POLÍTICAS GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN DE FUNDACIÓN SOLIDARIDAD POR COLOMBIA

ELABORADO POR:	REVISADO POR:	APROBADO POR:
EDWIN ALEJANDRO OLAYA CASTILLO Nombre	VICTORIA ANZOLA Nombre	Nombre
FUNDACIÓN SOLIDARIDAD POR COLOMBIA Empresa	SEQQE S.A.S Empresa	Empresa
Firma	Firma	Firma
Fecha: 15-02-2022	Fecha: 18-08-2022	Fecha:

TABLA DE CONTENIDOS

1. 4***2.***
4***3.***
4***4.***
4***5.***
5**5.1 MARCO JURÍDICO APLICABLE**
5
6. 5***7.***
6***8.***
7***9.***
¡Error! Marcador no definido.*10.*
7***11.***
8**11.1**
¡Error! Marcador no definido.*12.*
¡Error! Marcador no definido.12.1 POLÍTICAS GENERALES
10
12.2 9**12.3**
10**12.4**
11 12.4.1
¡Error! Marcador no definido. 12.4.2
11 12.4.3
11**12.5**
11 12.5.1
12 12.5.2
12 12.5.3
12**12.6**
13 12.6.3 Respaldo (Backup Disco duro Servidor NAS)
15
13. **¡Error! Marcador no definido.*14.***
15**14.2 BASE DE DATOS (RECURSOS HUMANOS)**
18
14.3 BASE DE DATOS DE PROVEEDORES 18
14.4 BASE DE DATOS DE CLIENTES INSTITUCIONALES **18**
14.5 BASE DE DATOS DE CLIENTES OCASIONALES O RECURRENTES **18**
14.6 BASES DE DATOS FÍSICAS **19**
15. 16***16.***
16**16.1 FUGAS DE DATOS**
19
16.2 OBJETIVOS. **20**
16.3 CHECKLIST. **20**

16.4 PUNTOS CLAVE **20**

16.2 BRECHAS DE SEGURIDAD. **20**

TABLA INVENTARIO DE EQUIPOS Y RECOMENDACIÓN **1**

CARTA CERTIFICACION DE LICENCIAMIENTO **2**

17. 18**ANEXO 1 Registro de Aplicaciones del Sistema Informático** **4**

ANEXO 2. Registro de dispositivos Portátiles **5**

ANEXO 3. Control de Acceso de usuarios del sistema informático de la empresa- Contraseñas **6**

ANEXO 4 Formato de Autorización salida de equipos **1**

ANEXO 5 CONTROL CLAVES **2**

ANEXO 6 FORMATO INTERNO **3**

ANEXO 7 UBICACIÓN DE LOS EQUIPOS DE CÓMPUTO E IMPRESORAS **5**

ANEXO 8 FORMATO INTERNO **6**

ANEXO 9. COMPLEMENTO DIGITAL EN EXCEL FORMATO F005 **8**

ANEXO 10 FORMATO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DE EQUIPOS **9**

ANEXO 12 AUTORIZACIÓN ENTREGA FICHEROS 5

1. CONTROL DE CAMBIOS: al finalizar la política

FECHA	VERSIÓN	CONTROL DE CAMBIOS
20/ 02/ 2022	V.1	REVISIÓN POR PARTE DE SEQQE
20/ 02/ 2022	V.2	CORRECCION Y ACTUALIZACION
20/ 02/ 2022	V.3	EN PROCESO DE DESARROLLO DE UN PLAN PARA LOS BACKUP AUTOMÁTICOS
20/ 02/ 2022	V.4	ACTUALIZACIÓN MANUAL DE TRATAMIENTO DE DATOS

20/ 02/ 2022	V.5	CAMBIO Y RETIRO DE PARTES DE LAS POLÍTICAS
20/ 02/ 2022	V.6	ACTUALIZACIÓN DETALLES DE LOS PROCESOS
20/ 02/ 2022	V.7	ACTUALIZACIÓN BASE DE DATOS Y POLÍTICAS DE CLICK PANDA Y ARCHIVOS HOJA DE VIDA
20/ 02/ 2022	V.8	SUGERENCIAS, CHEQUEO DE LAS LICENCIAS Y CERTIFICACIÓN DE MICROSOFT **Página 23**
20/ 02/ 2022	V.9	ACTUALIZACIÓN CONEXIÓN WIFI (DESHABILITACIÓN) Y PROTOCOLOS DE SEGURIDAD VPN.
20/ 02/ 2022	V.10	BRECHAS DE SEGURIDAD
20/ 02/ 2022	V.11	ACTUALIZACIÓN, TABLAS DE CONTENIDO Y ORGANIZACIÓN DE DOCUMENTOS

2. MEDIDAS DE SEGURIDAD

En el marco de la entrada en vigencia de la Ley 1581 de 2012 que desarrolla el artículo 15 de la Constitución Política para la protección de datos, **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** ha elaborado la presente política de seguridad "POLÍTICA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN", que contiene las medidas de seguridad, directrices y garantías legales aplicables para el procedimiento de recolección, tratamiento, uso, circulación y supresión de datos personales.

3. POLÍTICA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN

En consecuencia de lo anterior, **FUNDACIÓN SOLIDARIDAD POR COLOMBIA** se compromete con el cumplimiento de las disposiciones establecidas por la mencionada normatividad relacionadas con la protección de datos, con el propósito de respetar y garantizar los derechos de hábeas data, libertad, autodeterminación informática, intimidad entre otros, de los titulares de la información personal que sea tratada al interior de la organización, en virtud de la existencia de una relación comercial, civil o laboral.

En este sentido, cualquier persona natural que suministre información relacionada con datos personales, tendrá las facultades de autorizar el uso y tratamiento de la misma, actualizarla, corregir o rectificar.

4. OBJETIVO

La política de Gestión y Seguridad de la Información tiene como propósito definir y proporcionar instrucciones específicas, pautas, directrices y reglas para generar una adecuada gestión y seguridad de la información que reposa en la bases de datos en archivos electrónicos y físicos, estableciendo lineamientos para mantener la información tanto física como electrónica y que se encuentre alojada en los Equipos de Cómputo pertenecientes a **FUNDACIÓN SOLIDARIDAD POR COLOMBIA**. de forma segura.

5. ALCANCE

5.1 MARCO JURÍDICO APLICABLE

· Ley 1581 de 2012 y sus Decretos Reglamentarios

La política de Gestión y Seguridad de la Información ha sido elaborada para dar cumplimiento a la Ley 1581 de 2012 y sus decretos reglamentarios y otras normas que la modifiquen , complementen y adicionen. En su Artículo 4, literal, enuncia:

- **Principio de seguridad:** La información sujeta al Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Es política aplicable a todos los empleados, contratistas, consultores, personal externo y toda persona Natural o Jurídica que tenga convenios comerciales y/o laborales con **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** que cuenten con elementos tecnológicos conectados a la red; esta política es aplicable también a todo equipo y/o servicios propietarios o arrendados que de alguna manera tengan que utilizar local o remotamente el uso de red, sistemas de información, recursos tecnológicos de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** así como de los servicios e intercambio de archivos y programas.

