PLAN DE SEGURIDAD Y CONTINGENCIA

COMITÉ DE GOBIERNO EN LÍNEA Y DE INFORMÁTICA

Febrero de 2018

Todos controlamos!

Gobernación del Huila Piso 5. Teléfonos 8713304 – Fax 8713114
www.contraloriahuila.gov.co – E-mail: info@contraloriahuila.gov.co

PLAN DE CONTINGENCIA PROPUESTO PARA EL 2018

OBJETIVO

Formular un adecuado Plan de Contingencia, que permita la continuidad de los procedimientos informáticos, así como enfrentarse a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna.

ESTABLECIMIENTO DEL PLAN DE ACCIÓN

Con base en lo anterior, se debe definir cuáles son los activos a proteger, cómo clasificar la información, cuáles datos son públicos, qué información es privada o sensible, quiénes deben/pueden acceder, quién tiene la responsabilidad de definir qué información es crítica, sensible y definir sus accesos. Por ello, es necesario tener en cuenta los siguientes aspectos:

I. CARACTERIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN

La Contraloría Departamental cuenta con una infraestructura informática conformada por:

REDES

1) RED DE CABLEADO ESTRUCTURADO EN EL 5º. PISO DEL EDIFICIO DE LA GOBERNACIÓN DEL HUILA:

- Red Voz y Datos: El centro de cableado está ubicado en el piso 5, en cuarto técnico dispuesto para este fin. Salidas Lógicas de Voz: 56. Salidas Lógicas de Datos: 58.
- Bandeja para manejo de fibra óptica, que está conectando este centro de cableado principal con el centro de cableado ubicado en piso 6.
- 2 Switches 3Com de 48 puertos.
- Patch Panels (3) de 24 puertos para el manejo de las salidas para datos en donde se conectaron 58 puestos de trabajo.
- Patch Panels (3) de 24 puertos para el manejo de las salidas para Voz en donde se conectaron 56 puestos de trabajo.
- Patch Panel categoría 6e de 24 puertos en donde se conectó el multipar de 25 pares que se tendió entre el strip telefónico de piso y el centro de cableado.
- Patch Panel categoría 6e de 24 puertos que se entrega para que a él lleguen las extensiones telefónicas provenientes de la planta telefónica de la Entidad.

2) RED DE CABLEADO ESTRUCTURADO EN EL 6º PISO DEL EDIFICIO DE GOBERNACIÓN – OFICINAS Y AUDITORIO:

- Para equipos correspondientes a las oficinas ubicadas en el 6º piso conformado por un Rack de comunicaciones cerrado de 1.5 mts., cableado estructurado cat 6, cableado estructurado cat 6 para voz, datos y puntos telefónicos, switche de 24 puntos.

EQUIPOS

La Contraloría Departamental del Huila tiene los siguientes equipos:

DESCRIPCION	CANT	TIPO
Servidores	5	4 Servidores – 1 Work Station,
Unidad de Almacenamiento	1	NAS
Computadores	48	Escritorio
Computadores	27	Portátiles
Impresoras	9	Inyección de Tinta (2); Térmicas (3); Fotocopiadoras (4)
Escáner	9	4 de cama Plana, 1 vertical, 4 portátiles
Bancos de Energía	2	UPS de 10 Kva.
Discos Duros	6	Externos
Video Proyector	2	Epson Stylus
Video Cámaras	2	SONY
Cámara Digital	2	Nikon y Canon
GPS	2	Garmany
Planta Telefónica	1	Panasonic KX-TE
Fax	1	Panasonic
Firewall	1	ForteGate 80E

SISTEMAS DE INFORMACIÓN

La Contraloría cuenta con un total de 317 licencias y aplicativos, entre ellos sistemas operativos para servidores, pc de escritorio y portátiles, software ofimática, aplicativos comerciales y aplicativos entorno web desarrollados para el ejercicio del control fiscal, tal como a continuación se describe:

