PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
No. CONSECUTIVO 2
Actualizado el 16/01/2018

REALIZÓ	**REVISÓ**	**APROBÓ**
ING GIOVANNA DEL PILAR OLAYA RODRIGUEZ/ ACTUALIZADO POR: JOHANNA ACOSTA PEÑA	ING GIOVANNA DEL PILAR OLAYA RODRIGUEZ/ ACTUALIZADO POR: JOHANNA ACOSTA PEÑA	DRA DARLIN LENIS ESPITIA
PROFESIONAL UNIVERSITARIA	PROFESIONAL UNIVERSITARIA	GERENTE

TABLA DE CONTENIDO

INTRODUCCIÓN

Los requerimientos de seguridad que involucran las tecnologías de la Información son de carácter globalizador, llevando a que muchas instituciones desarrollen políticas para el uso adecuado de las tecnologías y recomendaciones para aprovechar los recursos disponibles, evitando se esta manera un uso indebido. Es de gran importancia el desarrollo y evolución de sistemas y políticas que generen seguridad en el manejo, control y gestión de la información de la Corporación Social de Cundinamarca, ya que es su activo más valioso y está definido en la legislación Colombiana.

La Oficina de Sistemas, realiza el manual de seguridad informática orientado en los lineamientos establecidos en el sistema de gestión de calidad, como un instrumento que concientice a los funcionarios, de la importancia y sensibilidad del manejo de la información, del control de los riesgos asociados, la superación de fallas y debilidades relacionadas, de tal forma que permitan a la Corporación cumplir con su misión y visión.

OBJETIVO GENERAL

Buscar el aprovechamiento de los servicios tecnológicos y de comunicaciones brindando confiabilidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso con el fin de asegurar su correcta funcionalidad, ofreciendo un nivel de seguridad óptimo.

DEFINICIONES

AJAX: acrónimo de Asynchronous JavaScript And XML (JavaScript asíncrono y XML), es una técnica de desarrollo web para crear aplicaciones interactivas o RIA (Rich Internet Applications). Estas aplicaciones se ejecutan en el cliente, es decir, en el navegador de los usuarios mientras se mantiene la comunicación asíncrona con el servidor en segundo plano. De esta forma es posible realizar cambios sobre las páginas sin necesidad de recargarlas, mejorando la interactividad, velocidad y usabilidad en las aplicaciones.

Base de datos SQL: (por sus siglas en inglés Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar, de forma sencilla, información de bases de datos, así como hacer cambios en ellas.

Bitvise: Es un cliente para administrar y modificar código fuente en programas web.

Copia de seguridad: Una copia de seguridad, copia de respaldo o backup (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales.

DATADOC: Software desarrollado para el control, la administración y la gestión documental de una entidad.

Direccionamiento IP: Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP).

Directorio Activo: Es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red. Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de

datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

Firewall – Trunk: Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. La opción "trunk" – "baúl" canaliza ciertas amenazas a un sitio seguro para después ser analizadas.

Firewall Fortinet: Es un producto que ofrece soluciones de servicios a nivel de seguridad informática con mecanismos de software y hardware. Solución adquirida por la Corporación Social de Cundinamarca.

ISOLUCION: Compañía de tecnología relacionada con el diseño, desarrollo, implementación y soporte de soluciones tecnológicas para los sistemas integrados de gestión y los sistemas de gestión de la Calidad, basados en modelos normativos ISO y sus complementarios.

Lenguaje PHP: Es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. Fue uno de los primeros lenguajes de programación del lado del servidor que se podían incorporar directamente en el documento HTML en lugar de llamar a un archivo externo que procese los datos. El código es interpretado por un servidor web con un módulo de procesador de PHP que genera la página Web resultante. Puede ser usado en la mayoría de los servidores web al igual que en casi todos los sistemas operativos y plataformas. PHP se considera uno de los lenguajes más flexibles, potentes y de alto rendimiento conocidos hasta el día de hoy.

LITISOFT: Es un sistema que controla los procesos judiciales, desde la presentación de la demanda hasta la terminación del proceso judicial. Tiene parametrizados todos los tipos de proceso y sus respectivos trámites por cada jurisdicción: civil, administrativa, penal, laboral y constitucional. Está compuesto por los módulos de: Información jurídica y financiera, control de términos y módulo de reportes.

Modo batch: Se conoce como sistema por lotes (en inglés batch processing), o modo batch, a la ejecución de un programa sin el control o supervisión directa del usuario (que se denomina procesamiento interactivo). Este tipo de programas se caracterizan porque su ejecución no precisa ningún tipo de interacción con el usuario.

