 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	1 de 16

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.

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	2 de 16

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

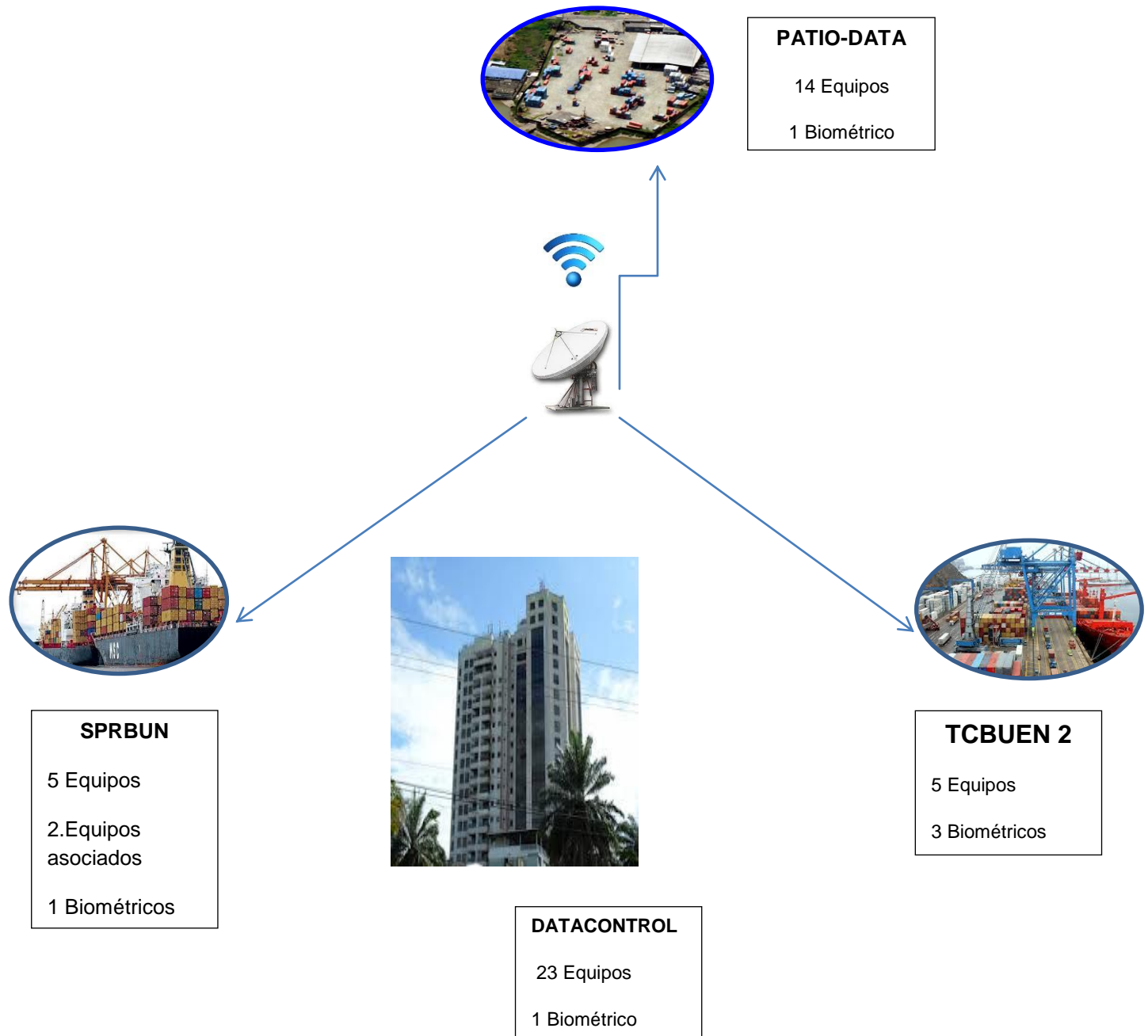
- Coordinador de proyectos (grupo PIO.S.A.S): establece los lineamientos y direcciona los controles
- Soporte de sistemas (DATACONTROL PORTUARIO): ejecuta los controles
- Usuarios de los sistemas informáticos: deben acatar los lineamientos y efectuar la administración, actualización y backups de la información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


V. NORMAS GENERALES

- 1- El auxiliar de sistemas velará porque todos los equipos e infraestructura estén ubicados en instalaciones físicas, 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 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 GRUPO PIO S.A.S, en la ciudad de Cali.