DOCUMENTOS Y REGISTROS DE REFERENCIA (SEQQE S.A.S)

1 – HERRAMIENTAS DE EVALUACIÓN DE LOS RIESGOS DEL SISTEMA
2 – MODELO MEDIDAS DE SEGURIDAD RGPD
3 – RNBD MEDIDAS DE SEGURIDAD
4 - GUÍAS

6. DEFINICIONES

AUTORIZACIÓN: Manifestación emitida por el titular de los datos personales, que puede ser expresa o a través de conductas inequívocas, con el fin de legitimar el tratamiento de los mismos. La autorización debe otorgarse a través de consentimiento informado, para asegurar que el titular conoce todos los usos para los cuales será empleada la información que suministre

AVISO DE PRIVACIDAD: Comunicación verbal o escrita generada por el responsable del tratamiento, con el fin de informar al titular de los datos sobre la aplicación de la política de tratamiento de información instaurada al interior de la organización

BASE DE DATOS: Conjunto organizado de datos personales. Las disposiciones sobre protección y tratamiento de datos, no serán aplicables en caso de bases para uso doméstico.

DATO PERSONAL PRIVADO: Según lo establecido por la ley 1581 de 2012, es aquel que por su naturaleza íntima o reservada sólo es relevante para el titular

DATO PERSONAL SENSIBLE: son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, entre otros los relacionados con el origen racial o étnico, la orientación política, las convicciones religiosas, etc.

DATO PÚBLICO: es aquel que no sea privado, semi privado o sensible. Son considerados de esta naturaleza los relacionados con el estado civil de las personas, su profesión u oficio, entre otros

ENCARGADO DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o a través de otros, designado por el responsable, realice el tratamiento de los datos

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o a través de otros, define el modo de ejecutar el tratamiento de los datos personales y la base de datos

TITULAR DE LOS DATOS: Persona natural que cuyos datos serán objeto de tratamiento

TRATAMIENTO DE DATOS: Operación relacionada con la recolección, uso, consulta, almacenamiento, actualización, circulación y supresión de los datos

USUARIO ESTÁNDAR: Es una cuenta limitada que solo puede realizar determinados cambios en el sistema, como, por ejemplo, cambios que solo afecten al usuario (cambiar iconos, fondo, etc) que no afecten al sistema en general como, cambios en el registro o instalar programas.

USUARIO ADMINISTRADOR: Son cuentas con un mayor nivel de privilegios. Los usuarios administradores pueden realizar todo tipo de cambios en el sistema, como cambios en la configuración, en el registro, instalar programas, e incluso cambios sobre el resto de usuarios con menor nivel de privilegios.

USUARIO INVITADO: Es un usuario especial. Tiene los mismos privilegios que un usuario estándar, pero es anónimo y sin contraseña. Es decir, la finalidad de la cuenta de invitado es permitir que cualquier usuario sin cuenta en el equipo pueda iniciar una sesión y utilizar el equipo, sin permisos de instalar programas o modificar la configuración del sistema.

7. CONSIDERACIONES

Esta política engloba todo detalle técnico de las medidas de seguridad de **FUNDACION SOLIDARIDAD POR COLOMBIA.**
Es frecuente escuchar que «el eslabón más importante de la seguridad es el empleado», ya que evitar el error humano es clave para proteger nuestros sistemas y nuestra información. Por ello es importante, además de realizar la oportuna concienciación y formación para fortalecer este eslabón, tomar medidas de seguridad en la gestión de los llamados «recursos humanos».
Una buena manera de garantizar que vamos a contar con una plantilla responsable en materia de ciberseguridad es establecer los oportunos filtros, pruebas y controles en la relación con nuestros colaboradores y empleados, especialmente en las fases de firma y finalización del contrato.

8. RESPONSABLE

Ingeniero Alejandro Olaya Castillo

9. FINALIDAD DE LA POLÍTICA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN

Es preservar la seguridad de los activos y personas que se encuentran en las instalaciones y Puntos de Venta así como la de controlar el ingreso y salida del personal, gestionar estadísticas internas, atención al cliente, fidelización de clientes, envío de comunicaciones, procedimientos administrativos, gestión de claves, administración de usuarios, desarrollo operativo, administración de sistemas de información, recolección de datos personales a través de cámaras de seguridad, para proteger y controlar el ingreso y salida de su personal y activos de sus instalaciones.

- **Visitantes:** Las personas que ingresan temporalmente a las instalaciones principales, esta política está dirigida a garantizar su seguridad personal en caso de una emergencia mientras visitan las instalaciones de Pasta Pronta.

- **Personal interno:** En virtud de la relación laboral, para establecer protocolos y procedimientos de seguridad.

- **Proveedores y Contratistas:** Para garantizar su seguridad física y digital tanto personal como empresarial.

10. APLICATIVO DE SEGURIDAD Y CONTROL

Esta política se aplica a todos los funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones requieren acceso a la información de **FUNDACION SOLIDARIDAD POR COLOMBIA.**

Para garantizar la seguridad de los datos, la empresa cuenta con medios digitales como Firewall, antivirus, para bloquear el acceso no autorizado, los cuales se encuentran para proteger las bases de datos, sitios web, y/o servicios, y concientizar a los usuarios que sean responsables por la administración, protección de la información y las claves que les han sido asignadas.

El acceso a la información de **FUNDACION SOLIDARIDAD POR COLOMBIA.** se otorga bajo los siguientes 10 principios de seguridad informática:

Lo que se necesita conocer: Solamente se concede acceso a la información que la persona o sistema necesitan para la realización de sus tareas. (diferente tarea/rol significa diferentes cosas que necesita saber y en consecuencia diferente perfil de acceso).

1. Un sistema de normas efectivo: Una parte de las medidas organizativas y técnicas requeridas consiste en documentar cómo los “datos” van a ser protegidos. No hay ninguna garantía al 100% contra la pérdida de información, pero si no hay documentos con los procedimientos que empleamos en caso de incidente.

2. Políticas sobre uso aceptable: Educar a los usuarios es una parte importante de un sistema de normas efectivas, y económicas para prevenir incidentes.

3. Antivirus moderno: utilizamos Kaspersky actualizado con la última tecnología moderna de consolas para el monitoreo de virus, con HIPS y tecnologías basadas en la nube para mejor protección

4. Prevención de pérdida de datos: Las políticas de prevención de pérdida de datos se han minimizado e identificado, **FUNDACIÓN SOLIDARIDAD POR COLOMBIA** tiene certificado **SSL** para la página web y para envío de correos por medio de la plataforma **Gsuite**.

5. Política de contraseñas seguras: Las contraseñas tienen complejidad suficiente para que sean robustas, alfanuméricas con una longitud mínima de 8 caracteres.

