I. OBJETIVO

Asegurar que los recursos de los sistemas de Información (material informático y programas) de la compañía Datacontrol Portuario, sean utilizados de la mejor manera y que el acceso a la información allí contenida así como su modificación solo sea posible por las personas que se encuentren acreditadas y dentro de los límites de su autorización.

El objetivo de este procedimiento es prevenir los riesgos y establecer los lineamientos para:

- proteger los sistemas de información de la compañía (hardware y software)
- proteger las bases de datos
- manejo de contraseñas de acceso
- seguridad de los correos electrónicos
- backup de la información
- soporte del área entre otros.

II. ALCANCE

Todos los sistemas de información (hardware y software) de la compañía.

III. DEFINICIONES

Backup: Seguridad, Recursos adicionales o copias duplicadas de datos como prevención contra emergencias.
Servidor: Modelo lógico de una forma de proceso cooperativo, independiente de plataformas hardware y sistemas operativos
Base de Datos: Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
Activo: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños o perdidas en sus activos.
Impacto: Medir la consecuencia al materializarse una amenaza.
Riesgo: Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.
Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal del negocio
Contraseña, password: Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a un usuario para acceder a un determinado recurso (Software/Hardware).
Usuario Final: es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona. Generalmente se identifica frente al sistema o servicio utilizando un nombre de usuario y a veces una contraseña

IV. RESPONSABLES

- Coordinador de proyectos (grupo GEPSA): establece los lineamientos y direcciona los controles
- Soporte de sistemas (DATACONTROL PORTUARIO): ejecuta los controles
- Usuarios de los sistemas informáticos: deben acatar los lineamientos y efectuar la administración, actualización y backups de la información asignada según su cargo.

V. NORMAS GENERALES

1- El encargado de soporte de sistemas velará porque los servidores y equipos de comunicaciones estén ubicados en instalaciones físicas, que estén debidamente administradas, cuenten con condiciones ambientales adecuadas, tengan mecanismos de seguridad lógica y física apropiados y que cuenten con planes de contingencia vigentes.

2- Bajo ninguna circunstancia el personal de la empresa podrá utilizar los recursos informáticos de la empresa para realizar actividades prohibidas por las normas de la institución o por normas jurídicas nacionales o internacionales.

3- Las copias de seguridad de los sistemas de información deben ser almacenados en las oficinas de GEPSA, en la ciudad de Cali.

VI. ESQUEMA E INFRAESTRUCTURA DE RED

TLBUEN

1 Equipo

1 Biométrico

PLATAFORMA

9 Equipos

1 Biométrico

SPRBUN

4 Equipos

2 Biométricos

DATACONTROL

19 Equipos

1 Biométrico

TCBUEN 2

2 Equipos

2 Biométricos

VII. RED TECNOLOGICA DE DATACONTROL PORTUARIO

1. SEDE PRINCIPAL RED LAN DATACONTROL

- Equipos de Cómputo: 19

Marca: Lenovo
Sistemas operativos : Windows 7(seven)

- **Impresoras de red**
  - Ricoh Aficio 2020D
  - Hp Color LaserJet 3800N
- **SCANNERS**
  - Hp Scanjet G2410
- **SERVIDOR**
  - PowerEdge SC1430

  Procesador Intel Xeon 5140 a 2.33GHZ
  4GB Memoria Ram
  Sistema Operativo Windows 2003 Server R2
  El cual soporta aplicaciones como CG1(software contable) y MP2(software de Gestion de mantenimiento)

Todos los elementos anteriores están soportados en:

- Switch 24 Puertos ALIED TE
- Router CISCO 1841 V04
- Router TPLINK N750 DUAL BAND para salida internet Inalámbrico

Soporte eléctrico 1 Ups, Marca APC, Modelo: Smart-ups 5000

Soporte internet

Proveedor: SERCONRED
IP Pública: 190.90.121.133
Velocidad: 4 Megas

2. **SEDE PLATAFORMA** RED LAN

- Equipos de Cómputo: 9
  Marca: Lenovo
  Sistemas Operativos: Windows 7(seven)
- **IMPRESORAS**
  Marca: hp
  Modelo: LaserJet p1102w
- **SCANNER**
  Marca: hp
  Modelo: scanjet G2410
- **SERVIDORES (2)**
  Marca: Hp
  Modelo: Proliant DL 120 G7
  Procesador: Intel Xeon E31220 a 3.10GHZ
  Memoria: 8GB
  Sistema Operativo: Windows 2008 server R2
  1 servidor soporta la aplicación WEB de Datacontrol Portuario para el manejo de la operación portuaria
  1 servidor soporta la aplicación de Proveedor Proware (sistema Biométrico)

