

PLATAFORMA TECNOLÓGICA HABILITANTE
PROPONENTE CONSORCIO AUDISALUD FONECA 2024
FONECA
Enero 5 de 2024

Contenido

I. OFRECIMIENTO PLATAFORMA TECNOLÓGICA	3
II. PLATAFORMA TECNOLÓGICA	3
III. FUNCIONALIDADES DEL SOFTWARE	4
IV. ASPECTOS TÉCNICOS DEL SOFTWARE	5
V. LICENCIAMIENTO SOFTWARE	6
VI. CONFIDENCIALIDAD DE LA INFORMACIÓN	6
VII. DE LA INFRAESTRUCTURA	7
VIII. NORMAS DE REDES Y SEGURIDAD	10
IX. CORREO ELECTRÓNICO	14
X. OTRAS DISPOSICIONES	15
XI. SEGURIDAD LÓGICA	16
XII. MANTENIMIENTO DE EQUIPOS DE TECNOLOGÍA	21
XIII. MANTENIMIENTO PREVENTIVO	22
XIV. MANTENIMIENTO CORRECTIVO	23
XV. ACTIVIDADES ADICIONALES	24
XVI. POLITICAS DE SOFTWARE Y APLICACIONES	24
XVII. MEDIDAS DISCIPLINARIAS	33

I. OFRECIMIENTO PLATAFORMA TECNOLÓGICA TECNOLÓGICA

3

El suscrito representante legal del CONSORCIO AUDISALUD FONECA 2024, ofrece para la ejecución del contrato que eventualmente se derive de la presente invitación, el software Care Soft Auditoría, propiedad de uno de los integrantes de la figura plural.

II. PLATAFORMA TECNOLÓGICA

Care Soft es una Plataforma Tecnológica basada en un desarrollo de software denominado Care Soft Auditoría, diseñado para procesos de auditoría integral, administrativa, técnica y financiera, tanto retrospectiva como concurrente de entidades relacionadas con el sector salud, seguros, régimen de excepción y seguridad social, así mismo genera los informes respectivos par cada actor de los procesos establecidos en el sistema.

Care Solutions Colombia SAS es el propietario de los derechos de Autor y de los Derechos Patrimoniales del Software Care Soft Auditoría, el cual fue un desarrollo por encargo ejecutado por una firma externa.

El software cuenta con su debido registro lógico ante la OFICINA DE REGISTRO de la UNIDAD ADMINISTRATIVA ESPECIAL de la DIRECCION NACIONAL DE DERECHO DE AUTOR del MINISTERIO DEL INTERIOR

El Care Solutions Colombia SAS pone a disposición del servicio un software que permite el cargue, validación y procesamiento de datos de todos los informes relacionados con la Prestación de Servicios de Salud de conformidad con la

información remitida por los contratistas y definida en la matriz de informes obligatorios de la EAPB.

Adicional a lo anterior, la herramienta tecnológica permite el seguimiento al cumplimiento de los planes de mejoramiento y de los indicadores relacionados con los mismos.

4

III. FUNCIONALIDADES DEL SOFTWARE:

El Care Solutions Colombia SAS cuenta con una plataforma para el desarrollo del proyecto que contiene, entre otras funcionalidades, los siguientes módulos.

- A. ASEGURAMIENTO
- B. CONTRATACIÓN
- C. AFILIACIONES
- D. VALIDADOR DE RIPS
- E. AUDITORIA DE CUENTAS MEDICAS
- F. AUDITORÍA MEDICA CONCURRENTE
- G. AUDITORIA DE LA CALIDAD
- H. PQRS – SIAU
- I. REFERENCIA Y CONTRAREFERENCIA
- J. PROMOCION DE LA SALUD Y PREVENCION DE LA ENFERMEDAD
- K. MÓDULO DE REPORTES (BI) PARA CÁLCULO DE INDICADORES DE OBLIGATORIO CUMPLIMIENTO Y OTROS INDICADORES

El software cuenta con un tablero de indicadores que permite la visualización de indicadores trazadores con el fin de tener información para la toma de decisiones, e indicadores que permiten la medición de la calidad y efectividad de la ejecución del contrato, desde todos los ámbitos de la interventoría.

El aplicativo cuenta con la capacidad para calcular los indicadores relacionados en el listado maestro de indicadores, así como los demás indicadores que priorice el Fondo o que sean adicionados por la normatividad vigente o requeridos por la entidad en cualquier momento de la ejecución del contrato.

Esta Plataforma permitirá a la interventoría calcular los indicadores de acuerdo con los tiempos indicados en la matriz de informes obligatorios de la EAPB y reportar los mismos de forma mensual a la entidad, para el estudio y seguimiento de la calidad y mejoramiento del servicio.

5

Estos informes incluyen:

1. Cuadro y gráficos comparativos que presentan el resultado del indicador conforme a la meta establecida.
2. Análisis de los principales indicadores que presentan desviación en su cumplimiento.
3. Indicadores que permiten evidenciar el avance en el cumplimiento de los planes de mejoramiento.

IV. ASPECTOS TÉCNICOS DEL SOFTWARE

ARQUITECTURA: El Care Solutions Colombia SAS pone a disposición un software que incluye un módulo para el manejo específico del sector de RIPS.

MÓDULOS PERSONALIZABLES Y ESCALABLES: La Plataforma cuenta con módulos personalizables y escalables: La plataforma está desarrollada con una arquitectura y estructura personalizable, parametrizable y escalable, que cumple con los requerimientos de la resolución 3374 de 2000 y las normas que la reglamenten, modifiquen o sustituyan.

BASES DE DATOS: La plataforma cuenta con un motor de Bases de datos de código abierto, robusta y con control de recuperación de la data, plan de copias de seguridad y plan de recuperación de la información.

SEGURIDAD INFORMÁTICA: Contamos con una Política y Plan de Seguridad Informática y Contingencia de la Información que garantizan un plan de seguridad, contingencia, respaldo y disponibilidad de la información.

ACCESIBILIDAD DE LA INFORMACIÓN: El sistema de información permite exportar la información de los reportes solicitados a Excel, archivo plano y formato xml, para de esta manera garantizar la integración con otros sistemas y entrega de información a las entidades que lo soliciten.

La plataforma funciona en un ambiente web y permite su utilización remota.