6. Política de gestión de incidentes: Los incidentes relacionados con seguridad ocurren con frecuencia, por eso se implementó una política de gestión de incidentes. En ella involucramos otros departamentos como contabilidad, financiera, comunicaciones, proyectos. La idea es que en cuanto ocurra algo todos en la empresa sepan lo que tienen que hacer. Con una gestión eficiente conoceremos con mayor prontitud el alcance del incidente, lo comunicaremos correctamente y minimizamos su alcance.

Clasificación de permisos:

- **Usuarios Estándar:** Usuario registrado en el dominio que puede acceder al sistema, pero tiene límites para la instalación y configuración; no puede añadir ni configurar usuarios, no puede editar parámetros del sistema, no puede acceder a las carpetas de otros usuarios, únicamente tiene acceso a la información que el Gerente ha permitido.
- **Usuarios Administradores:** Usuario registrado en el dominio que cuenta con el control total, puede añadir editar y eliminar usuarios, puede instalar editar y eliminar aplicaciones, tiene acceso total a la información, puede mover o eliminar archivos
- **Usuarios invitados:** usuarios que no están registrado en el dominio, su acceso es limitado no tienen acceso a ninguna carpeta de información

Clasificación de recursos:

- Software: Aplicaciones informáticas que permiten gestionar los datos
- Hardware: Equipos que permiten hospedar datos, aplicaciones y servicios
- Infraestructura: Instalaciones que acogen equipos informáticos

El almacenamiento de la información contenida en las bases de datos personales, se encuentra en dos servidores , un HP Proliant con Windows server 2019 y un servidor Western Digital n4000 (NAS) con su licenciamiento dentro de **FUNDACION SOLIDARIDAD POR COLOMBIA,** y cuenta con medidas de seguridad **FÍSICA:** está ubicado en un lugar libre de temperatura humedad, bajo llave y sus equipos están en un Gabinete metálico, organizado y con su nomenclatura, y protección de picos de voltaje por medio de una ups; **LÓGICA**: por medio de un rúter con aislamiento de ip, firewall, y antivirus Kaspersky para protegerlos de virus, anti fichiers, anti malware y otros ataques lógicos que pueden afectar la información; **SISTEMAS**: por medio de una ups de 3kva para la protección de voltajes y transientes de corriente que afecten el hardware de los equipos; y controles de acceso al cuarto de sistemas para garantizar el principio de seguridad, acceso y circulación restringida y confidencialidad.

11. INVENTARIO DE EQUIPOS

En el puesto de trabajo los empleados utilizan como herramienta equipos informáticos: ordenadores, teléfonos móviles, etc. También generan y transmiten información necesaria para el desempeño de sus funciones. Esta información a veces se almacena de manera local en los discos duros de estos equipos, por lo que se hace un levantamiento de información de los equipos, *ver: INVENTARIO EQUIPOS.xlsx* carpeta: **1.Autorizaciones Inventarios y Registros Generales**

12 POLÍTICAS Y PROCEDIMIENTOS INTERNOS

12.1 POLÍTICAS GENERALES

Usuarios

- Conocer y aplicar las políticas y procedimientos apropiados con relación al manejo, gestión y seguridad de los sistemas de información.
- No permitir y no facilitar información y/o documentación perteneciente a **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** a terceros no autorizados.
- No utilizar los recursos informáticos (hardware, software o datos) para otras actividades que no estén directamente relacionadas con el trabajo en **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.**
- El personal que tenga un equipo informático a su cargo tiene la responsabilidad de reportar inmediatamente al departamento de sistemas o a su jefe inmediato, cualquier evento que pueda comprometer los sistemas de información de la compañía y sus recursos informáticos, como por ejemplo virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.
- Reportar inmediatamente al departamento de sistemas cualquier falla que se pueda presentar en el computador o en la red, ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- Todo software utilizado por **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** Está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usarse para fines personales.
- Los usuarios que tienen habilitados medios extraíbles en sus equipos de cómputo como (CD/DVD, memorias USB, etc.), conexiones a redes externas o que poseen privilegios, **NO** deben extraer datos de **FUNDACION SOLIDARIDAD POR COLOMBIA.** sin la aprobación previa de la Gerencia Financiera y Administrativa.
- Se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente autorizado por Gerencia, quien tiene un inventario de Software y está en un archivo en Excel donde está toda la información del licenciamiento de los equipos,
- En caso que un equipo deba ser reparado por parte del departamento de sistemas, es función del usuario tener copias de respaldo como garantía de su información.
- El departamento de sistemas podrá realizar respaldos periódicos manuales de la información de los recursos de cómputo que tengan a su cargo, los cuales serán resguardados en las instalaciones de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.**

12.2 POLÍTICAS DE MANEJO DE LA INFORMACIÓN

Los soportes y documentos electrónicos con datos de carácter personal, están identificados por la información que contienen, y están almacenados en un lugar de acceso restringido en el cuarto de sistemas bajo llave. Solo tiene acceso el personal autorizado por la Gerencia Financiera y Administrativa para su tratamiento en el ejercicio de sus funciones.

Las salidas de documentos sólo serán posibles si están debidamente autorizadas por el Gerente General y/o Administrativo.

- La información almacenada en los equipos de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA** es responsabilidad de cada usuario asignado a este.

- Los usuarios tienen derecho a proteger su información crítica con contraseñas para evitar modificaciones o lecturas “no deseadas”, sin embargo, esta acción debe ser de conocimiento por parte del líder de proceso y en su caso informar a la Gerencia Administrativa.
- En los equipos se almacena información exclusivamente referente a la empresa, se prohíbe el almacenamiento o custodia de información personal dentro de los equipos de cómputo, tales como imágenes, fotografías, archivos de música, archivos de video, documentos, ejecutables, etc.
- Se sugiere a los usuario no configurar carpetas como “privadas” dentro del Sistema, esto para prevenir pérdidas de información en caso de colapsos del Sistema Operativo por que están excluidas de los backup.
- Toda la información generada en el desarrollo de la actividad laboral es estrictamente **CONFIDENCIAL** y solo puede ser compartida a terceros bajo la autorización expresa de la Gerencia o mandatos legales.
- La información generada en el desarrollo de la actividad laboral no pertenece a los Usuarios sino a **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** y/o al Titular de la misma, en concordancia con la Ley 1581 de 2012 y sus decretos reglamentarios.