	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	3 de 16

VI. ESQUEMA E INFRAESTRUCTURA DE RED



 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	4 de 16

VII. RED TECNOLOGICA DE DATACONTROL PORTUARIO

1. SEDE PRINCIPAL RED LAN DATACONTROL

- Equipos de Cómputo: 23
Marca: Lenovo
Sistemas operativos : Windows 7(seven)
- **Impresoras de red**
 - Ricoh Aficio MP2332D
- **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)
- **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(sistemaBiométrico)


Todos los elementos anteriores están soportados en:

- Switch 48 Puertos Cisco System Catalyst 2960
- 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: 7 Megas

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	5 de 16

2. SEDE PATIO-DATACONTROL RED LAN

- Equipos de Cómputo: 14
 Marca: Lenovo
 Sistemas Operativos: Windows 7(seven)
 - **IMPRESORAS(5)**
 Marca: hp
 Modelo: LaserJet p1102w
 - **SCANNER**
 Marca: Canon
 Modelo: QC3-5241-DB01-03

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 Patio Datacontrol actualmente en ampliación

DVR Marca: Trime 960H Real Time de 32 Puertos

Camaras : 27 camaras (marcas Infinova,sansumg y Gess)Incluidos 2 Domos
 ubicados en el área de cobertizo y las demás en todas las ares operativas y de
 oficina donde se requieren

Monitores : 2 Televisores 1 de 50" monitor Principal y un 2do para determinar una
 cámara fija previa necesidad operativa

Este circuito CCTV se encuentra conectado a internet para su visualización desde
 cualquier lugar del mundo

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	6 de 16

3. SEDE SOCIEDAD PORTUARIA

- Equipos de Cómputo: 5
Marca: Lenovo
Sistema Operativo: Windows 7(seven)
Soportados por:
Switch 16 Puertos
Marca: DLINK
Modelo: DES-1016D
- **IMPRESORAS (2)**
Marca: Ricoh
Modelo: Aficio MP301
Marca: HP
Modelo: LaserJet P3015

Esta sede se le adecua oficina al cliente Satlock con 2 equipos de computo conectados a nuestra Red Lan

4. SEDE TCBUEN


- Equipos de cómputo 5
Marca: Lenovo
Sistema Operativo: Windows 7(seven)
- **IMPRESORAS (2)**
Marca: hp
Modelo: LaserJet p1102w

NOTA:

Las sedes de SPRBUN, TCBUEN y PATIO DATACONTROL, 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

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	7 de 16

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.

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO CR-P-12	FECHA EMISION DD - MM - AA 17-07-2015	VERSION 3	PAGINA 8 de 16

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

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	9 de 16

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

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	10 de 16

Las contraseñas de las aplicaciones de Datacontrol Portuario

- *Sistemas contable CG1 (Control Y Registro)
- *Sistemas de gestión Integral de Información (GII)
- *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 al administrador el cambio de contraseña.

XI. HARDWARE

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

1. 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 en sede Central de Datacontrol portuario Edificio Pacific Trade Center Apoyado en seguridad por cámara externa perteneciente al entorno del edificio.
3. Servidor De Sistema control Biométrico : Ubicación en sede Central de Datacontrol portuario Edificio Pacific Trade Center Apoyado en seguridad por cámara externa perteneciente al entorno del edificio.

la sede 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

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	11 de 16

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 diariamente a las 3:30AM a través del proceso de copias de seguridad inserto en el sistema operativo esta copia se hace en un disco duro externo (USB) asignada al asistente de sistemas de la empresa
- **Software Biométrico:** La copia de seguridad de este servidor se hace diariamente a las 3:30AM a través del proceso de copias de seguridad inserto en el sistema operativo esta copia se hace en un disco duro externo (USB) 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

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	12 de 16

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 difamatorios 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 administrador.