V. LICENCIAMIENTO SOFTWARE:

Licenciamiento vigente de la plataforma: La plataforma, por ser un desarrollo de Care Solutions Colombia SAS no requiere licenciamiento pues es el titular de los derechos patrimoniales debidamente registrados.

VI. CONFIDENCIALIDAD DE LA INFORMACIÓN

Las personas pertenecientes a la compañía reconocen que toda la información a la que se pueda tener acceso en el marco del Contrato ya sea relacionada con el objeto de sus procesos o relacionada con la actividad u organización, tiene carácter confidencial, dado entonces que esta forma, no se permite divulgarla y mantener la más estricta confidencialidad respecto de dicha Información,

advirtiéndolo, en su caso, de dicho deber de confidencialidad y secreto a sus empleados, asociados y a cualquier persona que, por su cargo o relación personal o sentimental deba o pueda tener acceso a la misma.

Nadie podrá reproducir, modificar, hacer pública o divulgar a terceros la Información sin previa autorización escrita y expresa del representante de la compañía.

Las personas se comprometen a poner los medios necesarios para que la Información no sea divulgada ni cedida. Adoptarán las mismas medidas de seguridad que adoptarían respecto a la información confidencial de su propiedad, evitando su pérdida, robo o sustracción.

El receptor de la Información se compromete, en su caso, a advertir sobre la existencia del deber de confidencialidad a sus subalternos, asociados, y a toda persona a la cual se le facilite la Información, haciéndose responsable del uso indebido que estos puedan hacer de la Información relacionada.

Asimismo, todo empleado o vinculado a la compañía que recibe Información se compromete a poner en conocimiento cualquier acción o incidente por parte de terceros que pueda atentar contra la confidencialidad de la Información.

VII. DE LA INFRAESTRUCTURA

El departamento de Sistemas de CARE SOLUTIONS COLOMBIA SAS procura el óptimo funcionamiento de los sistemas de información y telecomunicaciones. Ofrece apoyo técnico y administrativo en los sistemas computarizados a todas aquellas divisiones y dependencias que componen la Empresa con el fin de solucionar cualquier problema que surja con los equipos o redes de datos. Dicho departamento participará en todas las actividades de nueva tecnología adquirida por la Empresa.

El departamento de sistemas abarca la infraestructura de software, hardware, equipos de comunicaciones, redes, servicios electrónicos internos, acceso Internet e Intranet.

El uso de las Estaciones de Trabajo de CARE SOLUTIONS COLOMBIA SAS es exclusivo para los empleados de la Empresa, quienes acatarán las siguientes normas:

1. Los computadores, los servicios asociados tanto internos como externos, el sistema de correo electrónico (e-mail), la Intranet y los documentos y programas que existan en la misma son propiedad única y exclusiva de CARE SOLUTIONS COLOMBIA SAS y sólo podrán ser utilizados para propósitos lícitos, prudentes, responsables y dentro de las funciones inherentes a la empresa.
2. Toda información, dato, obra literaria o de arte, escrito, documento, programas, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de los computadores será propiedad de la empresa, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario.
3. La información contenida en el computador, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (e-mail), información de la Intranet o la Internet y los documentos y programas existentes no podrán ser reproducidos o utilizados para fines ajenos a las funciones y poderes de la Empresa. Cualquier información podrá ser examinada o utilizada por el gerente o su personal autorizado.
4. Se prohíbe la Instalación, Reproducción o uso de programas o recursos para los cuales no exista una licencia o autorización de uso válido a nombre de CARE SOLUTIONS COLOMBIA SAS.

5. Se prohíbe copiar programas de computadora adquiridos por CARE SOLUTIONS COLOMBIA SAS y/o acceder o utilizar propiedad intelectual (“copyrighted information”) que viole derechos de autor.
6. Se prohíbe copiar programas de computadora adquiridos por CARE SOLUTIONS COLOMBIA SAS y/o acceder o utilizar propiedad intelectual (“copyrighted information”) que viole derechos de autor.
7. No se permite a ningún usuario el uso de los sistemas de cómputo y comunicaciones de la empresa para propósito personal, de recreo, para manejo de otra empresa o asunto privado del usuario o para el recibo o envío de mensajes en cadena, para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro asunto o servicio no oficial o ajeno a las funciones de la empresa. Dado lo anterior las Páginas Web (URL) serán restringidas al grupo de direcciones de uso normal de CARE SOLUTIONS COLOMBIA SAS; para el caso de requerir la autorización de Navegación a paginas adicionales, se debe diligenciar el TICKET a través de la Mesa de ayuda (Help-desk) debidamente justificado.
8. El departamento de sistemas podrá utilizar diferentes medios de programación para auditar y supervisar el uso de cada equipo de cómputo.
9. La Empresa se reserva el derecho a auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computarizados para garantizar que su propiedad sea utilizada sólo para propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente, al azar o cuando exista una investigación sobre una situación en particular. Al personal de la Empresa no le alberga expectativa de intimidad con relación a cualquier información, documento, mensaje creado, recibido o enviado a través del sistema de correo electrónico (E-mail) de carácter personal.

10. Se prohíbe el uso de computadoras portátiles o cualquier otro equipo electrónico para realizar trabajos en la Empresa si dichos equipos son personales.
11. Cualquier adquisición, traslado o asignación de equipos, así como de sus periféricos deberá ser coordinado con el personal de Sistemas.
12. El proceso de El departamento de sistemas debe tener bajo su custodia y reserva tres (2) Equipos de cómputo y una (1) impresora de última tecnología, con el fin de garantizar el funcionamiento de la infraestructura tecnológica por daño o mal funcionamiento de cualquiera de los equipos con que cuenta la Corporación. Para la reposición de estos equipos tendrán prioridad los procesos que presten servicios de cara al cliente. Cada vez que CARE SOLUTIONS COLOMBIA SAS adquiera nuevos equipos de cómputo, serán rotados los equipos de reserva por los nuevos de última tecnología.
13. Con el fin de lograr la mayor uniformidad, antes de la adquisición de computadores, redes, servicios electrónicos internos y programas deberá contarse con el asesoramiento de la Oficina de Sistemas.
14. Cada usuario es responsable de tomar las medidas necesarias para proteger el equipo bajo su uso.
15. El Proceso de El departamento de sistemas velará por el licenciamiento de los productos y registro de las licencias.