CANTIDAD	NOMBRE O UTILIDAD DEL PROGRAMA	No. DE CONTRATO Y /O FACTURA DE COMPRA	CONTRATISTA	OFICINA
1	MODULO DE PRESUPUESTO CONTABILIDAD, TESORERÍA Y NOMINA.	CONTRATO DE MAYO DE 2001. SE HA VENIDO ACTUALIZANDO ANUALMENTE	SINFA. VALOR $10.000.000. ULTIMA ACTUALIZACIÓN CONTRATO No. 007 DE 2017 POR VALOR DE $7.211.800	ADMINISTRATIVA Y FINANCIERA
50	CALL DE WINDOWS SERVER 2003	FACTURA Nos. 1425 A 1427 DE TENOMUSIC - CONTRATO 016 DE DICIEMBRE 18 DE 2007	TECNOMUSIC. VALOR $2.869.760	EQUIPOS DE LA CONTRALORIA
1	MODULO ADMINISTRACIÓN DE DOCUMENTOS	LICENCIA 2007-45623399 DE SYSMAN . CONTRATO 028 DE 2007. SE HA VENIDO ACTUALIZANDO ANUALMENTE	SYSMAN LTDA. VALOR $16.240.000. ULTIMA ACTUALIZACIÓN CONTRATO No. 014 DE 2017 POR VALOR DE $4.770.000.	ADMINISTRATIVA Y FINANCIERA
1	APLICATIVO WEB PARA EL CARGUE DE FORMATOS DE RENDICION DE CUENTAS EN LINEA PARA LOS SUJETOS DE CONTROL.	SYMDE LTDA. CONTRATO No. 018 DE MAYO-19 DE 2008.	SYMDE LTDA. VALOR $10.400.000	USUARIOS TECNOLOGIA
1	WINDOWS SERVER 2003	FACTURA Nos. 1425 A 1427 DE TENOMUSIC - CONTRATO 016 DE DICIEMBRE 18 DE 2008	TECNOMUSIC	EQUIPOS DE LA CONTRALORIA
75	SISTEMA OPERATIVO WINDOWS	VARIOS	VARIOS	USUARIOS TECNOLOGIA
1	LICENCIA WINDOWS SERVER STD. 2008 R2. PARA EL SERVIDOR HP DL 380G7, CODIGO No. 820	FACTURA No.25540 DE 2011, CONTRATO No. 014 de 2011. valor $2.800.000	TECNOMUSIC	USUARIOS TECNOLOGIA
1	LICENCIA FORTINET	Factura No. 9727 de Diciembre 22 de 2016. All Computer. Contrato No. 029 de 2016	ALL COMPUTER	USUARIOS TECNOLOGIA
1	LICENCIA DE ORACLE POR PROCESADOR	CONVENIO INTERADMINISTRATIVO 0096 DE 2011	DEPARTAMENTO DEL HUILA - SECRETARIA GENERAL	USUARIOS TECNOLOGIA
1	LICENCIA DE SUSE LINUX ENTERPRISE	CONVENIO INTERADMINISTRATIVO 0096 DE 2011	DEPARTAMENTO DEL HUILA - SECRETARIA GENERAL	USUARIOS TECNOLOGIA
1	LICENCIA DE WINDOWS WEB EDTION	CONVENIO INTERADMINISTRATIVO 0096 DE 2011	DEPARTAMENTO DEL HUILA - SECRETARIA GENERAL	USUARIOS TECNOLOGIA
75	LICENCIAS ANTIVIRUS ESET ENDPOINT	ADQUIRIDO DESDE EL AÑO 2012.	SE HA VENIDO RENOVANDO ANUALMENTE. LA ULTIMA MEDIANTE CONTRATO No. 037 DE 2017 CON CONTROLES EMPRESARIALES.	USUARIOS TECNOLOGIA
5	LICENCIAS CALL DE ESCRITORIO REMOTO	ADQUIRIDO MEDIANTE FACTURA No.0046489 DE CONTROLES EMPRESARIALES DE NOV.27 DE 2012. Y CONTRATO NO. 032 DE 2012. VALOR $660.000.	CONTROLES EMPRESARIALES	USUARIOS TECNOLOGIA
48	LICENCIA OFFICE. PROP PLUS 365 SUSCRIPCION A UN AÑO	ADQUIRIDO MEDIANTE FACTURA No.0046489 DE CONTROLES EMPRESARIALES DE NOV.27 DE 2012. Y CONTRATO NO. 032 DE 2012.	SE HA VENIDO REVONANDO ANUALMENTE. LA ULTIMA MEDIANTE CONTRATO 037 DE 2017 CON CONTROLES EMPRESARIALES.	USUARIOS TECNOLOGIA
50	CALL DE WINDOWS SERVER 2008 O 12	CONTRATO No. 018 DE 19 DE JUNIO DE 2014, POR VALOR DE $3.850.000	CONTROLES EMPRESARIALES	USUARIOS TECNOLOGIA
1	LICENCIA GOOGLE EARTH PRO V. 7.1	CONTRATO No. 018 DE 19 DE JUNIO DE 2014, POR VALOR DE $1.218.000	CONTROLES EMPRESARIALES	OFICINA DE CONTROL FISCAL - MEDIO AMBIENTE
1	LICENCIA ADOBE PREMIER PRO CC. PARA WORK STATION	CONTRATO No. 030 DE OCTUBRE 21 DE 2015 Y FACTURA No. 62639 DE NOVIEMBRE 11 DE 2015. VALOR $1.277.586	CONTROLES EMPRESARIALES	RESPONSABILIDAD FISCAL. (WORK STATION)
1	LICENCIA NERO PLATINUM 2015	CONTRATO No. 030 DE OCTUBRE 21 DE 2015 Y FACTURA No. 62639 DE NOVIEMBRE 11 DE 2015. VALOR; $401.724	CONTROLES EMPRESARIALES	RESPONSABILIDAD FISCAL. (WORK STATION)
1	LICENCIA AUTODESK AUTOCAD	CONTRATO No. 039 DE DICIEMBRE 1o. DE 2015 Y FACTURA No. 63118 DE DICIEMBRE 17 DE 2015. VALOR; $11.240.0000	CONTROLES EMPRESARIALES	OFICINA DE CONTROL FISCAL - MEDIO AMBIENTE
1	LICENCIA AUTODESK AUTOCAD COMERCIAL SUSCRIPCIÓN A UN AÑO	CONTRATO No. 039 DE DICIEMBRE 1o. DE 2015 Y FACTURA No. 63118 DE DICIEMBRE 17 DE 2015. VALOR: $1.640.000	CONTROLES EMPRESARIALES	OFICINA DE CONTROL FISCAL - MEDIO AMBIENTE
317	TOTAL			