Instalación de cuentas en celular

los usuarios que necesiten configurar su cuenta de correo corporativa en sus dispositivos móviles deberán contar con la aprobación de gerencia y este manifestarlo al área de sistemas quien se encargara del proceso


 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	13 de 16

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
Sub gerencia	Ricardo Ramirez	Jefe Mercadeo
Coordinadora Desempeño	Ángela Otero	Coor_desem
Recurso Humano	Mónica Motato	Mmotato
Contaduría	Carlos Mosquera	DCPcontador
Secretaria General y recepción	Cruz Elena Ramirez	DCPsecregerencia
Compras	David Colorado	DCP_compras
Control Y Registro	Gloria Corrales	DCPcontyregis
Control y Registro	Diego Guzman	DCPcontyregis1
Talento Humano	Yovanny Viveros	DCPtalento
Talento Humano	Elisa Rodriguez	DCPtalento1
Talento Humano	Geraldine Castro	DCPtalento2
Asistente Contable	Leidy Angulo	DCPcontable
Tesorería	Carmen Micolta	DCPtesoreria
Facturación	Luz Dary Moran	DCPfacturacion
Sistemas	Geiler Suarez	Lenovo sistemas
Sistemas	Jhoan Acosta	Jhoan Acosta
Video Conferencia	Geiler Suarez	Video Conferencia
Mercadeo	Practicante	DCPmercadeo
Área Scanner	Practicante	Scanner

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	14 de 16


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

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO CR-P-12	FECHA EMISION DD - MM - AA 17-07-2015	VERSION 3	PAGINA 15 de 16

- 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.

XVI.

XVII. RADIOS DE COMUNICACIÓN, TABLETS Y CELULARES

IDENTIFICACION Y UBICACIÓN

XVIII. MANTENIMIENTO Y REPOSICION DE EQUIPOS

ITEM	TIPO EQUIPO	ID	UBICACION	USUARIO	TIEMPO DE MANTENIMIENTO
1.1	PC MESA	MJ01KSBW	ADMON	David Colorado	3 MESES
1.2	PC MESA	MJ01KSBQ	ADMON	Carmen Micolta	3 MESES
1.3	PC MESA	MJ01KSC7	ADMON	Luz Moran	3 MESES
1.5	PC MESA	MJ01KSC8	ADMON	Gloria corrales	3 MESES
1.5	PC MESA	S1H00Q5E	ADMON	Area Talento	3 MESES
1.6	PC MESA	S1H00Q25	ADMON	Cruz Ramirez	3 MESES
1.7	PC MESA	S1H00PY1	ADMON	Sistemas	3 MESES
1.8	PC MESA	S1H00Q2V	ADMON	Ruth Palacios	3 MESES
1.9	PC PORTATIL	YB06207065	ADMON	Carlos Mosquera	3 MESES
1.10	PC PORTATIL	YB06302344	ADMON	Monica Motato	3 MESES
1.11	PC MESA	MJ01BFLK	ADMON	Sistemas	3 MESES

PROCEDIMIENTO PARA SEGURIDAD INFORMATICA

CODIGO
**FECHA EMISION
DD - MM - AA**
VERSION
PAGINA

CR-P-12

17-07-2015

3

16 de 16

1.12	PC MESA	VS130361C3	ADMON	Angela Otero	3 MESES
1.13	PC MESA	S1ATL69	ADMON	Aprencdices	3 MESES
1.14	PC MESA	CS00776098	ADMON	Diego Guzman	3 MESES
1.15	PC PORTATIL	VS70184378	ADMON	Geiler Suarez	3 MESES
1.16	PC PORTATIL	CB29300769	ADMON	Jhoan Acosta	3 MESES
1.17	PC MESA	VS81211159	ADMON	Leidy Angulo	3 MESES
1.18	PC MESA	VS81226706	ADMON	Yovanny Viveros	3 MESES
1.19	PC MESA	CS00776243	ADMON	Elisa Rodriguez	3 MESES
1.20	PC MESA	MJ01BFLK	ADMON	Geiler Suarez	3 MESES
1.21	PC-SERVIDOR	2M213804MD	ADMON	Sistemas	3 MESES
1.22	PC-SERVIDOR	2M213804NM	ADMON	Sistemas	3 MESES
1.23	PC-SERVIDOR	SC1430	ADMON	Sistemas	3 MESES
SOCIEDAD PORTUARIA					
1.24	PC MESA	MJ01KSBU	SPRBUN	Supervisores	3 MESES
1.25	PC MESA	S1AH00PZS	SPRBUN	Apoyo Supervisor	3 MESES
1.26	PC MESA	S1AH00Q2G	SPRBUN	Elly Hurtado	3 MESES
1.27	PC MESA	MXL131KDL	SPRBUN	Digitadores	3 MESES
1.28	PC MESA	3157C2S	SPRBUN	Capturados satlock	3 MESES
SEDE TCBUN					
1.29	PC PORTATIL	1320LA	TCBUN	Alex Posada	3 meses
1.30	PC MESA	S1H00Q4D	TCBUN	Capturadoras	3 MESES