VIII. NORMAS DE REDES Y SEGURIDAD

1. Cada Usuario de la Red de datos posee un Nombre de usuario ("Login") el cual consistirá en una estructura compuesta por su nombre seguido de un punto (.) y su apellido. Ej. El usuario Pedro Pérez poseerá el login pedro.perez en minúscula. Así mismo cada usuario posee un perfil de seguridad, el cual determina sus niveles de acceso y permisos en la Red de

datos. Este perfil lo asigna el departamento de sistemas(T.I.) al ser contratado un nuevo miembro de la Corporación; el departamento de recursos humanos deberá informar a sistemas con el fin de generar el login y el Perfil para el nuevo usuario.

2. El uso de un código de acceso de autenticación al dominio (“password”) no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en el computador asignado o en cualquier otro. Las contraseñas deben mantenerse en estricta confidencialidad ya que son personales e intransferibles y ser cambiadas cada noventa (90) días. La misma será de por lo menos ocho (8) caracteres de longitud, deberá ser una combinación de caracteres alfanuméricos (letras, números, símbolos) en cualquier proporción o arreglo y el primer carácter en mayúscula. La contraseña utilizada por el usuario no podrá repetirse cuando expire la validez en el sistema. Al momento de intentar ingresar al sistema, el usuario tendrá la oportunidad de equivocarse 5 veces; en el sexto intento la cuenta será bloqueada por espacio de 10 minutos; al cabo de este tiempo el usuario podrá intentar ingresar nuevamente. Cada Usuario debe ingresar con su Nombre de Usuario y Password a las estaciones; en caso de que el usuario se levante de su puesto, deberá bloquear su estación por medio de la combinación de teclas Ctrl + Alt + Suprimir y luego Enter. Para el caso de que se requiera el préstamo de la estación, el nuevo usuario deberá ingresar con su propio Nombre de usuario y password.
3. Ningún usuario diferente al personal del departamento de sistemas está autorizado para modificar los privilegios de acceso a las redes internas o externas.
4. información confidencial para fines no autorizados por CARE SOLUTIONS COLOMBIA SAS .

5. Ningún empleado está autorizado para el envío o recibo de mensajes de correo electrónico entre el personal de la Empresa y personas ajenas a la misma en los cuales se divulguen, comenten o expresen hechos, opiniones u otra situación o asuntos internos de CARE SOLUTIONS COLOMBIA SAS , que puedan poner en entredicho la reputación y la imagen de la Empresa.
6. La descarga de Software (*.exe, *.com, *.bat, *.mp3, *.mp4, *.aac, *.ogg, *.mpg, *.avi), y cualquier otro tipo de software ejecutable, de audio, de video queda restringida; para el caso que se requiera la descarga de alguno de estos tipos de archivo, se debe diligenciar el TICKET a través de la Mesa de ayuda (help desk) dirigido a el departamento de sistemas debidamente justificado. De la misma forma se prohíbe la instalación o uso de programas de descarga masiva o P2P tales como: Ares, Emule, eDonkey, LimeWire, Morpheus, Download Acelerator, Shareware, etc.
7. No se podrá modificar ni archivar la información propiedad de la Empresa con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos. Tampoco se podrá alterar el nombre del usuario u otra información que se utilice regularmente para identificar la información, mensajes o archivo. En caso de que algún usuario asigne contraseñas o codifique la información a fines de evitar que otras personas puedan leerla, este proveerá todos los datos para lograr acceso a los archivos al momento de su creación. La Empresa está facultada para decodificar la misma o restituirla a su condición original.
8. No se permite a ningún usuario modificar los parámetros y configuración adoptados por El departamento de sistemas en los computadores de la Corporación, en la capacidad de recibir llamadas telefónicas, conexión remota o cualquier otro tipo de acceso no autorizado en la red.
9. Todos los archivos de trabajo de carácter institucional que se creen o modifiquen en los computadores o estaciones de trabajo serán guardados por el usuario en "\\rutaServidor\Backup.X.XX; donde las X especifican la

dirección IP concedida por Sistemas; Es Responsabilidad de los usuarios el almacenar Única y Exclusivamente la información correspondiente a documentos de la Entidad (contenido institucional) dentro del espacio asignado; todo contenido diferente a archivos de trabajo tales como archivos de Música, Videos, Fotografías diferentes a las Institucionales, etc., serán borrados de las estaciones por el usuario respectivo

10. Los usuarios solo apagaran los equipos al finalizar el día laboral ya que durante el día se activan los mecanismos de resguardo automático del servidor de Copias de Seguridad de los archivos de las estaciones de trabajo de los usuarios a los cuales se les resguarda. Es Responsabilidad de los usuarios acatar esta directriz en toda su extensión ya que la omisión de esta regla causará que no se ejecute el proceso automático de la copia de seguridad de los archivos del usuario y por lo tanto El departamento de sistemas no se hace responsable de la información actualizada del usuario.
11. El uso de dispositivos de almacenamiento (Memorias USB, CD-ROM, DVD, etc.) deberá limitarse a CARE SOLUTIONS COLOMBIA SAS ; en caso de que por razones institucionales se requiera utilizar los dispositivos fuera del dominio de CARE SOLUTIONS COLOMBIA SAS al regresar estos dispositivos será responsabilidad del usuario realizar la respectiva vacunación con el antivirus instalado en el PC.
12. Ningún usuario está autorizado para realizar tareas de instalación de equipo, programas (software) ni de reparación. Solamente el personal autorizado por El departamento de sistemas podrá instalar y configurar los equipos de computadoras.
13. Cuando el usuario detecte problemas en el funcionamiento del sistema deberá notificarlo diligenciando el TICKET a través de la Mesa de Ayuda para el establecimiento de la prioridad e inclusión de actividades del personal técnico de tecnología.

14. Ningún usuario llevará alimentos ni bebidas a las estaciones de trabajo donde los equipos de computadoras estén localizados.
15. Se restringe el acceso al área física del departamento de sistemas al personal de otros procesos y personal externo no autorizado, teniendo en cuenta que el departamento de sistemas maneja uno de los activos más importantes para CARE SOLUTIONS COLOMBIA SAS como es la información.
16. Se prohíbe el acceso a personal ajeno a Tecnología o personal externo al DATACENTER. Solamente el personal externo o grupo de asesores autorizado por El departamento de sistemas podrá ingresar con el acompañamiento del personal de Tecnología para la ejecución de tareas específicas de la administración de la infraestructura tecnológica.

