener acceso a una**

	Chrome -Recomendado: **Tener acceso a una cuenta en Google** (gratis) y hacer uso de sus aplicaciones: Mail, Calendar, Meets, Drive, Docs, Sheets, Hangouts, Keep, etc. -**Java Actualizado**	**cuenta en Google** (gratis) y hacer uso de sus aplicaciones: Mail, Calendar, Meets, Drive, Docs, Sheets, Hangouts, Keep, etc. -J**ava Actualizado**	**cuenta en Google** (gratis) y hacer uso de sus aplicaciones: Mail, Calendar, Meets, Drive, Docs, Sheets, Hangouts, Keep, etc. -J**ava Actualizado**
• Configuración • Seguridad	-**Usuario separado** de la vida personal, perfil laboral **-Disco cifrado:** 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 -**Disco cifrado:** FileVault activado -**Bloqueo del usuario** por inactividad a los 10 minutos -Usuario con **contraseña**	-**Usuario separado** de la vida personal, perfil laboral -**Disco cifrado:** Home encriptada, preferible con eCryptfs -**Bloqueo del usuario** por inactividad a los 10 minutos -Usuario con **contraseña**
• Política de contraseñas	-Cambio cada **90 días** -**8 caracteres** (como mínimo) -**Complejidad**: 1 mayuscula, 1 minúscula, 1 número y 1 carácter	- Cambio cada **90 días** - **8 caracteres** (como mínimo) - **Complejidad**: 1 mayuscula, 1 minúscula, 1 número y 1 carácter	- Cambio cada **90 días** - **8 caracteres** (como mínimo) - **Complejidad**: 1 mayuscula, 1 minúscula, 1 número y 1 carácter especial (como

	especial (como mínimo) -6 o más, recordadas (no repetir las últimas 6)	especial (como mínimo) - 6 o más, recordadas (no repetir las últimas 6)	mínimo) - 6 o más, recordadas (no repetir las 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