Permisos SQL server: Asignar por parte de un administrador de la base de datos, derechos de acceso o restricción a las opciones o información contenida en las tablas de almacenamiento, administración y estructura de los datos contenidos en los servidores de información de la Organización.

Segmento DMZ: Llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.
Segmentos de red: Es un conjunto de equipos (computadoras y periféricos) conectados en red. Una red de una organización puede estar compuesta por varios segmentos de red conectados a la LAN principal llamada backbone, que existe para comunicar los segmentos entre sí.

Servidor DHCP: (siglas en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de host») es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Los servidores DHCP administran de forma centralizada direcciones IP e información relacionada y la ofrecen a los clientes automáticamente. Esto permite configurar la red de cliente en un servidor en lugar de hacerlo en cada equipo cliente.

Servidor DNS: Domain Name System o DNS (en español «Sistema de Nombres de Dominio») es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Servidor NTP: Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable. Una solución completa para sincronizar redes de gran tamaño. El servidor de hora combina un reloj de radio basado en GPS con un ordenador de estado sólido Linux incorporado y ofrece una configuración y administración sencillas a través de una interfaz de navegador.

Sistema Operativo Linux: Es un sistema operativo, una gran pieza de software que controla un computador. Es parecido a Microsoft Windows, pero completamente libre. El nombre correcto es GNU/Linux pero "Linux" se usa más. Linux no es el producto de una sola compañía, es el resultado de la contribución de un gran número de compañías y grupos de personas. De hecho, el sistema GNU/Linux es un componente central, el cual se transforma en muchos productos diferentes: las llamadas distribuciones.

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación. Se considera que el software es el equipamiento lógico e intangible de un ordenador. En otras palabras, el concepto de software abarca a todas las aplicaciones informáticas, como los procesadores de textos, las planillas de cálculo y los editores de imágenes.
SQL Server Management Studio (SSMS): Es una aplicación de software de Microsoft que se utiliza para configurar, gestionar y administrar todos los componentes dentro de Microsoft SQL Server. La herramienta incluye tanto los editores de scripts y herramientas de gráficos que trabajan con objetos y características del servidor. Una característica central de SSMS es el explorador de objetos, lo que permite al usuario navegar, seleccionar y actuar sobre alguno de los objetos dentro del servidor.

Switch: Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta. Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).

Tiempo real: Un sistema en tiempo real (STR) es aquel sistema digital que interactúa activamente con un entorno con dinámica conocida en relación con sus entradas, salidas y restricciones temporales, para darle un correcto funcionamiento de acuerdo con los conceptos de predictibilidad, estabilidad, controlabilidad y alcanzabilidad. La palabra tiempo significa que el correcto funcionamiento de un sistema depende no sólo del resultado lógico que devuelve la computadora, también depende del tiempo en que se produce ese resultado. La palabra real quiere decir que la reacción de un sistema a eventos externos debe ocurrir durante su evolución. Como una consecuencia, el tiempo del sistema (tiempo interno) debe ser medido usando la misma escala con que se mide el tiempo del ambiente controlado (tiempo externo).

Topología de red: Se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma. En algunos casos, se puede usar la palabra arquitectura en un sentido relajado para hablar a la vez de la disposición física del cableado y de cómo el protocolo considera dicho cableado. Así, en un anillo con un concentrador (unidad de acceso a múltiples estaciones, MAU) podemos decir que tenemos una topología en anillo, o de que se trata de un anillo con topología en estrella. La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

Usuarios de dominio: Es una cuenta compuesta por nombre y contraseña con el fin de acceder a los diferentes servicios de un servidor o grupo de servidores, redes, carpetas, archivos, información y recursos compartidos para compartir, editar o transferir la gestión digital de la Organización. La cuenta de un usuario del dominio registra toda la información necesaria para su definición, los grupos a los que pertenece el usuario, los derechos y permisos que tiene el usuario para utilizar el equipo y la red, así como para tener acceso a sus recursos. En los controladores de dominio de Windows Server, las cuentas de usuario se administran con usuarios y equipos de Active Directory.

VLAN: Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4). Una VLAN consiste en dos o más redes de computadoras que se comportan como si

estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.

ZIMBRA: La suite de colaboración Zimbra (en inglés Zimbra Collaboration Suite o ZCS) es un programa informático colaborativo o Groupware que consta de un servicio de correo electrónico creado por Zimbra Inc. compañía ubicada en San Mateo, California. Posee tanto el componente de servidor como su respectivo cliente.

1. ACCESOS, USUARIOS Y CONTRASEÑAS

4.1 USUARIO DE DOMINIO

Los funcionarios de la Corporación Social de Cundinamarca poseen un usuario de dominio, creado en el directorio activo, que les da acceso al ordenador y sus recursos, en donde se clasifica a diferentes privilegios y permisos.