IX. CORREO ELECTRÓNICO

1. Ningún empleado está autorizado para reclamar interés propietario o expectativa razonable de intimidad sobre comunicaciones como Internet o correo electrónico. La Empresa tendrá acceso a los mensajes electrónicos e información de los espacios virtuales (Web) visitados por empleados en cualquier momento y los mismos serán considerados parte de los expedientes de la Oficina.
2. Ningún usuario está autorizado para bajar información (download) de los servicios de Internet sin la debida autorización de la administración.
3. No se permite utilizar el sistema para acceder y almacenar información en cuentas de correo electrónico distintas a las cuentas provistas por la empresa, para el caso de requerir la autorización se debe diligenciar un requerimiento en el TICKET a través de la Mesa de ayuda (help desk) debidamente justificado.

4. No se permite el envío de copias de mensajes de correspondencia electrónica con información confidencial sin el consentimiento del remitente original.
5. No se permite a los usuarios el suscribirse a listas de correo electrónico o que participen en grupos de noticias (“newsgroups”) que divulguen información o mensajes ajenos a las funciones y deberes de la Empresa sin la debida autorización.
6. No se permite la reproducción maliciosa o voluntaria de virus, envío de correo que no sea oficial, envío de material ofensivo, ilegal o pornográfico o de cualquier otra índole no autorizada.
7. Cada usuario será responsable de sus actos y conducta al acceder a Internet o al utilizar el correo electrónico.

X. OTRAS DISPOSICIONES

1. El manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadores o del sistema de comunicación electrónica de la Empresa, no está permitido. Esto incluye, a modo de ejemplo, acceso a material erótico, bromas de cualquier forma o cualquier comentario o chiste que pueda violar excepto los autorizados por la gerencia o el representante autorizado de Sistemas.
2. La política adoptada para el uso de Internet será revisada periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la Empresa. Estas se incorporarán y se hará formar parte de estas guías todos aquellos documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de tiempo en tiempo y que estén relacionadas al uso de los computadores de la Empresa.

3. Cada empleado de la Empresa es responsable de conocer dichas órdenes administrativas sobre el uso y manejo del sistema de informática.
4. Todo empleado será responsable de informar por escrito al Gerente o encargado de la Oficina de Informática sobre cualquier situación de seguridad, incidente, acceso indebido o violación voluntaria o involuntaria de estas normas para el uso de los computadores o redes de la Empresa.

XI. SEGURIDAD LÓGICA:

1. Administración de Usuarios y contraseñas
2. Longitud mínima de la clave: La longitud de la clave debe ser mínima de ocho (8) caracteres y debe controlarse en el momento en que el usuario la construye o la selecciona.
3. Palabras claves difíciles de adivinar: Todas las palabras claves escogidas por el usuario para ingresar a los sistemas deben ser difíciles de adivinar. En general, no se deben utilizar palabras de un diccionario, derivados del usuario-ID, series de caracteres comunes tales como “123456”. Así mismo, no se deben emplear detalles personales como nombre del esposo, placas del carro, número del seguro y fecha de cumpleaños a menos que estén acompañadas por caracteres adicionales que no tengan ninguna relación. Las palabras claves escogidas por el usuario tampoco deben formar parte de una palabra. Por ejemplo, no se deben emplear nombres propios, sitios geográficos, acrónimos y jerga comunes.
4. Prohibición de utilizar palabras claves cíclicas: Los usuarios no deben construir palabras claves compuestas por caracteres que no cambian o combinadas con cierto número de caracteres que cambian predeciblemente. Es decir, que no se deben utilizar caracteres que

típicamente cambian tal como el mes, un departamento, un proyecto o algún otro factor que fácilmente puede adivinarse (por

5. Uso de palabras clave repetidas: Los usuarios no deben construir palabras clave que sean idénticas o muy similares a palabras clave utilizadas previamente.
6. Palabras clave con caracteres alfabéticos y no alfabéticos: Todas las palabras claves deben tener al menos un carácter alfabético y uno no alfabético; se consideran caracteres no alfabéticos los números y los signos de puntuación, no se deben utilizar caracteres de control y otros caracteres no impresos porque involuntariamente pueden causar problemas de transmisión en la red o sin intención llamar ciertos servicios del sistema.
7. Palabras claves con letras mayúsculas y minúsculas: Todas las palabras claves escogidas por el usuario deben tener al menos un carácter alfabético en minúscula y otro en mayúscula. Esto ayudará para que las palabras claves sean más difíciles de adivinar por personas no autorizadas o por espías industriales.
8. Visualización de palabras clave: Las palabras clave en pantalla o impresas no se deben presentar, esto con el fin de evitar que personas no autorizadas las puedan observar o recuperarlas.
9. Cambios periódico obligatorio de palabras claves: El sistema debe obligar automáticamente a que todos los usuarios cambien sus palabras claves al menos una vez cada noventa (90) días.
10. Cambio obligatorio de palabras clave al acceder por primera vez el sistema: Las palabras claves inicialmente emitidas por un administrador de seguridad deben ser válidas solamente para la primera conexión del usuario, momento en el cual el usuario debe cambiar la palabra clave antes de realizar cualquier otro trabajo.
11. Límite de intentos consecutivos infructuosos para ingresar la palabra clave: Después de cinco intentos consecutivos e infructuosos de ingreso de la

palabra clave, el sistema debe: (a) suspender el acceso del usuario hasta que el administrador del sistema lo ponga a funcionar de nuevo, (b) incapacitarlo temporalmente por no menos de tres minutos, o (c) si hay algunas otras conexiones o discado externos de la red desconectarlos.