PROCEDIMIENTO PARA SEGURIDAD INFORMATICA

CODIGO
**FECHA EMISION
DD - MM - AA**
VERSION
PAGINA

CR-P-12

17-07-2015

3

17 de 16

1.31	PC MESA	S1H00Q0C	TCBUEN	Inhouese Ripley	3 MESES
1.32	PC MESA	5485J7S	TCBUEN	Pilar Gomez	3 MESES
1.33	PC PORTATIL	LR4RF2K	TCBUEN	Aprendiz Siso	3 MESES
1.34	TABLETA ELCTRONICA	3FSYA06405	TCBUEN	CAPTURADORES EN BODEGA	5 MESES
1.35	TABLETA ELCTRONICA	3FSYA06407	TCBUEN	CAPTURADORES EN BODEGA	5 MESES
1.36	TABLETA ELCTRONICA	3FSYA06406	TCBUEN	CAPTURADORES EN BODEGA	5 MESES
1.37	TABLETA ELCTRONICA	3FSYA06408	TCBUEN	CAPTURADORES EN BODEGA	5 MESES
PATIO-DATACONTROL					
1.38	PC MESA	MJ01KSBY	PATIO-DATA	Cindy Grueso	3 MESES
1.39	PC PORTATIL	QB05380752	PATIO-DATA	Digitador Gii	3 MESES
1.40	PC MESA	S1AT693	PATIO-DATA	Ronald Azcarate	3 MESES
1.41	PC MESA	S1H00Q11	PATIO-DATA	Jarlin Panameño	3 MESES
1.42	PC MESA	4CE4020PLH	PATIO-DATA	Apoyo Super	3 MESES
1.43	PC PORTATIL	JVHFFC1	PATIO-DATA	Luis Tello	3 MESES
1.44	PC MESA	MJGWXT3	PATIO-DATA	Supervisores Patio	3 MESES
1.45	PC MESA	BTWW244	PATIO-DATA	Bascula	3 MESES
1.46	PC MESA	MJHBYG2	PATIO-DATA	Capturadores	3 MESES
1.47	PC MESA	S1H00Q23	PATIO-DATA	Jairo arboleda	3 MESES
1.48	PC MESA	S1H00Q3D	PATIO-DATA	Melba Orozco	3 MESES

PROCEDIMIENTO PARA SEGURIDAD INFORMATICA

CODIGO
**FECHA EMISION
DD - MM - AA**
VERSION
PAGINA

CR-P-12

17-07-2015

3

18 de 16

1.49	PC MESA	JMVMECB	PATIO-DATA	Jaime Guzman	3 MESES
1.50	PC MESA	4CI4300JPJ	PATIO-DATA	Hector Saenz	3 MESES
RADIOS PORTATILES					
2.1	RADIO	B3207495	TCBUEN	OPERACIONES	5 MESES
2.2	RADIO	B3800491	TCBUEN	OPERACIONES	5 MESES
2.3	RADIO	B3802313	TCBUEN	OPERACIONES	5 MESES
2.4	RADIO	9070324	TCBUEN	OPERACIONES	5 MESES
2.5	RADIO	80500670	TCBUEN	OPERACIONES	5 MESES
2.6	RADIO	342	TCBUEN	OPERACIONES	5 MESES
2.7	RADIO	351	TCBUEN	OPERACIONES	5 MESES
2.8	RADIO	213	TCBUEN	OPERACIONES	5 MESES
2.9	RADIO	343	TCBUEN	OPERACIONES	5 MESES
2.10	RADIO	B3403671	PATIO-DATA	OPERACIONES	5 MESES
2.11	RADIO	B3207541	PATIO-DATA	OPERACIONES	5 MESES
2.12	RADIO	71202166	PATIO-DATA	OPERACIONES	5 MESES
2..13	RADIO	B3802312	PATIO-DATA	OPERACIONES	5 MESES
2.14	RADIO	B3800545	PATIO-DATA	OPERACIONES	5 MESES
2.15	RADIO	B3801486	PATIO-DATA	OPERACIONES	5 MESES
2.16	RADIO	B3802332	PATIO-DATA	OPERACIONES	5 MESES
2.17	RADIO	B3802331	MANTTO	OPERACIONES	5 MESES
2.18	RADIO	B3403667	PATIO	OPERACIONES	5 MESES
2.19	RADIO	B3403675	PATIO	OPERACIONES	5 MESES