12.3 POLÍTICA DE USO DE EQUIPOS TECNOLÓGICOS

Dispositivos como portátiles, equipos pos, cpu, servidores, tablet, celulares, propiedad de la empresa que contienen datos personales están expuestos a pérdida o robo, están registrados para poder denunciar cualquier anomalía, incidencia de seguridad o fuga de datos de carácter personal que afecte el cumplimiento de la normativa desarrollada en el Manual de políticas y procedimientos o que pueda afectar a los Datos de Carácter Personal que trata la Fundación, será notificada de inmediato al Delegado de Protección de Datos **DPO** correctamente dicha pérdida, llenando el formato de incidencia de seguridad de equipos de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.**
El usuario autorizado para la utilización de la red **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.**, se compromete con el siguiente reglamento de uso de los recursos informáticos asignados:

- Para solicitar un servicio de soporte correctivo o preventivo para los equipos de cómputo, por disposición del DPO se comunicaran directamente con el ingeniero encargado Alejandro Olaya al telefono 3174348450 o al correo soporteing@solidaridadporcolombia.org y una vez resuelta la solicitud el Ingeniero asignado informará al usuario el procedimiento que fue realizado.
- En cumplimiento de las leyes de propiedad intelectual asociada con la Ley 603 del 2000 que dice: Está prohibida la instalación de cualquier tipo de aplicación que no se encuentre licenciada, autorizada por la Gerencia, al igual que el almacenamiento de archivos personales (No Corporativos) como archivos de música, videos, imágenes, etc., para cualquier instalación de software es necesario emitir un concepto técnico por parte del área de sistemas y la autorización de Gerencia.
- Es responsabilidad del usuario al salir de la compañía hacer la devolución de los equipos tecnológicos, (portatil, celular, equipo de escritorio, tablet, etc) y todos los elementos tecnológicos asignados por **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.**, en las mismas condiciones en las que se le fueron entregadas.
- Está prohibida la instalación y uso de software de socialización: Messenger, Skype, Google Talk, Yahoo!, Facebook, Twitter, Instagram, Spotify entre otros, a excepción de los casos autorizados por la Gerencia General y avalados por el departamento de sistemas.
- Se prohíbe el uso de computadores de uso personal dentro de la red de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.**, sin una respectiva autorización por parte de la Gerencia y previa revisión del departamento de sistemas.

- Está prohibido sacar información digital o física de la empresa o conexiones remotas a no ser que estén autorizados por la Gerencia y el DPO para el teletrabajo o en ocasiones de emergencia que se ameriten.

POLÍTICA DE SEGURIDAD PARA LAS COMUNICACIONES

12.3.1 Propiedad de la Información

Las comunicaciones de forma electrónica, como Teléfono, Correo Corporativo, Seguridad en Red Interna y demás comunicaciones implementadas, generadas y procesadas, incluyendo las copias de respaldo, se consideran propiedad de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** y no de los usuarios·

12.3.2 Uso de los Sistemas de Comunicación

Las empresas que se encargan del mantenimiento de las aplicaciones Informáticas, pueden disponer de conexiones remotas para acceder a los equipos y garantizar un nivel de seguridad equivalente o superior que maneja Fundación Solidaridad por Colombia, en el caso del programa contable siigo ellos manejan su licencia de Team Viewer como soporte remoto controlado por el usuario encargado de su equipo de cómputo y quien se hará responsable del servicio técnico.

- Los sistemas de comunicación de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** sólo deben usarse para actividades de trabajo. El uso de internet ocasional es permisible siempre y cuando esté acompañado por el administrador del área de trabajo y con acceso limitado a los datos de la empresa, y que no interfiera con la productividad del empleado ni con las actividades de la empresa, esta conectividad estará bajo la autorización del Delegado de Protección de Datos y supervisado por el soporte Técnico IT.

12.3.3 Confidencialidad y Privacidad

- No es permitido enviar a través de Internet mensajes con información confidencial. Para tal fin se utiliza la plataforma de **GOOGLE FOR WORKS** (Gmail, Drive, Contactos), u otros productos previamente aprobados por la administración, y el departamento de sistemas.
- Los empleados de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan, si hay alguna sospecha de intrusión, por favor comunicarse al departamento de sistemas o al DPO para cambio de claves y hacer seguimiento para su protección.
- El uso y el contenido de las comunicaciones pueden ser supervisadas para actividades de mantenimiento, seguridad o auditoría, Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

12.4 POLÍTICA DE SEGURIDAD LOGÍSTICA

La política de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** es prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de la información de la empresa, el usuario a cargo del equipo de cómputo es responsable de la integridad de su contenido·

12.4.1 RED

- Ningún usuario se encuentra autorizado para visualizar, copiar, alterar o destruir la información que reside en los equipos de cómputo, sin el consentimiento explícito del responsable del equipo.
- Las cuentas de los diferentes portales, sistemas de información, recursos de cómputo, entre otros son propiedad de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** y deben ser utilizadas única y exclusivamente para las actividades relacionadas con la labor asignada al área de trabajo.
- Todas las cuentas de acceso a los diferentes portales, sistemas de información, recursos de cómputo asignados al usuario son personales e intransferibles, a excepción de los casos autorizados por Gerencia, o por el delegado de protección de datos DPO.
- En el momento que se detecte un uso no aceptable dentro de la red, equipos de cómputo, sistemas de información y demás portales asignados al usuario, el departamento de sistemas realizará el debido bloqueo, desconexión, cancelación o actividades que haya lugar de las cuentas y se informará a la administración, esta acción será temporal o permanente. La reconexión se realizará cuando la administración lo considere.

12.4.2 Acceso a Funcionarios de FUNDACIÓN SOLIDARIDAD POR COLOMBIA.

- El usuario **NO** puede acceder a los servicios de **Wifi** de la empresa desde su celular porque está prohibido por políticas de la gerencia.

12.4.3 Contraseñas y Control de Acceso

Es responsabilidad del jefe de cada área, que determine qué datos son accesibles para cada usuario. Para ello el I.T establece contraseñas para evitar que un usuario tenga acceso a datos que no le han sido asignados, y cada usuario es responsable de su información que se encuentra bajo su responsabilidad en su equipo de computo. Para solicitar un alta, baja o alteración de un acceso es necesario notificarlo por escrito al ingeniero de sistemas, al correo de soporteing@solidaridadporcolombia.org indicando en el mismo el nombre y puesto de trabajo y su solicitud será gestionada por el **DPO**, y el departamento de Sistemas.

- La contraseña inicial para un usuario nuevo es válida para la primera sesión, en ese momento, el usuario debe realizar el cambio de contraseña (aplica para todas las plataformas Windows y correos corporativos), en donde la longitud de la contraseña debe contener mínimo 8 caracteres que incluyan letras en mayúsculas, minúsculas, números y caracteres especiales, y después la clave será enviada al correo de soporteing@solidaridadporcolombia.org para llevar control sobre el cambio de contraseñas.
- Se aconseja a los usuarios usar contraseñas que no sean idénticas o substancialmente similares a contraseñas previamente empleadas, pueden utilizar mayúsculas minúsculas, números y símbolos, y 8 caracteres como mínimo.

.

- Se encuentra prohibido compartir o revelar contraseñas a otros o personal externo a la compañía, el hacerlo el usuario se expone a las consecuencias por las acciones que los otros hagan con su “Login” (Intranet, Impresoras, Equipos de Cómputo, Portales Web, Aplicativos, Bases de Datos, Redes, Acceso a Archivos, entre otros), el único tercero autorizado por la compañía es **el ingeniero encargado de la administración de la red** quién puede saber y gestionar las claves de los usuarios.
- Los usuarios no deben intentar acceder abusivamente al sistema informático, obstaculizar ilegítimamente el sistema informático o redes de comunicaciones, interceptar datos informáticos,

causar daños informáticos, vulnerar o quebrantar los sistemas de seguridad y/o controles de acceso. Acciones de esta naturaleza se consideran violatorios dentro de las políticas de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** y serán sancionadas y evaluadas por la Gerencia.

