1. OBJETIVO

Minimizar la probabilidad de ocurrencia de riesgos y vulnerabilidades al esquema de la seguridad informática, con el fin de conservar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Este procedimiento es aplicable a la planeación e implementación de normas y políticas de seguridad hasta el seguimiento y control de los mismos.

3. RESPONSABLES

Coordinador de Sistemas: Es el directo responsable del cumplimiento de los lineamientos establecidos en este procedimiento.
Todo el personal: cumplir las políticas de seguridad establecidas por la empresa.

4. TERMINOS Y DEFINICIONES

Backup: realizar una copia de seriedad o respaldo de la información contenida en un servidor a través de medios electrónicos como CD, DVD, Discos Extraíbles o archivos ubicados en los servidores.

Backup por Demanda: Es el backup solicitado por un área específica, que puede encontrarse en un acuerdo de servicio o un Backup eventual, que no tiene unos parámetros específicos (día, hora), y se debe solicitar a el área de sistemas.

Backup Programado: Es que el backup que debe realizarse periódicamente saber su criticidad y debe tener tiempos de ejecución e información a respaldar, los cuales están previamente definidos.

Restauración de Backup: Es tomar la información del backup solicitado y restablecerla en un servidor, equipo o disco extraíble.

Logs: Son registros de trazabilidad dejados por las diferentes sistemas de información y demás eventos.

Sistemas de información: Inhouse, Forward y SIIGO, sistemas usados para el almacenamiento y procesamiento de la información contable y operativa de la empresa.

Cobian Backup: Marca de la herramienta de software de backup automatizado.

Microsoft ForeFront EndPoint Protection: Marca del antivirus instalado en los equipos de la empresa.

FingerPrint: Sistema de control de acceso con huella digital.

Firewall: Palabra que define la compuerta de seguridad de la infraestructura electrónica.

5. REQUISITOS LEGALES

NTC ISO 9001:2008

NTC ISO 28000:2007

6. PLATAFORMA DE SEGURIDAD

En la actualidad CARGEX cuenta con tres sistemas ISA SERVER, PF SENSE y MICROSOFT FOREFRONT ENDPOINT PROTECTION, que permiten la protección de la red logica y de datos ante posibles eventos como: ataques internos y externos a la red, protección de los servicio web, filtrado de contenido, ataques de intrusos y protección de virus.

7. BACKUPS Y RESTAURACION DE LA INFORMACIÓN.

Los backups se realizan de forma periódica en tareas programadas previamente en la herramienta de backups COBIAN BACKUP definidos en las políticas de Backup.

Dentro de la programación mensual se extraen mensualmente los backup para ser entregados a la Sra. Ángela Torres para ser custodiados. Relacionado en la planilla de entrega de backups.

En caso de que un disco duro extraíble se dañe, se diligencia la planilla de daño de discos, la cual se reporta a la gerencia para hacer la reposición de este y de la información si es necesario.

Después de haber terminado el backup el coordinador de sistemas verifica que el mismo no presente ningún error y que termino en estado completo sin ningún inconveniente.

En caso de ser necesaria la recuperación de la información, la persona debe comunicarse con su jefe inmediato para que este haga la solicitud por correo o personalmente al área de sistemas.

8. COPIAS DE USUARIO FINAL

En todos los computadores conectados a la red de la oficina principal, se encuentra una carpeta en “MI PC” con el nombre del usuario de equipo. Allí los usuario deben guardar los archivos a lo que deseen que se les hagan copias de seguridad. Los cuales se ejecutar los viernes al final del día.

9. ACCESO AL CENTRO DE CÓMPUTO Y SERVIDORES

Para el acceso al centro de cómputo solo las personas autorizadas tienen las llaves para acceder a este cuarto. Las personas que deseen ingresar deben pedir aprobación al área de sistemas y con acompañamiento del coordinador de sistemas.