4.1.1 INICIAR SESIÓN EN EL DOMINIO CON EQUIPOS QUE EJECUTAN WINDOWS 7 Ó XP

1. Cierre la sesión del equipo o reinicie el equipo.
2. Presione Ctrl + Alt + Supr. Aparecerá la pantalla de inicio de sesión.
3. Haga clic en **Cambiar de usuario** y, a continuación, haga clic en **Otro usuario**.
4. En **Nombre de usuario**, escriba su dominio y nombre de usuario con el formato *dominio\usuario*. Por ejemplo, para iniciar sesión en el dominio de corsocun.gov con una cuenta llamada **Usuario-01**, escriba **corsocun\Usuario-01**.
5. En **Contraseña**, escriba la contraseña de su dominio y, a continuación, haga clic en la flecha o presione Entrar.

4.2 USUARIO DE NOVASOFT:

El ingreso al Sistema Integrado NOVASOFT ENTERPRISE , está soportado en el módulo de seguridad, para ingresar es necesario contar con un nombre de usuario y una clave, esta identificación será suministrada por el administrador del sistema.

4.2.1 IDENTIFICACIÓN DE INGRESO

Al ingresar al Sistema Integrado NOVASOFT ENTERPRISE, aparece una pantalla de autenticación SQL en donde se debe digitar el nombre y clave del usuario, luego debe hacer clic en el botón de Entrar; el sistema autenticará la información suministrada y permitirá el ingreso o el cambio de la clave si el usuario lo desea:

Sí, seleccionó la opción de Cambiar clave, se mostrara una ventana que le solicitara la nueva clave y la confirmación de la clave, luego haga clic en el botón Aceptar, el sistema validara que estos datos concuerdan y de ser así mostrara un mensaje que le indica que el cambio fue realizado.

Sí no quiere continuar puede cancelar haciendo clic en Salir.

4.3 USUARIO DE LITISOFT:

Litisoft es un Software de información jurídica que controla los procesos judiciales, desde la presentación de la demanda hasta la terminación del proceso judicial.

El ingreso Litisoft , previa creación por parte del administrador, se realizará por la url: http://aplicaciones:8095/ de la siguiente forma:

Para ingresar nombre de usuario, clave y luego hacer clic en el botón ingresar o si lo desea: seleccionar la opción de Cambiar clave, en donde se mostrara una ventana que le solicitara la nueva clave y la confirmación de la clave, luego haga clic en el botón "aceptar", el sistema validara que estos datos concuerdan y de ser así mostrara un mensaje que le indica que el cambio fue realizado.

4.1 USUARIO DE DATADOC:

DataDoc es un software de gestión documental en donde se consulta información por medio de metadatos, Automatiza tareas relacionadas con distribución y clasificación de documentos, permite la llegada de la información a las personas autorizadas y responsables de los documentos.

El ingreso Datadoc , previa creación por parte del administrador, se realizará por la url http://10.168.20.114:80/ de la siguiente forma:

Para ingresar se debe digitar nombre de usuario, clave y luego digitar la tecla Entrar.

4.1 USUARIO DE ISOLUCION:

Isolucion es un software para la administración del Sistema de Gestión de Calidad, herramienta que facilita la definición, automatización y la implementación de los modelos normativos complementarios.

El ingreso Isolucion, previa creación por parte del administrador, se realizará por la url:
http://10.168.20.11:81/isolucion/ de la siguiente forma:

Para ingresar se debe digitar nombre de usuario, clave y luego clic en el botón Iniciar Sesión.

4.1 USUARIO DE ZIMBRA:

Zimbra es el correo institucional de tipo cliente/servidor de correo y calendario. El ingreso al correo Zimbra por parte de los empleados de la CSC, previa creación por parte del administrador, se realizará por la url: https://correo.csc.gov.co/#1 o https://192.168.20.251/ de la siguiente forma:

Para ingresar se debe digitar nombre de usuario, contraseña y luego clic en el botón Iniciar Sesión.