PROCEDIMIENTO PARA SEGURIDAD INFORMATICA

CODIGO
**FECHA EMISION
DD - MM - AA**
VERSION
PAGINA


CR-P-12

17-07-2015

3

19 de 16

2.20	RADIO	B1502747	PATIO	OPERACIONES	5 MESES
2.21	RADIO	B3800484	SPRBUN	OPERACIONES	5 MESES
2.22	RADIO	B3800544	SPRBUN	OPERACIONES	5 MESES
2.23	RADIO-BASE	80A00252	SPRBUN	OPERACIONES	5 MESES
2.24	RADIO	B0702463	SPRBUN	OPERACIONES	5 MESES
2.25	RADIO	90202131	SPRBUN	OPERACIONES	5 MESES
2.26	RADIO	B1502750	SPRBUN	OPERACIONES	5 MESES
RADIOS BASE					
2.27	BASE		NTU 131(REPARA CION)	OPERACIONES	5 MESES
2.28	BASE	B0400937	NTU 132	OPERACIONES	5 MESES
2.29	BASE	B0400933	NTU 135	OPERACIONES	5 MESES
2.30	BASE	B0400934	NTU 136	OPERACIONES	5 MESES
2.31	BASE	B0400947	NTU 137	OPERACIONES	5 MESES
2.32	BASE	B0400936	NTU 139	OPERACIONES	5 MESES
2.33	BASE	B0400937	NTU 143	OPERACIONES	5 MESES
2.34	BASE	B0400940	NTU 143	OPERACIONES	5 MESES
2.35	BASE	B0400938	NTU 144	OPERACIONES	5 MESES
2.36	BASE	BIC02312	OWI 02	OPERACIONES	5 MESES
2.37	BASE	BIC02318	OWI 03	OPERACIONES	5 MESES
2.38	BASE	BIC02316	OWI 04	OPERACIONES	5 MESES


 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	20 de 16

2.39	BASE	BICO2305	OWI 07	OPERACIONES	5 MESES
2.40	BASE	BICO2303	OWI 09	OPERACIONES	5 MESES
2.41	BASE	BICO2313	OWI 08	OPERACIONES	5 MESES
2.42	BASE	BICO2315	OWI 09	OPERACIONES	5 MESES
2.43	BASE	BICO2314	OWI 10	OPERACIONES	5 MESES
2.44	BASE	BICO2301	OWI 11	OPERACIONES	5 MESES
2.45	BASE	BICO2317	OWI 12	OPERACIONES	5 MESES

XIX FUNCIONES DEL RESPONSABLE DEL SOPORTE DE SISTEMAS

1. INTERNET

- Garantizar el servicio en todas las sedes 24/7
- Verificando físicamente en desplazamiento cada frente los dispositivos existentes (Radios Enlaces, Swiches, Routers, Red y conexión de los puntos de los equipos)
- Configurar y administrar las redes Inalámbricas de acceso a internet en todas las sedes de la organización
- Contacto directo con el proveedor cuando se presentan fallas el por qué, y dar solución
- Garantizar el suministro eléctrico del rack de comunicaciones donde se encuentra el nodo de conexión a internet y la Red
- Estar atento a los posibles problemas eléctricos de conexión de los dispositivos y mantenimiento encargado para los mismos así como las reparaciones por daño.
- Configurar acceso vía Internet al Sistema de CCTV de la empresa creando usuarios y contraseñas