II. IDENTIFICACION DE RIESGOS O AMENAZAS

El análisis de riesgos supone el hecho de calcular la posibilidad que ocurran cosas negativas; imaginarse lo que puede ir mal, tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma, se priorizarán los problemas y su costo potencial desarrollando un plan de acción adecuado:

SEGURIDAD FISICA

- Al agua, que puede dañar los equipos y archivos.
- Al fuego, que puede destruir los equipos y archivos.
- A un robo común, llevándose los equipos y archivos
- Al vandalismo, que dañen los equipos y archivos.
- A terremotos, que destruyen el equipo y los archivos.
- A daños por cortos en el fluido eléctrico.

SEGURIDAD LOGICA

- A equivocaciones, que dañen los archivos.
- A la acción de virus, que dañen los equipos y archivos.
- A fallas en los equipos, que dañen los archivos.
- Al robo de datos, difundiéndose los datos sin cobrarlos.
- Al fraude, desviando fondos merced a la computadora.
- A accesos no autorizados, filtrándose datos no autorizados

Luego de elaborar esta lista, se evalúan los efectos que estos riesgos tendrán sobre la Plataforma Tecnológica de la Contraloría Departamental del Huila:

¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados?

Al agua, que puede dañar los equipos y archivos.

- ¿Se cuenta con protección para la filtración de aguas de un piso a otro?
- ¿Se realiza mantenimiento y revisión a las tuberías de agua?
- ¿Se toman las medidas necesarias al momento de realizar alguna reparación a las mismas?

Al fuego, que puede destruir los equipos y los archivos

- ¿La Institución cuenta con protección contra incendios?
- ¿Diversos extintores?
- ¿Detectores de humo?

- ¿Los empleados están preparados para enfrentar un posible incendio?

A un robo común, llevándose los equipos y archivos

- ¿Hay personal de seguridad en la Institución?
- ¿Cuántos vigilantes hay?
- Robo común, se cierran las puertas de entrada y ventanas
- ¿Los vigilantes, están ubicados en zonas estratégicas?
- Al vandalismo, que dañen los equipos y archivos
- ¿Existe la posibilidad que algún individuo cause daños intencionados?