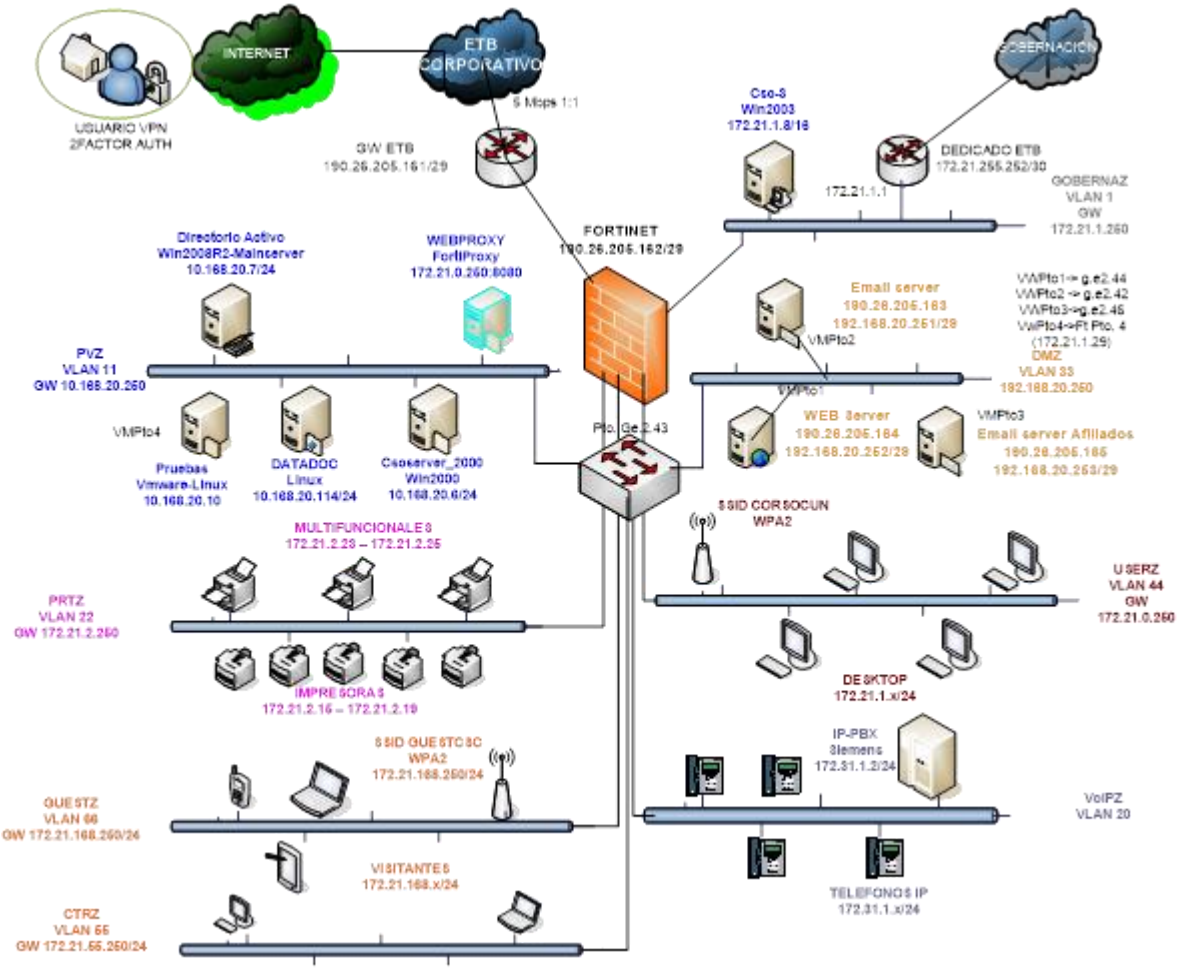
Este correo ya no se cuenta activo pero se deja nombrado ya que allí hay información de los diferentes usuarios de la csc que realizaron uso de él, en la actualidad el correo que s3e maneja es autlook echain o por via web el cal es administrador directamente por la oficina de TIC de la Gobernación de Cundinamarca

2. INFRAESTRUCTURA

2.1. TOPOLOGÍA DE RED

La topología de red de la Corporación Social de Cundinamarca corresponde a una red segmentada en 8 VLAN en dónde cada una está diseñada para conectar dispositivos para un servicio específico y el tráfico entre los segmentos es independiente a nivel de capa 2 y se controla mediante el Firewall en capa 3.

Diagrama general de red:



La corporación cuenta con una distribución de 90 puntos de red aproximadamente los cuales parten desde el centro de cómputo ubicado en el tercer piso y se extienden a través de las cuatro plantas del mismo. Estos puntos cuentan con un estándar certificado de categoría 6E (1 Gbps) y cumplen el protocolo Power Over Ethernet (IEE802.3af-2003) en toda su extensión. Todos estos derivan desde dos switch capa 3 **Enterasys B5G124-48P2**, que están dispuestos en el rack de comunicaciones, y esta a su vez alimenta eléctricamente los teléfonos IP de la corporación.