- Cada 6 meses el sistema de manera automática solicitará cambio de las contraseñas en Windows y en el correo electrónico, y la nueva clave es enviada al correo de **soporteing@solidaridadporcolombia.org** para llevar control sobre el cambio de contraseña en el

- Nivel de acceso **FUNDACION SOLIDARIDAD POR COLOMBIA**

NIVEL	VALORACIÓN	INTEGRIDAD
4	MUY ALTA	Información que no puede ser modificada por ningún usuario. La pérdida de la exactitud o consistencia de esta información no puede repararse y afecta gravemente en su operación, términos legales, bases de datos, información personal de los usuarios.
3	ALTA	Información que solo puede ser Manejada y modificada por la Gerencia, Bases de datos, información personal de la empresa y empleados.
2	MEDIA	Información que solo puede ser modificada bajo la autorización del autor según lineamientos de la Dirección, Jefe de Área, Documentos Compartidos.
1	BAJA	Información que puede ser modificada por el personal de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA**, escáner.

12.5 POLÍTICA DE SEGURIDAD FÍSICA

Las Instalaciones de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** cuentan con los estándares vigentes de cableado estructurado, para el diseño de nuevas áreas o el crecimiento de las mismas, así mismo, se debe garantizar la estabilidad y funcionalidad de la conectividad en las comunicaciones.
El resguardo de los equipos de cómputo se encuentra establecido por parte del departamento de sistemas, quienes cuentan con un control de los equipos, que permita conocer siempre la ubicación física, usuario asignado, especificaciones técnicas, segmento de red, licenciamiento, entre otros.

12.6.1 Física

.
Los equipos de comunicaciones y los servidores se alojan, en una sala de acceso restringido, (Rack ubicado en el quinto piso junto a recepción).
En caso de ser vulnerada la seguridad por causa de un tercero, los equipos cuentan con contraseña de entrada, y los datos más sensibles se encuentran alojados en un servidor NAS como backup y los protocolos se ajustarán según donde se debe llenar el formulario para pasarlos a la policía si es el caso, o reportarlo como equipos dañados para darles de baja.

Limitación al Personal autorizado así:

- Ingeniero de Sistemas: Acceso total a los equipos de empresa.
- Departamento de Contabilidad: Acceso al servidor de Siigo.

En el supuesto de que cualquier persona externa a **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** requiera acceso a dicha Sala, deberá estar acompañada por Personal autorizado de la Empresa.
Cuando se diera lugar a retirar un equipo de las instalaciones de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.,** deberá llenar el el cual debe estar firmado y autorizado por delegado de protección de datos **DPO**, y comunicar su salida al personal de vigilancia para su respectivo chequeo·

12.6.2 Logística

FUNDACIÓN SOLIDARIDAD POR COLOMBIA. Cuenta con medidas de protección que permiten la identificación y autentificación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función.

- Departamento de sistemas IT: Alejandro Olaya Castillo
- Departamento de Contabilidad: Karen Meza

12.6.3 Respaldo (Backup Disco duro Servidor NAS)

El servidor **NAS** de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** es un dispositivo de almacenamiento conectado al segmento de los equipos internos; Su función es hacer copias automáticas de los archivos que los usuarios encargados de cada equipo nos han indicado que son los más sensibles e importantes; llenando el formato interno

El NAS que hay en la empresa se comporta como un ordenador con su propio sistema operativo y que está adaptado para estar todo el día funcionando.

Las copias de seguridad para los equipos de niveles de valorización 3 y 4 está programado para que todos los días se ejecuten entre 6:00 am a 18:00 pm y para los equipos de valoración 1 y 2 se harán copias lunes, miércoles, y viernes, en el horario de 6:00 am a 18:00 pm intercalados para no congestionar la red de datos, la información que previamente es solicitada al usuario de cada equipo es la que se guardará en google drive, siendo el encargado el departamento de sistemas quien gestione y esté pendiente de la tarea.

Los procedimientos para realizar dichas Copias de Seguridad para cualquier nivel, permitirán la reconstrucción de los documentos y base de datos al estado que se encontraba el Fichero al momento de producirse la pérdida o destrucción del mismo, esto va a depender del día y hora en que el backup fue realizado.

El Ingeniero de sistemas, verificará manualmente los procedimientos para realizar dichas copias.

Las copias de Seguridad nivel 1, 2, 3, y 4 se almacenan en un disco duro externo de 2 terabytes de capacidad, y su resguardo está en un lugar seguro donde está protegido de fluctuaciones de voltaje y del hurto.

13 INVENTARIO DE BASES DE DATOS

Al efectuar el inventario de bases de datos se tuvo en cuenta lo siguiente:

- Cantidad de bases de datos con información personal.

Hay (1) bases de datos, SIIGO

- Cantidad de titulares por cada base de datos.

En cada base de datos están las personas encargadas y la información detallada de los canales o medios que se tienen previstos para el soporte, y están alojados en recursos humanos, como: datos de identificación, ubicación, socioeconómicos, etc.

- SIIGO. Soporte técnico de siigo . 6161818

Todos los datos son sensibles y de nivel 3 (Valoración Alta).

- Ubicación física de las bases de datos (almacenamiento en medios propios, como, archivadores o servidores, internos o externos a las instalaciones físicas del responsable).
- Datos de identificación y ubicación de los encargados del tratamiento de la información.

- Medidas de seguridad y/o controles implementados en la base de datos para minimizar los riesgos de un uso no adecuado de la información personal tratada.
- Información sobre la autorización de los titulares de los datos contenidos en las bases de datos teniendo autorización como administrador de cada área.
- Forma de obtención de los datos (directamente del titular o mediante terceros). Directamente del titular
- Cuando se ha realizado transferencia o transmisión internacional de la base de datos, se solicitará la información básica del destinatario.

14 MEDIDAS DE SEGURIDAD DE LAS BASES DE DATOS PERSONALES

Base de datos: Todo conjunto organizado de archivos, registros, archivos, bases o banco de datos personales de los titulares o individuos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados, informáticos, manuales, mecánicos, digitales o electrónicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, cotejo o interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos, así como su bloqueo, supresión o destrucción.