12. Passwords ilegibles en estaciones de trabajo externas: Los passwords fijos nunca deben estar en forma legible fuera de la Entidad en estaciones de
13. Almacenamiento de palabras claves en forma legible: Las palabras claves no se deben almacenar en forma legible en archivos batch, manuscritos de login automáticos, software de macros, terminales, computadores sin controles de acceso o en otros sitios en donde personas no autorizadas puedan descubrirlas.
14. Incorporación de palabras claves dentro del software. Las palabras claves no se deben incorporar dentro de los programas de software, esto para que las claves se puedan cambiar en el momento que sea necesario.
15. Control de acceso al sistema con palabras individuales para cada usuario. El sistema de control de acceso al computador y al sistema de comunicación se debe realizar por medio de palabras claves únicas para cada usuario, es decir que no se admite el acceso a archivos, base de datos, computadores y otros recursos del sistema por medio de palabras claves compartidas.
16. Cambio de códigos claves proporcionados por el fabricante (palabras default). Todas las palabras claves de fábrica proporcionadas por el fabricante se deben cambiar antes que la entidad utilice cualquier sistema de computación o de comunicaciones para sus negocios.
17. Utilización de palabras claves diferentes cuando se tiene acceso a varios sistemas. Si un usuario tiene acceso a varios sistemas de información, se deben emplear palabras claves diferentes para cada uno de los sistemas a los cuales tiene acceso.
18. Permiso para usar la misma palabra clave en diferentes sistemas. Los usuarios deben abstenerse de utilizar el mismo código o palabra clave en

múltiples sistemas de computación de la entidad, a menos que el departamento de seguridad de información les haya informado por escrito que si lo hacen indebidamente comprometen la seguridad.

19. Cambio de clave cuando se sospecha que ha sido descubierta. Todas las palabras clave se deben cambiar tan pronto como se sospeche que han sido descubiertas o que podrían conocerlas personas no autorizadas
20. Escribir palabras claves (passwords) y dejarlas en donde otros pueden descubrirlas. No se deben escribir passwords y dejarlos en lugares donde personas no autorizadas pueden descubrirlos.
21. Escribir passwords usando técnicas secretas. Los usuarios no deben escribir sus passwords al menos que: (1) ellos hayan realmente ocultado estos relacionados, o (2) que ellos hayan usado un sistema de código para ocultar el password.
22. Prohibición de passwords compartido. No importa las circunstancias, los passwords nunca deben ser compartidos o revelados a nadie más que al usuario autorizado. Hacerlo expone al usuario autorizado a responsabilizarse de acciones que otras personas hagan con la palabra clave. Si los usuarios necesitan compartir información permanente del computador, ellos deben usar correo electrónico, o los mecanismos de carpeta compartida en los servidores de red del área local u otros mecanismos aceptados por la Gerencia.
23. Usuarios responsables de todas las actividades involucrando su código de identificación de usuario. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario. Los códigos de identificación de usuario no pueden ser utilizados por nadie más, sino por aquellos a quienes se les ha expedido. Los usuarios no deben permitir que otros realicen ninguna actividad con sus códigos de identificación de usuario. Asimismo, se les prohíbe a los usuarios que realicen

cualquier actividad con códigos de identificación de usuario que pertenezcan a otros usuarios (exceptuando user-IDs anónimo como “Huésped”).

24. Cambio forzoso de todos los password: Siempre que un sistema ha sido atendido por partes no autorizadas, los administradores del sistema deben cambiar inmediatamente cada password en el sistema. Incluso si sospechan además de un arreglo se requiere que todos los password se cambien inmediatamente. En cualquiera de estas circunstancias, una versión verdadera del manejo del sistema y de todo el software relacionado con seguridad debe también volverse a cambiar. Así mismo bajo ninguna de estas circunstancias, todos los cambios recientes al usuario y privilegios del sistema deben revisarse para modificaciones no autorizadas.
25. Acreditación personal de Identidad para obtener un password. Los passwords nunca deben descubrirse por medio de líneas telefónicas habladas. Para obtener un nuevo password o para cambiarlo, un usuario debe presentarse en persona y acreditar la identificación adecuada.
26. Requerimiento de Identificación positiva para el uso del sistema. Todos los usuarios deben estar identificados positivamente antes de poder usar cualquier MEDIO -- o por otros medios que proporcionen una seguridad igual o mayor antes de permitirles usar computadores de la Entidad conectados a una red.
27. No se deben almacenar juegos ni usar los sistemas del computador de la entidad para estas actividades. No deben almacenarse ni usarse juegos en ninguno de los sistemas del computador de la entidad.
28. Uso personal del computador y sistemas de comunicación. El computador de la Entidad y los sistemas de comunicación deben usarse solamente para asuntos de negocios. Se permite su uso para fines personales únicamente con permiso especial del administrador del Departamento.

29. Usos permitidos de información de la entidad. La información de la Entidad debe usarse solamente con fines comerciales expresamente autorizados por la administración.
30. Responsabilidad por daño a información y a programas por negligencia. La Entidad usa controles de acceso y otras medidas de seguridad para proteger la veracidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos, la administración debe tener la autoridad para: (1) restringir o derogar cualquiera de los privilegios del usuario, (2) inspeccionar, copiar, remover, o bien alterar algún dato, programa, u otro sistema que pueda socavar estos objetivos, y (3) tomar cualquier otra acción que estime necesaria para manejar y proteger sus sistemas de información. Esta autoridad puede emplearse con o sin notificación a los usuarios. La Entidad desconoce cualquier responsabilidad por pérdida o daño a la información o software que resulte de sus esfuerzos para lograr estos objetivos de seguridad.
31. El acceso no autorizado por medio de los sistemas de información de la entidad. Se prohíbe a los funcionarios que usen los sistemas de información de la Entidad para tener acceso no autorizado a cualquier otro de los sistemas de información o de cualquier forma dañar, alterar, o interrumpir las operaciones de estos sistemas. Del mismo modo se les prohíbe capturar o de otra forma obtener palabras claves, claves encriptados o cualquier otro mecanismo de control de acceso que pueda permitirles un acceso no autorizado.