1.1. SEGMENTOS DE RED:

DESCRIPCION	NOMBRE	VLAN	IP	GW
Servidores internos	PVZ	11	10.168.20.0/24	10.168.20.250
Servidores públicos	DMZ	33	192.168.20.248/29	192.168.20.250
Red de impresoras	PRTZ	22	172.21.2.0/24	172.21.2.250
Red de usuarios	USERZ	44	172.21.0.0/24	172.21.0.250
Red de telefonía	VoIPZ	20	172.31.1.0/24	172.31.1.1
Red de Invitados Wireless	GUESTZ	66	172.21.168.0/24	172.21.168.250
Red cámaras	VDZ	55	172.21.3.248/29	172.21.3.250
Red anterior	Default	1	172.21.1.0/24	172.21.1.1

Dada esta segmentación, algunos equipos tienen la siguiente descripción de red fija:

HOST	IP
Mainserver	10.168.20.7
CSC-3	172.21.1.8
Datadoc	10.168.20.114
Aplicaciones	10.168.20.11
Audio línea	172.21.1.12
DVR CSC	172.21.3.251
VMWare ESXi	10.168.20.10
Correo afiliados	192.168.20.253
Correo corporativo	192.168.20.251
Portal transaccional	192.168.20.252
CSCServer2000 (Inactivo)	10.168.20.6
Multifuncional Créditos	172.21.2.23
Multifuncional Pre-jurídica	172.21.2.22
Multifuncional Sub-Admin	172.21.2.24
Impresora código de Barras	172.21.2.25
Impresora Jurídica	172.21.2.15
Impresora Sub-Admin	172.21.2.16
Impresora Sub-Corporativa	172.21.2.17
Impresora Bienestar	172.21.2.18
Impresora Tesorería	172.21.2.19
Reloj HandPunch	172.21.1.200
Consola telefónica Siemens	172.31.1.2
Administración Switch	172.21.1.11
Administración Switch	172.31.1.1

1.1. DIRECCIONAMIENTO IP:

SERVIDOR	IP
Mainserver	10.168.20.7
Datadoc	10.168.20.114
Cscserver_2000	10.168.20.6
Pruebas	10.168.20.10

IMPRESORA	IP
Multifuncional Créditos	172.21.2.23
Multifuncional Prejuridica	172.21.2.22
Multifuncional Subgerencia Admin	172.21.2.24
Impresora Código de Barras	172.21.2.25
Impresora Desgloses	172.21.2.18
Impresora Jurídica	172.21.2.15
Impresora Subgerencia Admin	172.21.2.16
Impresora Subgerencia Corporativa	172.21.2.17
Impresora Tesorería	172.21.2.19

Existe un ámbito en el servidor de DHCP de la red que contiene la ip de las estaciones de usuario con los siguientes parámetros:

Conjunto de direcciones	172.21.0.1 - 172.21.0.100
Enrutador	172.21.0.250
Servidor DNS	10.168.0.7
Nombre de dominio DNS	corsocun.gov
Servidores NTP	10.168.20.7

Direccionamiento de los servidores públicos en el segmento DMZ

SERVIDOR	IP Privada	IP Pública
Email Server Corporativo	192.168.20.251	190.26.205.163
Web Server (Aplicaciones)	192.168.20.252	190.26.205.164
Email Server Afiliados	192.168.20.253	190.26.205.165

1.1. INTERNET:

La Corporación cuenta con un canal de Internet con el proveedor de servicios ETB a través del cual se brinda la conexión a la red pública con los siguientes parámetros

Router ETB	190.26.205.161/29
IP Públicas asignadas	190.26.205.162 190.26.205.163 190.26.205.164 190.26.205.165
DNS público	200.75.51.132 200.75.51.133

1.2. SWITCH:

Las VLAN están asociadas a los puertos de conexión de los diferentes dispositivos de acuerdo al segmento:

DISPOSITIVO	PUERTO	VLAN
Mainserver	Ge.1.3	11
Datadoc	Ge.2.12	11
Cscserver_2000	Ge.1.45	11
Pruebas	Ge.2.7	11
Multifuncional Créditos	Ge.2.40	22
Multifuncional Prejuridica	Ge.2.3	22
Multifuncional Subgerencia Admin	Ge.1.39	22
Impresora Código de Barras	Ge.2.3	22
Impresora Desgloses	Ge.2.18	22
Impresora Jurídica	Ge.2.33	22
Impresora Subgerencia Admin	Ge.1.39	22
Impresora Subgerencia Corporativa	Ge.1.12	22
Impresora Tesorería	Ge.2.9	22
Firewall - Trunk	Ge.2.43	11,22,33,44,55

3. SERVIDORES

La Corporación Social de Cundinamarca cuenta con 7 servidores físicos:

- ✓ PROLIANT DL360e G8 (Portal Web)
- ✓ PROLIANT DL380 G3 (Servidor Histórico)
- ✓ PROLIANT DL380 G5 (Terminal Server)
- ✓ PROLIANT DL380 G7 (MainServer)
- ✓ PROLIANT ML 310e G8 (Aplicaciones)
- ✓ PROLIANT ML110 G6 (Datadoc)
- ✓ PROLIANT ML110 G6 (Audio-línea)