Tipos de bases de datos personales

- Físicos
- Automatizados

MEDIDAS DE SEGURIDAD FÍSICAS Y LÓGICAS

FUNDACIÓN SOLIDARIDAD POR COLOMBIA responsable del tratamiento del sistema de datos personales adoptará las medidas de seguridad conforme a lo siguiente:

Tipos de seguridad:

a) Física. FUNDACIÓN SOLIDARIDAD POR COLOMBIA tiene como medida orientada a la protección de variación de voltaje una UPS Tripp Lite de 3 kva en el rack donde están los servidores de Base de Datos, y está en un lugar seguro con acceso limitado y bajo llave para la prevención de riesgos por caso fortuito.

b) Lógica. FUNDACIÓN SOLIDARIDAD POR COLOMBIA cuenta con el ingeniero Alejandro Olaya Castillo para el soporte y mantenimiento preventivo y correctivo de sistemas de cómputo, en la parte de contabilidad **SIIGO** está la empresa de Informática y Gestión**.**

14.1 ANÁLISIS Y ALOJAMIENTO DE LAS BASES DE DATOS

Las Bases de Datos digitales son almacenadas en un servidor físico que tiene la empresa, uno que es un HP PROLIANT ML350e G8 para la parte de contabilidad y servidor de dominio.

14.2 BASE DE DATOS DE CLIENTES INSTITUCIONALES

Base de datos compuesta por el correo electrónico, dirección de domicilio, número de teléfono y celular de personas que han entregado con su autorización, sus datos a esta empresa, para recibir información de pagos y demás generada durante el giro normal de la relación comercial con la empresa. Se encuentra alojada en los computadores del departamento de contabilidad y en el servidor propio de la empresa, alojada en el sistema SIIGO.

Estas bases son actualizadas en el momento en que el cliente informa cambios en sus datos. La modificación, supresión o inclusión de datos en estas bases se encuentra a cargo de la jefe y asistente del Dpto de Contabilidad.
La información que se obtuvo anteriormente sin el previo consentimiento del cliente, no son utilizadas para el envió de información promocional, de eventos, entre otros; estas son conservadas en el sistema únicamente para procesos de facturación y fiscales.
Del sistema Siigo, el área de contabilidad realiza backups de manera semanal en una carpeta compartida alojada en el servidor de dominio.

14.3 BASES DE DATOS FÍSICAS

Las bases de datos contenidas en libros, carpetas, tarjeteros, y agendas, que son administrados por el personal para los fines del objeto social de la empresa, se encuentran almacenadas en archivadores bajo llaves asignadas y custodiadas por cada funcionario, cuyo acceso y uso son exclusivos de cada empleado.

- ## 14.4 INVENTARIO DE EQUIPOS

El Inventario de equipos de cómputo es actualizado cada año donde relacionamos la información de Hardware y Licenciamiento que permita construir una línea base para determinar el estado actual de los equipos, responsable, averías y dependencias o área al que pertenecen dichos equipos de cómputo.

15. FUGAS DE DATOS Y BRECHAS DE SEGURIDAD

El análisis de las brechas de seguridad tiene un componente tecnológico enfocado a los controles y medidas de seguridad y otro en que es necesario la valoración de los riesgos para los derechos y libertades de las personas.

15.1 FUGAS DE DATOS

Son situaciones en las que los usuarios perciben ganar en funcionalidad, y no piensan en los riesgos que su conducta, puede estar introduciendo en la empresa, el correo electrónico es el método más utilizado por los ciberdelincuentes para tratar de vulnerar la empresa. A través del phishing y la ingeniería social se cuelan cada día en la oficina esperando que caigamos en la trampa.

Los delincuentes han ingeniado la mejor manera de que estos correos se parezcan lo más posible a los que forman parte del día a día de tu organización (archivos adjuntos que simulan facturas, mensajes suplantando la identidad de mandos superiores, comunicaciones bancarias etc.); Esto unido a la necesidad de gestionar las cosas cuanto antes, tiene como consecuencia que en ocasiones no nos fijemos en los pequeños detalles que alertan de que ese correo no es el que

realmente esperábamos recibir y así, desencadenar en que nos convirtamos en víctimas de estos engaños.

Las normas de protección de la propiedad intelectual obligan a **FUNDACIÓN SOLIDARIDAD POR COLOMBIA** a usar en todo momento software legal. El uso de software pirata o adquirido de forma fraudulenta podría conllevar sanciones económicas y penales. Además, la instalación y uso de software ilegal en algún dispositivo incrementa los riesgos de infección por malware.

Por otra parte, para evitar **fugas de información** y garantizar la privacidad de los datos de carácter personal, **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** controla qué software está autorizado para el tratamiento de la información dentro de la empresa.

Cualquier incidente de seguridad puede repercutir en la imagen de la compañía.

Para hacer cumplir esta política **FUNDACIÓN SOLIDARIDAD POR COLOMBIA.** cuenta con:

- un listado de software autorizado.
- un repositorio del software autorizado y un registro de licencias.

Donde se identifica a los responsables de cada equipo para realizar las actualizaciones del software y las auditorías.

15.2 OBJETIVOS.

Controlar que siempre se usa software autorizado en **FUNDACIÓN SOLIDARIDAD POR COLOMBIA**, y que ha sido adquirido de forma legal.

15.3 CHECKLIST.

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a aplicaciones permitidas.

Los controles se clasifican en dos niveles de complejidad.

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales como el Antivirus.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos, Backups, Antivirus, y Malware Byte.

Los controles tendrán el siguiente alcance:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

Ver check-list a continuación

15.4 PUNTOS CLAVE

Los puntos clave de esta política son:

Registro de licencias. El software que dispone **FUNDACIÓN SOLIDARIDAD POR COLOMBIA** es legal con factura de compra y hay un registro actualizado de licencias.
Ver anexo Archivo hoja de inventario en excel de los equipos y licencias de la **FUNDACION SOLIDARIDAD POR COLOMBIA Ver: Carpeta: 1.Autorizaciones Inventarios y Registros Generales**

Técnicas para la instalación, actualización y borrado. Para asegurarnos una configuración óptima en los equipos de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA** es aconsejable que únicamente el ingeniero encargado pueda instalar, actualizar y eliminar software.

15.5 BRECHAS DE SEGURIDAD.

Cualquier anomalía, incidencia de seguridad o fuga de datos de carácter personal que afecte el cumplimiento de la normativa desarrollada en el Manual de políticas y procedimientos o que pueda afectar a los Datos de Carácter Personal que trata la Empresa será notificada de inmediato al Delegado de Protección de Datos DPO, y se pasaría como una incidencia.

Todos los **INFORMES DE INCIDENCIAS** se registran en el **REGISTRO DE INCIDENCIAS DE SEGURIDAD,** en las siguientes tablas.

En el caso de una violación de datos personales que probablemente resulte en un riesgo grave para los derechos y libertades de las personas, el Administrador de zona notificará sin demora a las autoridades y al interesado / empresa a más tardar 36 horas después de haber tenido conocimiento de ello.

Reportar una violación de datos personales

1. Cuando la notificación a la autoridad de control no se pueda realizar dentro de las 36 horas siguientes, deberá ir acompañada de los motivos del retraso.
2. El Administrador de zona deberá notificar a la Compañía sin demora después de conocer una violación de datos personales.
3. La notificación incluirá:

- Descripción de la naturaleza de la violación de los datos personales y cuando sea posible, las categorías y el número aproximado de interesados, y las categorías y el número aproximado de registros de datos personales correspondientes;
- Comunicar el nombre y los detalles de contacto del caso reportado para obtener más información;
- Describir las medidas adoptadas o propuestas que debe tomar el controlador para abordar la violación de los datos personales, incluidas, cuando corresponda, medidas para mitigar sus posibles efectos adversos.