No se permite el ingreso y/o salida de ninguna clase de elementos, por parte de los visitantes al centro de cómputo sin previa autorización del coordinador de sistemas.

Para horarios no hábiles o por emergencia se permite solicitar autorización a través de llamada telefónica o correos electrónicos al coordinador de sistemas. En este caso debe especificar para que necesite el acceso al centro de cómputo.

10. ANTIVIRUS

CARGEX SAS cuenta con Microsoft ForeFront EndPoint Protection, el cual se actualiza automáticamente y mantiene protegido los equipos.

11. ADQUISICION DE SOFTWARE

Al adquirir software se verifica que los programas estén respaldados por los documentos de licenciamiento o transferencia de propiedad respectivos.

En el evento en que se requiera la titularidad del derecho de autor sobre desarrollo de software, la titularidad de esos derechos consta en el respectivo contrato o funciones a cumplir.

Se lleva un inventario de todos los soportes del licenciamiento adquirido por la entidad.

12. INSTALACION DE SOFTWARE

Dentro de las actividades realizadas en el mantenimiento preventivo, se tiene el levantamiento de información de todos los programas y comparados con las hojas de vida de ellos, para saber que programas licenciados tienen.

En caso de encontrarse software sin licencia o no permitido se procede a su desinstalación de los equipos de cómputo.

En caso de encontrar software libre se pide se explique si se requiere para el cumplimiento de las funciones.

El área de sistemas son los únicos autorizados para instalar software en los equipos de cómputo. Cuando las áreas solicitan software adicional al instalado, se requiere visto bueno del coordinador de sistemas.

13. USO DE MEMORIAS EXTRAIBLES Y QUEMA DE CD

Se tiene restringido el uso de dispositivos de almacenamiento extraíble por puerto USB y quemar discos.

Solo los equipos de los siguientes procesos tienen permisos para el almacenamiento de archivos en discos extraíbles

Gerencia
Director administrativo y financiero
Director comercial perecedero
Directora carga seca
Coordinador SIG y Compra
Jefe de cartera dólares
Jefe operativo perecedero
Asistente Gerencia
Contador

14. DESCRIPCION DE LAS ACTIVIDADES

ITEM	ACTIVIDAD	DESCRIPCION	REGISTRO/DOCUMENTO	RESPONSABLE
1	BACKUP	Realizar copia de seguridad del respaldo de la información.	Planilla de backup.	COORDINADOR DE SISTEMAS
2	BACKUP POR DEMANDA	Realizar copia de seguridad por parte del área solicitante.	Planilla de backup.	COORDINADOR DE SISTEMAS
3	BACKUP PROGRAMADO	Realizar copia de seguridad que tiene un periodo programado de ejecución.	Planilla de backup.	COORDINADOR DE SISTEMAS
4	RESTAURACION DE BACKUP	Se restaura copia de seguridad a petición del área.	Planilla de backup	COORDINADOR DE SISTEMAS
5	INHOUSE	Mantenimiento del sistema y desarrollo de nuevas funciones.		COORDINADOR DE SISTEMAS
6	FORWARD	Control y soporte junto con forward al sistema.		COORDINADOR DE SISTEMAS
7	SIIGO	Soporte y control de planos de facturas.		COORDINADOR DE SISTEMAS
8	COBIAN BACKUP	Creación de eventos para generación de backup y revisión de informe.	Correos enviados por el sistema.	COORDINADOR DE SISTEMAS
9	FINGERPRINT	Manejo y Reporte de ingreso y salida del personal de la empresa.	Reporte de ingreso enviado por correo a RRHH y Gerencia.	COORDINADOR DE SISTEMAS

15. CONTROL DE CAMBIO AL DOCUMENTO

NUMERO	DESCRIPCION DEL CAMBIO	VERSION	FECHA

ELABORADO POR	REVISADO POR	APROBADO POR
COORDINADOR SISTEMAS	DIRECTOR ADMINISTRATIVO Y FINANCIERO	GERENTE GENERAL