SOPORTE ELECTRICO 1 UPS, Marca: APC, Modelo: Smart-ups 5000
Todo interconectado a través de Switch, Marca: DLINK 16 Puertos
Modelo: DES-1016D

CIRCUITO CERRADO DE TV en Plataforma actualmente en ampliación

- DVR
  Marca: Infinova
  Modelo: V3010116L
  6 cámaras Infinova – actualmente se instalan nuevas cámaras
  1 Domo PTZ – actualmente se instalan 3 domos adicionales

3. SEDE SOCIEDAD PORTUARIA

- Equipos de Cómputo: 4
  Marca: Lenovo
  Sistema Operativo: Windows 7(seven)
  Soportados por:
  Switch 16 Puertos
  Marca: DLINK
  Modelo: DES-1016D
- **IMPRESORAS (2)**
  Marca: Hp
  Modelo: LaserJet p2050 RED
  Marca: HP
  Modelo: LaserJet 1020 USB

4. SEDE TCBUEN

- Equipos de cómputo (2)
  Marca: Lenovo
  Sistema Operativo: Windows 7(seven)
  Marca: Intel
  Sistema Operativo: Windows XP SP3
- **IMPRESORAS (**1)
  Marca: hp
  Modelo: LaserJet p1102w

5. SEDE TLBUEN

Cuenta con sistema integrado de seguridad que incluye CCTV, control de acceso, control de intrusión y control de incendios. La información detallada se suministrará en caso de ser requerida.

NOTA:

Las sedes de SPRBUN, TLBUEN, TCBUEN y CROSS-DOKING(Nuevo patio de Datacontrol – antiguo granmuelle), están interconectadas a la red de Datacontrol oficina principal a través de la tecnología “CLEAR CHANNEL” servicio que presta nuestro proveedor por lo cual los equipos de estas sedes los vemos como si estuvieran directos en nuestra red LAN.

VIII. LAS AMENAZAS

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es el backup (en el caso de los datos) y la descentralización.

Estos fenómenos pueden ser causados por:

El usuario: Causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).
Programas maliciosos: Programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el servidor abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.
Un intruso: Persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido.
Un siniestro (robo, incendio, por agua): una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.
El personal interno de Sistemas: Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.
Términos relacionados con la seguridad informática

IX. NIVEL DE SEGURIDAD

En la compañía DATACONTROL PORTUARIO hemos establecido los siguientes niveles de seguridad, para proteger la información de los riesgos a los cuales está expuesta: adulteración, pérdida, filtración, divulgación no autorizada, información errónea, información incompleta, ocultar información.

Estos niveles de seguridad están asociados a los cargos de los empleados de la compañía y aseguran la seguridad en la información.

CLASE DE INFORMACION

I	INFORMACION DE PROVEEDORES
II	INFORMACION DE CLIENTES Y FACTURACION
III	INFORMACION OPERATIVA
IV	INFORMACION DE NOMINA
V	INFORMACION DE MANTENIMIENTO
VI	INFORMACION SISTEMAS DE GESTION
VII	INFORMACION FINANCIERA Y CONTABLE
VIII	INFORMACION GERENCIAL
IX	INFORMACION DE ALMACEN

TIPO DE RESPONSABILIDAD

A	CONTACTO - CONSULTA
B	ARCHIVO - CONTACTO - CONSULTA
C	ACTUALIZACION - ARCHIVO - CONTACTO - CONSULTA

NIVEL DE SEGURIDAD

ALTO	mayor responsabilidad dirigido a cargos de alto rango y específicos autorizados para la actualización y archivo de la información
MEDIO	dirigido a aprendices y asistentes que requieren acceder a la información
BASICO	solo consulta la información

X. POLÍTICAS DE IDENTIFICACIÓN DE USUARIO

1. Usuarios

La empresa Datacontrol Portuario tiene como política para la creación de usuarios en sus equipos de cómputo, la identificación del mismo a través del nombre del cargo a ostentar evitando así cambios por salida o remoción de los usuarios a otras dependencias de la empresa.

2. Contraseñas

Las contraseñas de los equipos de cómputo de Datacontrol están definidas en primera instancia por el soporte de sistemas, quien genera una contraseña estándar, la cual será solicitada al primer ingreso del usuario y le pedirá cambio, generando así una contraseña que solo será conocida por el usuario autorizado.

Normas generales para el buen manejo de contraseñas:

- Tener ocho caracteres alfanuméricos (letras y números) como mínimo.
- No contener nombres (del usuario, de familiares, de amigos, etc.).
- No ser una palabra o nombre común.
- Ser significativamente diferente de otras contraseñas anteriores.
- La contraseña es personal e intransferible
- tendrán una duración mínima de 10 días y máxima de 56.