12. CHECK LIST Y ANEXOS

MEDIDAS DE SEGURIDAD BÁSICAS	SI	NO
Utiliza Cámaras de Video-vigilancia		X
Graban imágenes		X
Tiene máquina de destrucción de documentos		X
Procedimiento de asignación/control de contraseñas?	X	
Biométricos		X
Periodicidad del cambio de contraseñas		
Semanal, si a los más sensibles, Base de datos.	X	
Mensual, si según consentimiento del jefe de área y usuario del equipo.	X	
Semestral		
Anual		
Composición del Sistema		
Tiene un Servidor interno propio?	X	
Ubicado en una sala de acceso restringido?	X	
¿Tiene un Servidor externo propio?		X
¿Tiene un servidor alojado en otro país?		X
¿Tiene un Servidor externo a cargo de un tercero?		X
Copias de Seguridad - Back ups		
¿Realiza copias de Seguridad?	X	
¿Existe un procedimiento para realizar las copias de seguridad?	X	
Tiene un encargado de realizar las Copias de Seguridad	X	
Periodicidad		
Cada cuánto realiza copias de Seguridad:		
Diario a Bases de datos sensibles y documentos de los usuarios del dominio	X	
Semanal a datos sensibles de los usuarios	X	
semestral		X
anual	X	
Control de Accesos y Contenidos		
Controla los contenidos a los que pueden acceder las diferentes áreas o personas ?	X	
¿Cuenta con una política y procedimientos de control de accesos y contenidos?	X	
Soporte en el que se hacen las Copias de Seguridad:		
servidor propio	X	
servidor externo		X
computador		X
cloud	X	
dispositivo móvil		X
disco duro externo		X
Otros, interno NAS	X	
Incidencias de Seguridad		
¿Tiene implementado un sistema de reportes de incidencias de seguridad?	X	
¿Tiene procedimientos implementados para atender incidentes de seguridad?	X	
¿Tiene medidas para investigar, corregir, mitigar y prevenir futuras violaciones a la privacidad?	X	

ANEXO 1 Reporte de Incidentes de Seguridad de la información

		SISTEMA INTEGRADO DE GESTIÓN	Código:	
	PROCESO	GESTIÓN DE LA INFORMACIÓN Y COMUNICACIONES	Versión:	
	FORMATO	REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	Fecha:	___/___/__

REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
FECHA Y HORA REPORTE DE INCIDENTE	
LUGAR DEL INCIDENTE	
CONSECUTIVO ASIGNADO A INCIDENTE	

DETALLES DE PERSONA QUE REPORTA/IDENTIFICA INCIDENTE:	
Nombre Completo:	
Documento :	

DESCRIPCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:
Qué Sucedió?:
Cómo Sucedió?:
Por qué Sucedió?:
Consideraciones Iniciales sobre componente(s) / Activo(s) de información afectados?:
¿Impactos adversos para la Entidad?: SI NO Cual?
¿Se identifica Vulnerabilidad alguna?: SI NO Cual?
¿Se identifica responsable del Incidente?: SI NO Cual?

ESTADO DEL INCIDENTE		
Sucediendo :	Sucedió :	Sucede Nuevamente :

DETALLE DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:	
Fecha y Hora en la que sucedió el incidente?:	
Fecha y Hora en la que se descubrió el incidente?:	
Fecha y Hora en la que se reportó el incidente?:	

La respuesta a este incidente ya ha finalizado?:	SI	NO

En caso afirmativo, especifique cuánto tiempo duró el incidente (Días / Horas / Minutos)?: Una hora Aprox.

ANEXO 2. AUTORIZACIONES PARA LA ENTREGA ARCHIVOS DIGITALES, FÍSICOS O CONEXIONES REMOTAS PARA EL TELETRABAJO

Empleado autorizado para la entrega de archivos digitales o físicos que contienen datos personales o conexiones para el manejo de teletrabajo a un usuario / empleado de la empresa.

DESCRIPCIÓN (si es Activo de Fundación Solidaridad Por Colombia)
.....

EMPLEADO …….....

CC……

DETALLE DEL TRABAJO:

……..……

……..…

……..…
AUTORIZADA POR:

.....……..……..

FIRMA:
…….....FECHA:……..

FIRMA DEL EMPLEADO: …….....FECHA:……..……..

EJECUTADO: .....

INGENIERO DE SOPORTE:……

FIRMA: …….....FECHA:……..…..……..

EL EMPLEADO SE COMPROMETE A MANEJAR LA INFORMACIÓN CONTENIDA EN ESTOS DOCUMENTOS DE ACUERDO A LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES Y AL CONTRATO DE PRESTACIÓN DE SERVICIOS

ANEXO 4 FORMATO USUARIO RESPONSABLE CARPETA CONTENEDORA

	FORMATO DE USUARIO RESPONSABLE DE CARPETA CONTENEDORA	**Código:** SGI-SI-FO04 **Versión:** 00 **Vigencia:** 21/03/2022 **Página 1 de 1**

Empleado autorizado para la entrega de archivos digitales o físicos que contienen datos personales o conexiones para el manejo de teletrabajo a un usuario / empleado de la empresa.

DESCRIPCIÓN (si es Activo de Fundación Solidaridad Por Colombia) .....

EMPLEADO …….....

CC……

DETALLE DEL TRABAJO:

……

……

……

AUTORIZADA POR:

.....……..……..

FIRMA:
…….....FECHA:……..

FIRMA DEL EMPLEADO: …….....FECHA:……..……..

EJECUTADO: .....

INGENIERO DE SOPORTE:……

FIRMA: …….....FECHA:……...…..……..

EL EMPLEADO SE COMPROMETE A MANEJAR LA INFORMACIÓN CONTENIDA EN ESTOS DOCUMENTOS DE ACUERDO A LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES Y AL CONTRATO DE PRESTACIÓN DE SERVICIOS

ANEXO 5 FORMATO CAMBIO Y ASIGNACIÓN DE CLAVES DE CORREO ELECTRÓNICO

GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN Y DATOS

MEDIDAS DE SEGURIDAD INTERNAS

- Tenido en cuenta la naturaleza, el alcance, el contexto y la finalidad de los datos personales tratados por **Fundación Solidaridad Por Colombia**

y después de haber evaluado el riesgo a los derechos y libertades de los individuos que este tratamiento pueda causar, la empresa ha adoptado las siguientes medidas de seguridad:

Contraseñas

- Cada Usuario tiene un "login" o Identificador que se autentifica mediante una contraseña.
- Las Contraseñas son de Uso Personal y No puede hacerse un Uso Compartido de las mismas.
- Nuestros Sistemas o Aplicaciones que requieran la Autenticación del Usuario, establecen una limitación del número de intentos fallidos para accesos de usuarios no autorizados.