CANTIDAD	DESCRIPCION DE LOS EQUIPOS
1	SERVIDOR COMPAQ PROLIANT DL 380-G2
1	UNIDAD STORAGE CON 7 HDDD
1	SERVIDOR HP PROLIANT DL380 G5
1	SERVIDOR HP PROLIANT DL380 G7
1	UNIDAD STORAGE
1	SERVIDOR HP DATADOC
1	SERVIDOR HP APLICACIONES

3 Servidores Virtualizados con VMWare ESXi para los servicios de correo corporativo, correo afiliados y portal. Instalado en un servidor **HP PROLIANT DL 360G8**

3.1. FIREWALL FORTINET

A nivel de red, el **Firewall Fortinet F200B** permite la administración lógica de las anteriores plataformas, por lo que físicamente tiene conectados a sus interfaces algunos de los dispositivos. Esta dispuesto en el rack de comunicaciones como se muestra en la imagen.

1: Troncal Fa/01 SW1
7: Gobernación WAN (1.5 Mbps)
10: Internet Corporativo (5Mbps)
11: Troncal Fa/43 SW2

4. PÁGINA WEB Y PORTAL TRANSACCIONAL

La Corporación Social de Cundinamarca tiene su nube página web con los parámetros dados de la matriz de gobierno en línea:

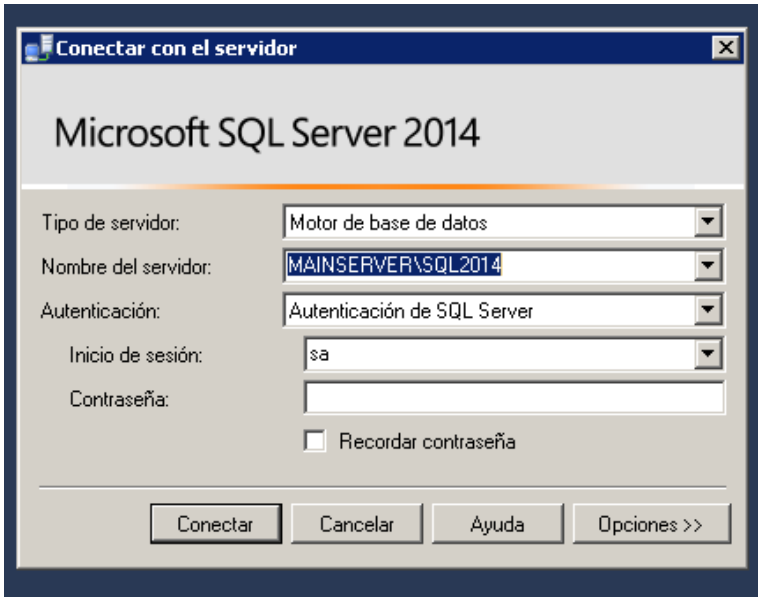
Es un sitio web que ofrece al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios. Incluye: Portal transaccional, información Institucional de la Corporación, publicaciones y noticias, créditos, información de trámites, normatividad, etc.

El rediseño de la página web de la entidad está diseñada en wordpress y alojada en un hostin propio de la Corporación Social de Cundinamarca, la pagina web de la entidad fue rediseñada por los parámetros dados de la matriz de gobierno en línea, la cual indica que todas las entidades del estado tienen que estar alineadas con los 7 componentes en especial el de transparencia donde debe ir todo el contenido de las entidades, adicional a esto se realizó la vinculación de botón de pagos PSE el cual le permite a nuestros afiliados realizar el pago de sus obligación por este medio.

Este rediseño de la página web de la CSC ha permitido que sea más amigable hacia el cliente interno y externo, lo cual le permite estar al día con la información que tiene la entidad para sus afiliados y el público en general.

5. BASES DE DATOS

5.1. ADMINISTRACIÓN SQL:



El Motor de base de datos Microsoft SQL Server es un sistema de administración y análisis de bases de datos relacionales para la línea de negocio de la Corporación Social de Cundinamarca con almacenamiento de datos que alimenta por el aplicativo Novasoft. Unificando el explorador de la utilidad y los puntos de vista de la utilidad en SQL Server Management Studio (SSMS)

Novasoft trabaja directamente con la Base de Datos, en la máquina donde se encuentra instalado Microsoft SQL 2014, o en una máquina que tenga acceso a través de la red o al Motor de Microsoft SQL 2014. La base de datos va con un grupo (función, roll) llamado Novasoft por defecto, el cual tiene privilegios sobre todos los componentes de la base de datos. Se debe crear un "Login" o inicio de sesión que pertenezca al grupo Novasoft, para poder ejecutar la aplicación. La base de datos y la aplicación se adecuan a los parámetros por defecto de configuración para los servidores de base de datos.