Procedimiento para el cambio de contraseñas:
Las Contraseñas de usuario serán cambiadas a través de la configuración del sistema operativo que automáticamente le exigirá al usuario el cambio después de 56 días, esta podrá ser cambiada por el usuario antes de este periodo en caso de que el usuario presienta que su contraseña fue Vulnerada.
Las contraseñas de administrador de sistema serán cambiadas por este de acuerdo a su criterio y no podrá ser superior a 90 días, proceso de salvaguarda de estas

Las contraseñas de correo electrónico son administradas por el departamento de sistemas de la compañía

Las contraseñas de las aplicaciones de Datacontrol Portuario
*Sistemas contable CG1 (Control Y Registro)
*Sistema s de gestión Integral de Información (GII
*Sistema de Gestión de Bodega
*Sistema Control Biométrico

Para realizar el cambio de contraseña en las aplicaciones de la empresa se deben seguir los siguientes pasos.

1. Ingresar a las aplicaciones de la empresa

El auxiliar de sistemas ingresa como administrador a cada una de las aplicaciones.

2. Cambiar Contraseña

En cada de una de las aplicaciones se debe escoger usuario por usuario para cambiarle la contraseña.

3. Notificación a los usuarios

Se debe comunicar de manera personal a cada uno de los usuarios el cambio de su contraseña.

4. Olvido de Contraseña

Si por algún motivo el usuario se le olvida la contraseña debe solicitar por escrito via mail al administrador el cambio de contraseña.

XI. HARDWARE

Los equipos servidores se encuentran ubicados en buenaventura en instalaciones propias de la siguiente manera:

1. Servidor De sistema contable CG1: Ubicación en sede Central de Datacontrol portuario Edificio Pacific Trade Center Apoyado en seguridad por cámara externa perteneciente al entorno del edificio.
2. Servidor De Gestión Integral De Información GII : Ubicación Patio de Contenedores (antiguo gran muelle) en 2do Piso del contenedor asegurado por sistema de CCTV con condiciones ambientales reguladas para tal fin.
3. Servidor De Sistema control Biométrico : : Ubicación Patio de Contenedores (antiguo gran muelle) en 2do Piso del contenedor asegurado por sistema de CCTV con condiciones ambientales reguladas para tal fin.

Todas las sedes de estos servidores cuentan con su respectivo sistema de contingencia y apoyo eléctrico que garantiza la sostenibilidad de estos en caso de fallas en el suministro

XII. SOFTWARE

La empresa Datacontrol portuario cuenta con sus respectivos procesos de respaldo de seguridad de sus sistemas que se realizan de la siguiente Configuración

- **sistemas Contable CGUNO y de nómina NMUNO**: se le realiza copia diaria a través de la red antes de empezar la jornada laboral donde se copian todos los archivos pertenecientes del software CG1 al equipo del área contable Control Y Registro este proceso es ejecutado por el usuario Asignado al puesto proceso denominado HIJO.

  Los días sábados 3:30AM de cada semana se le hace copia general a este servidor a través del asistente para Copias de seguridad inserto en el sistema operativo Windows 2003 server que este posee esta copia va directo al disco extraíble designado para esta labor proceso denominado PADRE copiando así las bases de datos tanto del software CG1 como el de MP2 (sistemas Gestión Almacén)

  Los días finales del mes se realiza una copia master de los servidores que incluye pasar las Copias HIJO, PADRE a otra unidad Externa a cargo del Asistente de Sistemas que es Ubicada fuera de los recintos Físicos de la empresa

- **Software GII**: La copia de seguridad de este servidor se hace semanal los días Viernes a las 3:30AM a través del proceso de copias de seguridad inserto en el sistema operativo esta copia se hace en la red a una carpeta compartida Ubicada en el servidor Biométrico, Luego esta copia es recogida y llevada a una unidad de disco externo asignada al asistente de sistemas de la empresa
- **Software Biométrico**: La copia de seguridad de este servidor se hace semanal los días Viernes a las 3:30AM a través del proceso de copias de seguridad inserto en el sistema operativo esta copia se hace en la red a una carpeta compartida Ubicada en el servidor GII, Luego esta copia es recogida y llevada a una unidad de disco externo asignada al asistente de sistemas de la empresa

La compañía Datacontrol portuario mantiene el último software de detección de virus para PC disponible, así como otras funciones de seguridad de los sistemas, como el spam y los sistemas de protección con cortafuegos.