 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	21 de 16

2. EQUIPOS DE CÓMPUTO

- Administrar equipos servidores de CGUNO, GII y Biométricos
- Garantizar la operatividad de los equipos de cómputo existentes en la organización a cualquier horario
- Verificar la configuración en la red
- Mantener inventario de equipos
- Mantenimiento físico de los equipos (Limpieza)
- Mantenimiento lógico de los equipos (evitar y quitar virus software no requerido)
- De acuerdo a directriz asignar equipo a usuarios instalando el software necesario para el desempeño de la labor
- Atender los llamados personalizados de los usuarios
- Procurar y concienciar a los usuarios sobre el uso del recurso
- Instalar en equipo y Red las impresoras de la organización
- Estar pendiente de daños en ellas ocasionados y brindar solución

3. EQUIPOS DE COMUNICACIÓN (radios)

- Estar atento al funcionamiento de la Frecuencia adquirida
- Garantizar y estar al pendiente de la comunicación por este medio
- Estar atento a fallas recibidas y hacer contacto con el proveedor para solucionarlas
- Estar pendiente de los tiempos de mantenimientos
- Verificar estado físico de los mismos para cambio de componentes
- Revisar las facturas recibidas por reparaciones efectuadas y que estas hayan sido realizadas

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	22 de 16

4. EQUIPOS BIOMETRICOS

- Estar atento a la operatividad de las unidades
- Configuración de las mismas en la red
- Descarga de datos desde las unidades
- Grabar nuevo personal en las unidades
- Crear usuarios Administradores según directriz

5. MANEJO DE SOFTWARE FINGERPRINT

Software para control remoto de las Unidades Biométricas en la empresa donde se pueden gestionar las diferentes configuraciones del mismo como direcciones IP en la red , copiado de personal ,

6. MANEJO DE SOFTWARE CONTROL PRESENCIA


Software que permite gestionar y brindar información requerida sobre la llegada del personal permitiendo información precisa, que además se encarga de proporcionar el tiempo extra para el proceso de nomina
Actualización de marcaciones de los usuarios por directriz vía correo de supervisores

7. MANEJO SOFTWARE COSMOS E INTEGRA

Software requerido en las operaciones para el retiro, verificación y gestión de los contenedores en Sociedad portuaria que se encuentra instalado tanto en oficinas propias de data en Sociedad como en los diferentes frentes exceptuando el puerto TCBUEN

8. MANEJO Y CONFIGURACION DE LAS CUENTAS DE CORREO

Crear y eliminar cuentas por directrices recibidas
Gestionar el espacio en servidor para evitar llenado de cuota
Crear listas de re-envíos
Brindar soporte por mal funcionamiento de la cuenta

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	23 de 16

9. MANEJO DE ESPACIO DE ALMACENAMIENTO ICLOUD

Administrar Icloud interno

Crear carpetas personales para usuarios con el fin de hacer copia de seguridad de archivos críticos para cada quien

Crear carpeta general para uso compartido de archivos

10. MANEJO DE SOFTWARE KAS10

Verificar funcionamiento del software de posicionamiento satelital de los RD"S y brindar soporte en caso de falla

11. MANEJO DE SOFTWARE SISCOMBAS (BASCULA)

Instalación de Software de ser requerido

Pendiente a copia de seguridad

12. SOPORTE CCTV


Verificación de funcionamiento de las cámaras y Unidad de grabación DVR

Crear usuarios para acceso al mismo tanto presencial como vía Internet

Coordinar mantenimientos y reparaciones al circuito adiciones y reubicaciones

Descarga de eventos en caso de presentarse

Elaborado por:		Revisado y Aprobado por:
Geiler Suarez	Ángela María Otero	Diego Yepes Gerente General
Soporte de Sistemas	Coordinadora de Desempeño	

 DATACONTROL PORTUARIO S.A.	PROCEDIMIENTO PARA SEGURIDAD INFORMATICA			
	CODIGO	FECHA EMISION DD - MM - AA	VERSION	PAGINA
	CR-P-12	17-07-2015	3	24 de 16

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
2	17/02/2014	Actualización estructura (sale TLBUEN)
3	17/07/2015	Inclusión de funciones de soporte