XII. MANTENIMIENTO DE EQUIPOS DE TECNOLOGÍA

El mantenimiento preventivo y correctivo de los equipos de cómputo de la Empresa, será canalizada a través de Sistemas, cumpliendo con las siguientes disposiciones:

XIII. MANTENIMIENTO PREVENTIVO

22

1. El departamento de sistemas elaborara la programación de mantenimiento preventivo de los equipos de cómputo al inicio de cada vigencia, tomando como base el inventario de equipos de cómputo general de la Empresa provisto en la Mesa de ayuda (help desk) .
2. La programación de mantenimiento general se socializará una vez al año; adicionalmente se enviará la programación mensualmente a las dependencias de la Empresa a través del sistema de correo electrónico.
3. El mantenimiento preventivo de los equipos de cómputo e impresoras, se ejecutará dos (2) veces al año, garantizando procesos de la Empresa para el correcto funcionamiento y disponibilidad permanente de los equipos de cómputo.
4. Las Unidades Estratégicas de Negocios y procesos a las que le corresponda el mantenimiento de acuerdo con la programación establecida, deberán facilitar el espacio y los equipos de cómputo al personal técnico de mantenimiento para la ejecución del mantenimiento preventivo.
5. Actividades mantenimiento de equipo de cómputo: Se orientará a limpieza interna y externa, eliminación de virus informáticos, anti espías, liberación de espacio en disco (archivos temporales), uso de las herramientas del sistema (scandisk, desfrag, tareas programadas) y la eliminación de los cookies e historial de Internet.

6. Actividades mantenimiento de impresoras: Se orientará a la limpieza interna y externa, lubricación de piñonearía, alineación y limpieza de agujas, lubricación de barra estabilizadora, barra térmica, porta tonner, tarjeta lógica.
7. El personal técnico de mantenimiento de Sistemas, realizará las pruebas
8. Finalizado el procedimiento del mantenimiento, se procederá a diligenciar el TICKET de las actividades realizadas y el usuario hará la calificación de la atención recibida.

XIV. MANTENIMIENTO CORRECTIVO

1. El mantenimiento correctivo de los equipos de cómputo e impresoras, tendrá como requisito el diligenciamiento del TICKET a través de la Mesa de ayuda (help desk) por parte del usuario, indicando las anomalías o fallas presentadas.
2. El Usuario procederá a enviar el equipo de cómputo a Sistemas, con el fin se realice el diagnostico técnico de las fallas presentadas y su ejecución se realizará en la oficina de Gestión Tecnología.
3. Realizada la comprobación del problema el equipo, El departamento de sistemas enviará por correo electrónico el diagnostico técnico a la dependencia solicitante, con el fin de que se proceda a gestionar la compra del hardware requerido.
4. El tiempo de respuesta para la solución del mantenimiento correctivo, se hará teniendo en cuenta el trámite que realice Gestión Administrativa para la adquisición del hardware necesario para la ejecución y corrección de la falla presentada.
5. Finalizada las actividades de mantenimiento correctivo, el técnico realizará las pruebas necesarias para garantizar el correcto funcionamiento del

equipo, y hará entrega de conformidad al usuario final solicitante, registrando en la Mesa de ayuda (help desk) los hallazgos y actividades realizadas.

XV. ACTIVIDADES ADICIONALES

24

1. Brindar soporte técnico y asesorías de software y hardware, asesoría en redes, Internet y backups.
2. Acondicionar los equipos de cómputo e impresoras nuevos adquiridos por la Empresa, asegurando la correcta instalación y configuración del hardware y software, teniendo en cuenta el licenciamiento de la máquina y el nivel de acceso del usuario al uso de las aplicativos de la Empresa.
3. La administración de la infraestructura tecnológica

XVI. POLITICAS DE SOFTWARE Y APLICACIONES

1. El objetivo primordial de esta política es establecer los criterios para coordinar, estandarizar y controlar el proceso de desarrollo de software, administración y mantenimiento de aplicaciones para CARE SOLUTIONS COLOMBIA SAS mediante el establecimiento de disposiciones normativas que faciliten el cumplimiento de las necesidades de la empresa en materia de Sistemas informáticos
2. Todas las personas que hacen parte del departamento de sistemas de CARE SOLUTIONS COLOMBIA SAS deberán acatar las siguientes normas:

3. Todas las normas previstas en el presente documento son autorizadas por la Gerencia de Sistemas que tendrá el control de todos los accesos y privilegios sobre la oficina de Desarrollo y artículos que contiene este documento.
4. Bandera de advertencia de seguridad en el sistema de acceso: Todo proceso de log-in para computadores multiusuario debe incluir una advertencia especial. Esta advertencia debe indicar: (1) el sistema es para ser usado solamente por usuarios autorizados, y (2) el continuo uso del sistema por el usuario indica que él / ella es un usuario autorizado.
5. Asignación de pertenencia de la información: La administración debe claramente especificar por escrito la asignación de las responsabilidades de pertenencia para bases de datos, archivos principales, y otra información compartida. Estas declaraciones deben también indicar los individuos a quienes se les ha dado autoridad para originar, modificar, o borrar tipos específicos de información encontrada en estos conjuntos.
6. Separación de actividades y datos de usuario-a-usuario: La administración debe definir los privilegios del usuario para que usuarios comunes no puedan lograr acceso, o de otra forma interferir con actividades individuales o datos privados de otros usuarios.
7. Capacidades del usuario para el acceso de archivos y su implicación en cuanto al uso: Los usuarios no deben leer, modificar, borrar, o copiar archivos que pertenezcan a otro usuario sin obtener primero permiso del propietario del archivo. A menos que el acceso general haya sido claramente proporcionado, la habilidad para leer, modificar, borrar, o copiar un archivo que pertenezca a otro usuario no
8. Actualización de la Información comercial en producción: Definir privilegios del sistema para que el personal que no pertenezca al usuario final responsable (auditores internos, coordinadores, ingenieros de soporte, etc.)

no se les permita modificar directamente los datos de información comercial en el ambiente de producción.