Los cortafuegos, filtros de spam y otras aplicaciones que se proporcionan a nivel mainframe. La protección contra virus y spyware, cuando es necesario, se proporcionan a nivel de estación de trabajo

XIII. MAIL E INTERNET

La empresa mantiene un sistema de correo electrónico (e-mail) para ayudar a los empleados en la realización de negocios en la empresa. El acceso a Internet se proporciona a los empleados, siempre y cuando tengan una necesidad demostrable para acceder a Internet. Todos los mensajes que se redactan, envió o recibió en el sistema de correo electrónico y la Internet es y siguen siendo propiedad de la empresa. Los empleados no deben tener ninguna expectativa de privacidad de las comunicaciones por correo electrónico o Internet. La confidencialidad de cualquier mensaje no debe ser asumido. Incluso cuando un mensaje se borra, todavía es posible recuperar y leer el mensaje. La empresa se reserva el derecho a leer, revisar, auditar, interceptar, acceder y divulgar todos los mensajes creados, recibidos o enviados a través del sistema de correo electrónico o Internet.

Correo electrónico e Internet no debe usarse para beneficio personal o el adelanto de puntos de vista individuales. Oferta de negocio sin compañía, o cualquier uso para beneficio personal, está estrictamente prohibido. Los mensajes con comentarios despectivos o inflamatorios sobre un individuo o grupo, raza, religión, origen nacional, atributos físicos, o preferencia sexual no pueden ser transmitidos o recibidos a través de equipos de la empresa o de software. Ciertas áreas de la Internet se bloqueará automáticamente el acceso, como los sitios que contienen referencias a los juegos de azar o pornografía.

La violación de las políticas de correo electrónico o de Internet puede resultar en acción disciplinaria hasta e incluyendo el despido. Los empleados son alentados a informar de cualquier uso ilegal de la Internet a su Manager.

XIV. Página de Identificación de Usuarios

Todos los usuarios serán creados por el administrador del sistema de la red a cargo del asistente de sistemas de Datacontrol Portuario previa Autorización del gerente de la empresa

UBICACIÓN	USUARIO	ID(Identificador de Usuario)
Gerencia	Diego Yepes Isaza	Ggraldata
Gerente Operaciones	Glaston Panchano mena	Glastonp
Coordinadora Desempeño	Ángela Otero	Coor_desem
Recurso Humano	Mónica Motato	Mmotato
Contaduría	Carlos Mosquera	Cmosquera
Secretaria General	Cruz Elena Ramirez	Secretaria
Compras	David Colorado	Asis_Compra
Control Y Registro	Gloria Corrales	Contr_YRegist
Control y Registro	Diego Guzman	Aux_cont_Regis
Talento Humano	Maribel Portocarrero	Talento
Talento Humano	Ma. del Pilar Gomez	Aux_Talento
Asistente TLBUEN	Leidy Angulo	Asis_tlbuen
Auxiliar Administrativo	Edwin Caicedo	Aux_Admin
Tesorería	Carmen Micolta	Tesoreria
Facturación	Luz Dary Moran	Facturacion
Video Conferencia	Geiler Suarez	Video Conferencia
Auxiliar Sena	Practicante	Aux_sena
Área Scanner	Practicante	Scanner

XV. SISTEMA DE DETECCION IDS (Política y Responsabilidades)

Responsabilidades del administrador del sistema:

- El administrador del sistema emitirá todos los ID de usuario.
- El administrador del sistema emitirá la contraseña inicial para el ID de usuario, sin embargo, el empleado será responsable de cambiar la contraseña.
- Cada usuario del sistema debe tener un ID de usuario individual y no puede ser compartida.
- Inactivo o no utilizados del ID de usuario se desactivará después de 90 días y se eliminan después de 6 meses de inactividad.
- El administrador del sistema revocará la autorización por las siguientes razones:
  - El empleo se termina.
  - Empleado o las solicitudes del gerente de la revocación.
  - Hay varios intentos de acceder a datos no autorizados.
  - Seguridad es violada.

Responsabilidades del empleado:

- Cada empleado autorizado se le asigna una identificación de usuario y contraseña para acceder a sus equipos. A menos que una persona no autorizada obtiene una contraseña, no será capaz de acceder a bases de datos de Datacontrol Portuario SA.
- Los nuevos usuarios deberán cambiar sus contraseñas la primera vez que se accede a la cuenta.
- Los empleados no deben compartir su ID de usuario o contraseñas con otras personas o que les permitan acceder al sistema utilizando su ID de usuario
- Los empleados están obligados a notificar a la gerencia y el administrador de sistemas si creen que su ID de usuario o la contraseña ha sido comprometida.

Elaborado por:	Revisado y Aprobado por:
Ángela María Otero Coordinadora de Desempeño	**Diego Yepes** Gerente General

Lista de Copias Controladas del Procedimiento

Copia No.	Área de Ubicación	Firma Recibido	Fecha

Registro de Actualizaciones del Procedimiento

Versión No.	Fecha	Descripción del Cambio