Para el GRUPO SOUL, es importante una Política que enmarque los procesos y aspectos relacionados con la adecuada gestión de la información que hace parte de las operaciones de la Organización:

- Control de acceso a los sistemas de información y recursos de red.
- Protección de la información de acceso frente a terceros, procedimiento de control de acceso a sistemas de informacion y tecnologías INF-PC-11.
- Garantía de disponibilidad de la información.INF-PP-04 política de backups management.
- Cumplimiento de las obligaciones legales, regulatorias, contractuales y administrativas

Las herramientas y servicios informáticos asignados a cada usuario son para uso limitado a la función institucional.

Toda la información catalogada por las áreas como critica debe contar con copias de respaldo para garantizar su seguridad.

Mediante esta política se formalizará el compromiso de la Organización, desde las áreas directivas para el adecuado proceso de gestión de la información con el fin de garantizar su integridad, confidencialidad y disponibilidad y demás características que contribuyan a la seguridad de la información.

En ninguna circunstancia se podrá divulgar la información clasificada como CONFIDENCIAL o RESERVADA a personas no autorizadas o en espacios públicos o privados.

El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos de la Organización está prohibido.

1. SEGURIDAD FÍSICA Y DEL ENTORNO

1.1 Controles de Acceso

Se debe tener acceso controlado y restringido a la información, servicios, aplicaciones e instalaciones físicas como por ejemplo el DATA CENTER. Todos los permisos y privilegios deben ser concedidos, denegados, limitados o revocados de acuerdo al caso y debe quedar evidencia de ello. Se han establecido procedimientos que aseguran el control de accesos tales como:

1. TH-PC-08 PROCEDIMIENTO D CONTROL DE ACCESO FISICO.

1.2 Seguridad en los equipos

Todos los computadores deberán tener accesos restringidos, mediante claves de ingreso suministrados a cada usuario del equipo.

Toda información institucional en formato digital debe ser mantenida mediante accesos restringidos bajo usuario y contraseña, dentro de los servidores internos de la institución. No se permite el alojamiento de información institucional en servidores externos

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Para los dispositivos móviles se debe aplicar la Política de Dispositivos móviles de uso corporativo (INF-PP-05) en cuanto al control de acceso a través de usuario y contraseña, con el fin de garantizar el acceso a la información, y salvaguardar las bases de datos gestionadas en estas herramientas, cumpliendo con la presente política de seguridad de la información.

2. SEGURIDAD EN HERRAMIENTAS DIGITALES, APLICACIONES, SOFTWARE, BASES DE DATOS:

Para la gestión de la información a través de las herramientas digitales, como software, aplicaciones (app) o bases de datos, se debe asegurar el debido control de acceso, manejo de perfiles de usuarios, gestión de back ups y gestión actualizaciones de seguridad. Con el fin de impedir accesos no autorizados a los sistemas de información.

3. PROHIBICIONES

3.1 Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre en cualquiera de las siguientes conductas y las demás contempladas en la ley 1273 de 2009" (delitos informáticos):

- Suministrar información confidencial o que tenga carácter reservado a quien no tenga derecho conocerla.
- Usar la información con el fin de obtener beneficio propio o de terceros.
- Ocultar la información maliciosamente causando cualquier perjuicio.
- Hacer pública la información sin la debida autorización.
- Descargar software, a través de Internet sin la debida autorización.

- Intentar modificar, reubicar o sustraer equipos de cómputo, software, Información o periféricos sin la debida autorización.
- Capturar sin autorización la información de los accesos de otros usuarios a los sistemas.
- Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
- Utilizar la infraestructura del GRUPO SOUL (computadores, software, información o redes) para acceder a recursos externos con propósitos ilegales o no autorizados.
- Enviar cualquier comunicación electrónica fraudulenta.
- Apropiarse de los aplicativos, desarrollos o información del GRUPO SOUL y publicarla como propio.
- Adueñarse del trabajo de otros individuos, o de alguna manera apropiarse del trabajo ajeno.
- Usar cualquier medio para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
- Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.
- Descargar o publicar material ilegal, o que implique la vulneración de derechos de terceros, o material nocivo usando un recurso del GRUPO SOUL.
- Uso personal de cualquier recurso informático del GRUPO SOUL para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material prohibido.
- Violar cualquier Ley o Regulación Nacional respecto al uso de sistemas de información.
- intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.
- El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes.
- Realice alguna de las conductas tipificadas en la LEY 1273 DE 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos.

Toda violación de esta política se deberá notificar inmediatamente al área de IT, a través de la cuenta de correo it@infectologia.com.co. Se busca asegurar que todos comprendan y respeten la política con el fin de reducir al mínimo el riesgo, protegiendo a todas las personas, así como al GRUPO SOUL.

3.2 Se deberán notificar situaciones tales como:

- Personas ajenas al GRUPO SOUL en el centro de datos de computo sin la debida autorización.
- Correos con virus (correos extraños, redacción sospechosa, solicitudes extrañas).

- Mala manipulación de los recursos.
- Uso ilegal del software.
- Alteración de la información.
- Olvido de documentos confidenciales en la impresora sin supervisión.

4. LISTA DE SOCIALIZACIÓN

Esta política será socializada a todo el personal de la Organización.

ADA DURAN COGOLLO
GERENTE GENERAL

CONTROL DE CAMBIOS				
VERSION ANTERIOR	ITEM MODIFICADO	DESCRIPCIÓN	FECHA DE MODIFICACIÓN Y ACTUALIZACIÓN	
04	1. TODO EL DOCUMENTO	1. SE INCLUYO CONTENIDO 2. SE INCLUYERON PROHIBICIONES 3. SE INCLUYO NOTIFICAR SITUACIONES 4. ELIMINARON PUNTOS 1-1.1-1.2-2-3-3.1-4-5-7-7.1-8-9-10-10.1-12.	14-05-2024	
ELABORÓ JORGE AMAYA DIRECTOR IT	REVISIÓN ADA DURAN GERENTE GENERAL	APROBÓ ADA DURÁN GERENTE GENERAL	REVISIÓN POR VIGENCIA JORGE AMAYA DIRECTOR IT	ÚLTIMA REVISIÓN SGC ZAYDA TORRES DIRECTORA OPERATIVA Y DE CALIDAD
FECHA: 10-05-2024	FECHA: 14-05-2024	FECHA: 14-05-2024	FECHA: 14-05-2024	FECHA: 14-05-2024