Condiciones establecidas para las Contraseñas:

- Se deben evitar los nombres comunes y cualquier combinación del usuario en el que intervenga su fecha de nacimiento, matrícula del coche, etc.
- La Contraseña contendrá un mínimo de ocho caracteres Alfanuméricos y que contengan letras mayúsculas y minúsculas.
- Deberá cambiarse como mínimo UNA VEZ AL AÑO.

Usuarios

- No permitir y no facilitar información y/o documentación perteneciente a **Fundación Solidaridad Por Colombia**
-
- No utilizar los recursos informáticos (hardware, software o datos) para otras actividades que no estén directamente relacionadas con el trabajo en **Fundación Solidaridad Por Colombia**
-
-
- El personal que tenga un equipo informático a su cargo tiene la responsabilidad de reportar inmediatamente al departamento de sistemas o a su jefe inmediato, en el caso de los empleados de los puntos de venta, cualquier evento que pueda comprometer los sistemas de información de la compañía y sus recursos informáticos, como por ejemplo virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.
- Reportar inmediatamente al departamento de sistemas cualquier falla que se pueda presentar en el computador o en la red, ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- Todo software utilizado por **Fundación Solidaridad Por Colombia**
-
- Está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usarse para fines personales.
- Los usuarios que tienen habilitados medios extraíbles en sus equipos de cómputo como (CD/DVD, memorias USB, etc.), conexiones a redes externas o que poseen privilegios, **NO** deben extraer datos de **Fundación Solidaridad Por Colombia**
-
- sin la aprobación previa de la Gerencia Financiera y Administrativa.
- Se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente autorizado por la Gerencia.
- En caso que un equipo deba ser reparado por parte del departamento de sistemas, es función del usuario tener copias de respaldo como garantía de su información.
- La información almacenada en los equipos de **Fundación Solidaridad Por Colombia**
-
- Es responsabilidad de cada usuario asignado a este.
- Los usuarios tienen derecho a proteger su información crítica con contraseñas para evitar modificaciones o lecturas "no deseadas", sin embargo, esta acción debe ser de conocimiento por parte del líder de proceso y en su caso informar a la Gerencia Administrativa.
- En los equipos se almacena información exclusivamente referente a la empresa, se prohíbe el almacenamiento o custodia de información personal dentro de los equipos de cómputo, tales como imágenes, fotografías, archivos de música, archivos de video, documentos, ejecutables, etc.
- Se sugiere a los usuarios no configurar carpetas como "privadas" dentro del Sistema, esto para prevenir pérdidas de información en caso de colapsos del Sistema Operativo porque están excluidas de los backup.
- Toda la información generada en el desarrollo de la actividad laboral es estrictamente **CONFIDENCIAL** y solo puede ser compartida a terceros bajo la autorización expresa de la Gerencia o mandatos legales.
- La información generada en el desarrollo de la actividad laboral no pertenece a los Usuarios sino a **Fundación Solidaridad Por Colombia**
-

y/o al Titular de la misma, en concordancia con la Ley 1581 de 2012 y sus decretos reglamentarios.

EQUIPO DE COMPUTO ……. **FECHA ……..……**

NOMBRE Y FIRMA DEL USUARIO RESPONSABLE DEL EQUIPO……

ANEXO 6 FORMATO AUTORIZACIÓN SALIDA DE EQUIPOS DE COMPUTO

GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN Y DATOS

Autorización salida periódica dispositivo portátil propiedad de **FUNDACIÓN SOLIDARIDAD POR COLOMBIA**

SERIAL Y MARCA DEL EQUIPO PORTÁTIL: ……

NOMBRE DEL EMPLEADO:……

SALIDA DE SOPORTES

DESCRIPCIÓN

……

……

……

FRECUENCIA: Darío ____ Semanal ____ Fin de Semana ____ Mensual ____

Otros (Explique)……

AUTORIZADO DESDE:……

HASTA: ……

AUTORIZADO POR: ……

FIRMA RESPONSABLE DE SEGURIDAD ……

FECHA ……

NOTA: El empleado es responsable de devolver los ficheros que contienen datos personales descritos en esta autorización, en el estado en perfectas condiciones, sin dejar copias o derivaciones de los datos personales fuera de las instalaciones de la empresa.

Dispositivos de la compañía - El empleado volverá todos los dispositivos portátiles de la empresa con todos sus archivos de datos personales en la terminación de su contrato de trabajo o al final del periodo de autorización, sin alterarlos.

Dispositivos propiedad de los empleados - El empleado permitirá a la compañía revisar los dispositivos para asegurar que todos los datos personales que pertenecen a la Compañía se han borrado del dispositivo (s) a la resolución del contrato o al final del período de autorización

FIRMA DEL EMPLEADO: ……

FECHA:……

ANEXO 7 CONTROL CAMBIO DE CLAVES

CONTROL DE CAMBIOS DE CLAVES					
NOMBRE DE EQUIPO	**CLAVE DE INGRESO**	**FECHA CAMBIO**	**RESPONSABLE**	**FECHA CAMBIO**	**CLAVE NUEVA**

ANEXO 9 FORMATO DE CONTROL DE CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD

MEDIDAS DE SEGURIDAD BÁSICAS	SI	NO
Utiliza Cámaras de Video-vigilancia		
Graban imágenes		
Tiene máquina de destrucción de documentos		
Procedimiento de asignación/control de contraseñas?		
Biométricos		
Periodicidad del cambio de contraseñas		
Semanal, si a los más sensibles, Base de datos.		
Mensual, si según consentimiento del jefe de área y usuario del equipo.		
Semestral		
Anual		
Composición del Sistema		
Tiene un Servidor interno propio?		
Ubicado en una sala de acceso restringido?		
¿Tiene un Servidor externo propio?		
¿Tiene un servidor alojado en otro país?		
¿Tiene un Servidor externo a cargo de un tercero?		
Copias de Seguridad - Back ups		
¿Realiza copias de Seguridad?		
¿Existe un procedimiento para realizar las copias de seguridad?		
Tiene un encargado de realizar las copias de seguridad ?		
Periodicidad		
Cada cuánto realiza copias de Seguridad:		
Diario a Bases de datos sensibles y documentos de los usuarios del dominio		
Semanal a datos sensibles de los usuarios		
semestral		
anual		
Control de Accesos y Contenidos		
Controla los contenidos a los que pueden acceder las diferentes áreas o personas. SI POR MEDIO DE UN DOMINIO QUE ESTÁ CONFIGURADO EN EL SERVIDOR		
¿Cuenta con una política y procedimientos de control de accesos y contenidos?		
Soporte en el que se hacen las Copias de Seguridad:		
servidor propio		
servidor externo		
computador		
cloud		
dispositivo móvil		
disco duro externo		
Otros, interno NAS		
Incidencias de Seguridad		
¿Tiene implementado un sistema de reportes de incidencias de seguridad?		
¿Tiene procedimientos implementados para atender incidentes de seguridad?		
¿Tiene medidas para investigar, corregir, mitigar y prevenir futuras violaciones a la privacidad?		