9. Parámetros y convenciones estándar para utilizar en los sistemas: Para alcanzar un control de acceso seguro a través de diferentes tipos de sistemas automatizados, se deben utilizar estándares para los códigos de identificación de usuario, nombres estándar para programas y archivos tanto en ambientes de producción como en pruebas, nombres de sistemas de información y otras convenciones utilizadas en tecnología. Mantenimiento del código de identificación del Usuario Master y Base de Datos privilegiadas: Para revocar oportunamente los privilegios en los registros de los códigos de identificación de usuario almacenados en los sistemas automáticos, deben actualizarse y respaldarse los archivos que los contienen.
10. Eventos relevantes de seguridad a almacenarse en los Logs del sistema: Todos los sistemas automáticos que operen y administren información sensible, valiosa o crítica para CARE SOLUTIONS COLOMBIA SAS , deben tener archivos Logs donde se tenga evidencia sobre todos los eventos relevantes que se sucedieron con la información automatizada y con las seguridades necesarias relacionadas con la consulta, modificación o borrado. Ejemplos sobre seguridades, intentos de adivinar la palabra clave, intentos para usar privilegios que no han sido autorizados, modificaciones al software de aplicación en el ambiente de producción, y modificaciones al software ambiental del sistema.
11. Contenido de Logs en los sistemas de aplicaciones en ambiente de producción: Todo software aplicativo habilitado en ambiente de producción de CARE SOLUTIONS COLOMBIA SAS debe incluir archivos Logs que registren como mínimo la siguiente información: (1) la actividad hecha en la sesión abierta por el usuario incluyendo la identificación del código del usuario, fecha/hora de la entrada y de la salida de cada sesión del sistema,

aplicaciones invocadas, (2) cambios de información en los archivos de las aplicaciones críticas (3) adiciones y/o cambios a los privilegios de los usuarios, y (4) fecha/hora de iniciación y terminación de ingreso al sistema de información.

12. Logs para reanudación rápida de actividades de producción del sistema:

Las aplicaciones comerciales de carácter vital o crítico para CARE SOLUTIONS COLOMBIA SAS , requieren tener archivos de Logs robustos. Todas las aplicaciones comerciales críticas deben apoyarse en Logs que permitan que las actividades del sistema puedan ser reanudadas, después de presentarse una contingencia.

13. Arquitectura de los sistemas para actividades que se apoyan en Logs: Los actividades del usuario y sus estadísticas, que permitan detectar y disparar alarmas que reflejen eventos sospechosos.

14. Programas que consumen excesivos recursos del sistema: Los usuarios del sistema no deberán escribir o ejecutar ningún programa o proceso automático que consuma demasiados recursos de máquina y que puedan afectar el normal rendimiento de los trabajos de CARE SOLUTIONS COLOMBIA SAS.

15. Los usuarios del sistema no deben incluir virus en el software: Los usuarios del sistema no deberán escribir, generar, compilar, copiar, propagar, ejecutar, o intentar introducir intencionalmente cualquier código a la computadora, que haya sido diseñado para causar daño o impedir la normal actuación de la memoria de la máquina, archivos de datos o programas, sistemas operativos o software aplicativo. Estos programas nocivos son conocidos como virus.

16. Identificación los requerimientos de seguridad antes del desarrollo o adquisición de un sistema: Antes de que un nuevo sistema se desarrolle o se adquiera, los responsables de proceso deberán haber especificado los requerimientos de seguridad necesarios. Es conveniente tener en cuenta

las alternativas sugeridas por los diseñadores, vendedores y/o proveedores, para que se obtenga un equilibrio apropiado entre la seguridad y los objetivos de facilidad de uso, eficiencia operacional, facilidad de actualización, escalabilidad y costo aceptable, entre otros.

17. Estándares para el desarrollo de sistemas de CARE SOLUTIONS COLOMBIA SAS.

18. El departamento de sistemas de información deberá asegurar que todo desarrollo de software y actividades de mantenimiento de este, cumplan con las políticas, normas, procedimientos, controles y otras convenciones estándares aplicables para el desarrollo de sistemas.

19. No ejecutar pruebas al software en ambientes de producción: No es permitido ejecutar pruebas al software aplicativo con datos o información real del ambiente de producción. Documentar la ocurrencia de errores y las acciones a seguir para el software desarrollado: Todo software que se desarrolle o personalice en CARE SOLUTIONS COLOMBIA SAS y que produzca resultados no esperados, siempre deberá producir mensajes de error y las acciones a seguir por parte del usuario deberán documentarse.

20. Todo sistema de información automático deberá presentar mensajes de respuesta cuando se ejecute una transacción: Toda intervención que tenga un usuario con el sistema, deberá reportar un mensaje automático que indique si la transacción o evento se ejecutó correctamente o presentó alguna falla.

21. Todo desarrollo de software debe tener requerimientos formales: Se deberán definir previamente las especificaciones o requerimientos formales para todo desarrollo

22. El acuerdo deberá ser completado y aprobado antes de comenzar el desarrollo o personalización del código del sistema.

23. Eliminación todas las rutas de acceso no autorizadas en los ambientes de producción: Antes de trasladar al ambiente de producción el software

desarrollado, los programadores o personal técnico de informática deberán eliminar todas las rutas de acceso especiales o privilegiadas, para que solamente puedan ser obtenidas de acuerdo con los procedimientos corporativos normales de seguridad. Todos los privilegios de usuarios especiales que se concedieron para el desarrollo del software no deberán ser permitidos en el ambiente de producción.

24. Utilización técnicas y herramientas de desarrollo probadas y confiables: Para todo desarrollo de software se deberán utilizar técnicas y herramientas de desarrollo conocidas en el mercado local del que se tenga certeza que su comportamiento es seguro y confiable.
25. Uso de lenguajes de programación de alto nivel: Utilizar lenguajes de programación de últimas generaciones para reducir el volumen de código a desarrollar, la dificultad de mantenimiento del software, el tiempo exigido para desarrollar una aplicación, y el número de fallas.
26. Utilización de convenciones estándar para nombrar los archivos en el ambiente de producción: Se deberán utilizar convenciones estándar para nombrar los archivos del ambiente de producción, que permitan diferenciarlos claramente de los respectivos archivos utilizados en los ambientes de desarrollo, pruebas o con propósitos de entrenamiento.
27. Documentación estandarizada para toda la tecnología que se encuentre en el ambiente de producción: Cada usuario que desarrolle o implemente software o hardware para ser usado por CARE SOLUTIONS COLOMBIA SAS en las actividades propias del negocio, deberá documentar el sistema de acuerdo con el avance de la Implementación. La documentación deberá ser escrita para que el sistema pueda ser utilizado por personas no familiarizadas con él. La documentación deberá cubrir usuarios finales operativos y técnicos.
28. El uso de medios de almacenamiento para los sistemas de utilidades residentes en ambientes de producción: Los discos y otros medios de

almacenamiento en línea usados en sistemas de computación en producción no deberán contener compiladores, ensambladores, editores de texto, procesadores de palabra u otras utilidades de propósito general que puedan utilizarse para comprometer la seguridad del sistema.