5.2 COPIAS DE SEGURIDAD DE LA BASE DE DATOS

Se manejan tareas programadas para realizar las copias de la Base de Datos al medio día y a la media noche en dos archivos diferentes, estas copias se realizan en el disco duro del Servidor y luego son extraídas a un DVD.

5.3 PERMISOS

Las aplicaciones Novasoft basan su seguridad en los permisos que se asignan a los componentes de la base de datos por el SQL Server, adicionalmente, Novasoft Enterprise administra la asignación de permisos en cada una

de las aplicaciones y por cada uno de sus módulos a: archivos, documentos, procesos especiales, reportes, y estructuras. Mantiene un proceso de auditoría sobre todos los eventos que suceden dentro de la aplicación.

Estos permisos se asignarán para cada función o rol definido previamente en la base de datos.

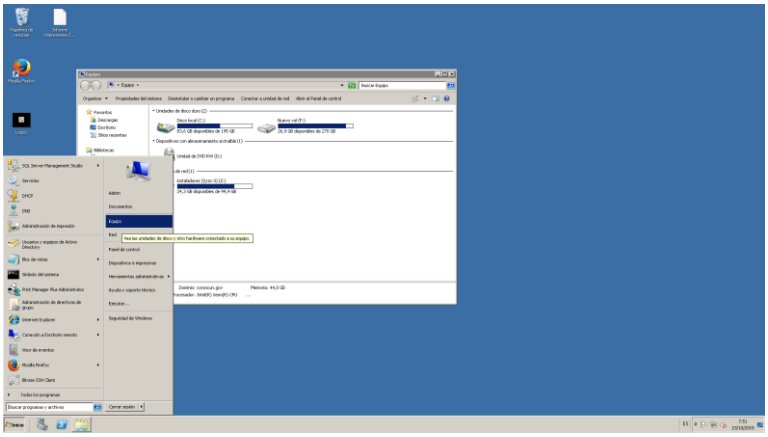
6 COPIAS DE SEGURIDAD

Copiando los datos originales y trasladándolos a una ubicación en otra máquina, se puede disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante los siguientes eventos:

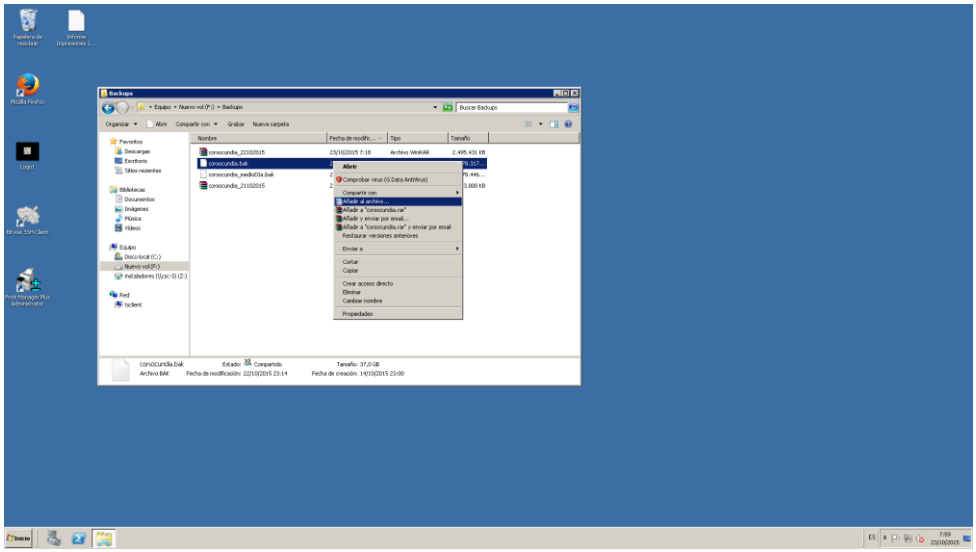
- Recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque
- Restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas.
- Guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales.