29. El personal de desarrollo de sistemas no debe ser el responsable de las pruebas
30. Todo cambio por terceros al software en producción deberá requerir aprobación especial: Se deberá obtener primero un permiso por escrito del jefe del área, para que el proveedor o desarrollador del software de aplicación efectúe modificaciones a este sistema. Cuando las modificaciones han sido aprobadas, el software modificado deberá documentarse, probarse, y en general, ajustarse a los procedimientos de control de cambios establecidos por CARE SOLUTIONS COLOMBIA SAS , antes de ser trasladado al ambiente de producción.
31. Los mantenimientos al software deberán realizarse únicamente sobre el código fuente: Todos los cambios permanentes al software en producción deberán hacerse con el código fuente en lugar del objeto u otro código ejecutable.
32. Procedimientos para el regreso a una versión anterior del software en producción: Procedimientos para el regreso a una versión anterior "back off" deberán ser desarrollados para todos los cambios al software que se encuentre en producción (del sistema, aplicativo). Ellos permiten a las actividades de procesamiento de datos un rápido y conveniente regreso a la anterior versión del software o estado de datos, para que las operaciones del negocio puedan continuar.
33. Todo software que se incorpore a producción debe tener su propio plan de contingencia: Siempre que se pase al ambiente de producción un nuevo software o uno significativamente modificado, se requieren procedimientos contingentes especiales para evitar considerables pérdidas en CARE

SOLUTIONS COLOMBIA SAS . La administración deberá preparar un plan de contingencia de conversión que refleje las diferentes formas o maneras de asegurar la continuidad del servicio a los usuarios que potencialmente se puedan ver afectados.

34. Los funcionarios deberán conceder a CARE SOLUTIONS COLOMBIA SAS, exclusividad sobre los derechos de propiedad intelectual de sus desarrollos: Todos los derechos de propiedad intelectual de los productos desarrollados o modificados, por los empleados de la institución, durante el tiempo que dure su relación laboral son de propiedad exclusiva de CARE SOLUTIONS COLOMBIA SAS.
35. Todos los derechos de propiedad sobre el software y la documentación desarrollada para uso corporativo son exclusivos de CARE SOLUTIONS COLOMBIA SAS: Sin excepción alguna, todo el Software y su documentación generada y desarrollada por funcionarios, consultores, proveedores o contratistas para el beneficio y uso Corporativo, es propiedad exclusiva de CARE SOLUTIONS COLOMBIA SAS.

El jefe de Sistemas deberá asegurarse que todos los funcionarios, consultores, proveedores o contratistas proporcionen a CARE SOLUTIONS COLOMBIA SAS una declaración escrita en constancia de aceptación de esta política, antes de iniciar.

1. Todos los derechos de propiedad legal sobre archivos fuente de aplicación y mensajes, son exclusivos de CARE SOLUTIONS COLOMBIA SAS : CARE SOLUTIONS COLOMBIA SAS tiene propiedad legal sobre el contenido de todos los archivos almacenados en los equipos de cómputo y sistemas en red, así como de todos los mensajes que viajan a través de estos

sistemas. CARE SOLUTIONS COLOMBIA SAS se reserva el derecho de permitir el acceso a esta información a terceras personas.

2. Adquirir las licencias de software necesarias para desarrollar las actividades corporativas: El jefe de sistemas deberá adquirir licencias de software de uso generalizado adicionales, para los casos en que los funcionarios las soliciten.
3. Para el intercambio de software y/o datos con terceros se requiere de acuerdos por escrito: Los intercambios de software y/o datos entre CARE SOLUTIONS COLOMBIA SAS y cualquier tercero, no se deberán realizar sin un acuerdo por escrito. Tal acuerdo, debe especificar los términos del intercambio, así como las formas que el software y/o los datos serán manejados y protegidos.
4. Toda solicitud de los usuarios debe ser soportada con su respectivo código diligenciado en el TICKET a través de la Mesa de Ayuda (help desk)
5. El usuario debe diligenciar y remitir a sistemas el TICKET a través de la mesa de ayuda (help desk) teniendo en cuenta siguientes características:
6. Necesario: Un requerimiento es necesario si su omisión provoca una deficiencia en el sistema a construir, y además su capacidad, características físicas o factor de calidad no pueden ser reemplazados por otras capacidades del producto o del proceso.
7. Conciso: Un requerimiento es conciso si es fácil de leer y entender. Su redacción debe ser simple y clara para aquellos que vayan a consultarlo en un futuro.
8. Completo: Un requerimiento está completo si no necesita ampliar detalles en su redacción, es decir, si se proporciona la información suficiente para su comprensión.
9. Consistente: Un requerimiento es consistente si no es contradictorio con otro requerimiento.

- 10.No ambiguo: Un requerimiento no es ambiguo cuando tiene una sola interpretación. El lenguaje usado en su definición no debe causar confusiones al lector.
- 11.Verificable: Un requerimiento es verificable cuando puede ser cuantificado de manera que permita hacer uso de los siguientes métodos de verificación: inspección, análisis, demostración o pruebas.
- 12.Disponibilidad presupuestal: Todo requerimiento que implique nuevas herramientas tecnológicas deberá tener su debido estudio que será revisado y aprobado por el área de planeación de CARE SOLUTIONS COLOMBIA SAS

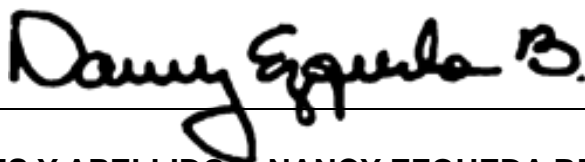
XVII. MEDIDAS DISCIPLINARIAS

El incumplimiento de las disposiciones de este reglamento estará sujeto a investigación administrativa y a la imposición de las medidas disciplinarias correspondientes.

Cordialmente

En constancia, se firma a los CINCO (5) días del mes de ENERO de 2024

FIRMA



NOMBRES Y APELLIDOS: NANCY EZQUEDA BENITO REVOLLO

Cédula de Ciudadanía No. 64.555.294