6.1 PROCESO

En la actualizad se realiza copia de seguridad de la base de datos de Novasoft, que con anteriormente se programó por SLQ directamente desde el servidor llamado Mainserver ubicado en la VLAN 11 Puerto: Ge.1.3 máquina: PROLIANT DL380 G7 Dirección IP: 10.168.20.7 De la siguiente manera:



Inicio_equipo_disco F_ Backups_ se elije la base de datos que se va a copiar así:



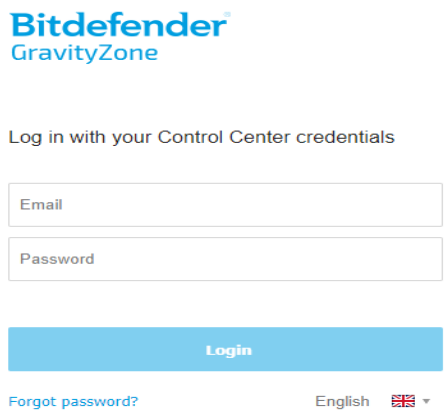
Comprimiéndola para de esta forma poder exportarla a una unidad externa de almacenamiento, se guarda con la fecha cómo nombre para identificación, usualmente un DVD, del cual se realizan dos copias, posterior a esto se hace entrega de una de ellas a la subgerencia Administrativa para ser enviada a la sede atención al cliente de la Gobernación y que alli permanecerá custodiado en una caja fuerte y la otra copia de seguridad reposa en las instalaciones de la CSC.

7 ANTIVIRUS

El antivirus es un programa que ayuda a proteger los computadores contra la mayoría de los virus, worms, troyanos y otros invasores indeseados que puedan infectar un ordenador.

Entre los principales daños que pueden causar estos programas están: la pérdida de rendimiento del microprocesador, borrado de archivos, alteración de datos, información confidencial expuesta a personas no autorizadas y la desinstalación del sistema operativo.

La consola administradora del antivirus Bitefender enpoint secutity tool Administrador se encuentra ubicada en el en la nube en la siguiente ruta https://gravityzone.bitdefender.com/ este antivirus se adquirió en marzo del 2017 con un periodo de duración de 3 años



Bitefender proporciona protección antivirus de gama alta para la red. Mediante este antivirus se protegen todas las máquinas pertenecientes a la red, Bitefender enpoint secutity tool basado en configuración centra. Todos los clientes se controlan de forma centralizada. Asignada en la nube , controla dispositivos de almacenamiento externo, aplicaciones no seguras, contenido web e internet.

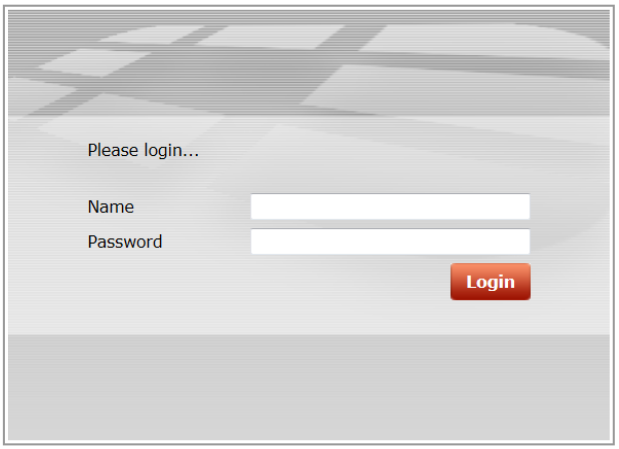
8. FIREWALL

Un firewall es software y hardware, siendo una configuración y máquina que comprueba la información procedente de Internet y de la red y luego procede a bloquear o permitir el paso de ésta al equipo.

Un firewall puede ayudar a impedir que hackers o software malintencionado obtengan acceso al equipo a través de una red o de Internet. Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos.

La Corporación Social de Cundinamarca usa una consola Fortinet cómo soluciones de seguridad de firewall y provee: VPN, antivirus, prevención de intrusión (IPS), control de aplicaciones, filtro web, antispam, etc. **Fortinet** complementa sus soluciones con un conjunto de servicios compuestos de gestión, análisis, correo electrónico, bases de datos y productos de seguridad de punto final.

Se accede por direccionamiento IP: 172.21.0.250 a la consola administrativa así: https://172.21.0.250/



En donde se debe realizar autenticación con Token "Fortitoken" administrativo. Cómo un segundo control de seguridad

REFERENCIAS

- ✓ Seguridad en la información ISO/IEC 27001
- ✓ Estatuto de propiedad intelectual de la Universidad del Atlántico
- ✓ Ley 527 de 1999 - Por medio de la cual se define y reglamenta el acceso y uso de los
- ✓ mensajes de datos, del comercio electrónico y de las firmas digitales.
- ✓ Ley *1273 de 2009* - "De la Protección de la información y de los datos"
- ✓ www.redeszone.net/seguridad-informatica/
- ✓ https://msdn.microsoft.com/es-es/library/ff929050(v=sql.10).aspx

- ✓ https://technet.microsoft.com/es-es/library/ee210548(v=sql.105).aspx
- ✓ http://ayudaenterprise.novasoft.com.co/