A fallas en los equipos, que dañen los archivos

- ¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?
- ¿Cuáles son las condiciones actuales del hardware?
- ¿Es posible predecir las fallas a que están expuestos los equipos?

A terremotos, que destruyen los equipos y archivos

- ¿La Institución se encuentra en una zona sísmica?
- ¿Se encuentran asegurados los equipos?
- ¿El edificio cumple con las normas antisísmicas?
- Un terremoto, ¿cuánto daño podría causar?
- Vandalismo, se cierra la puerta de entrada.

A equivocaciones que dañen los archivos

- ¿Cuánto saben los empleados de computadoras o redes?
- Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?
- Durante el tiempo de vacaciones de los empleados.
- ¿Qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

A la acción de virus, que dañen los archivos

- ¿Está permitido el uso de memorias USB en las oficinas?
- ¿Todas las máquinas tienen unidades para puerto USB?
- ¿Se cuentan con procedimientos contra los virus?

A accesos no autorizados, filtrándose datos importantes

- ¿Qué probabilidad hay que un competidor intente hacer un acceso no autorizado?

Al robo de datos; difundiéndose los datos.

- ¿Cuánto valor tienen actualmente las bases de datos?
- ¿Cuánta pérdida podría causar en caso de que se hicieran públicas?

III. EVALUACIÓN DEL ESTADO ACTUAL DE SEGURIDAD DE LA CONTRALORIA DEPARTAMENTAL DEL HUILA

SEGURIDAD FISICA: La Contraloría Departamental se encuentra ubicada en el Edificio de la Gobernación del Huila, su entorno cuenta con la seguridad física apropiada; aislada de otras edificaciones en los alrededores, cuenta con la seguridad de celaduría y Policía Nacional que realizan las actividades de vigilancia y control del personal que ingresa y sale, como del que retira equipos de cómputo u otros bienes del edificio, exigiendo autorizaciones de retiro de cualquier máquina.

Este registro se lleva a través de un libro radicador en la portería de la Gobernación, habiéndose diseñado un formato para que el Jefe de Oficina del órgano de control autorice la salida de elementos de la entidad (Ver Anexo 1).

Una de las principales amenazas para la Contraloría Departamental del Huila son las inundaciones, ya que por tratarse de una edificación antigua con tubería muy deteriorada, presenta fugas de agua y rotura de tubos que ocasionan inundaciones que provienen desde el 6º piso de la Gobernación. Este problema viene siendo tratado por la Gobernación del Huila, encargada del mantenimiento de la planta física del edificio.

Para solucionar este problema se solicitó directamente al Señor Gobernador efectuándose el respectivo mantenimiento a las tuberías; no obstante persisten las fallas de goteras e inundaciones provenientes de la casa privada del Señor Gobernador..

SEGURIDAD LOGICA: Se lleva a cabo a través de administración de usuarios mediante claves de acceso a los servicios tecnológicos, con parámetros específicos como longitud mínima de las contraseñas, las cuales se ha fijado en 6 caracteres, frecuencia de cambio de contraseña y los períodos de vigencia de las mismas, entre otras.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos tienen roles predefinidos que precisan las acciones permitidas por cada uno de estos.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos, con la siguiente estructura: nombre.apellido.

Todos los equipos tienen definidos los perfiles de usuario de acuerdo con la función y cargo de las personas que acceden a él.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tiene controles de acceso y es sometida a procesos de respaldo para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los Jefes de Oficina, en conjunto con la Oficina Asesora de Planeación, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño hasta la conversión a un sistema en producción.

SEGURIDAD EN COMUNICACIONES. Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, son consideradas y tratadas como información confidencial.

Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la Entidad, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de ciframiento y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

SEGURIDAD PARA USUARIOS TERCEROS. Los dueños de los recursos tecnológicos e informáticos que no son propiedad de la Contraloría Departamental del Huila y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento.

Los usuarios terceros tendrán acceso a los Servicios y Recursos Tecnológicos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el Jefe inmediato o coordinador del proyecto. En todo caso, deberán firmar el acuerdo de buen uso de los Recursos Informáticos. y/o certificado de confidencialidad para el manejo de la información.

SOFTWARE UTILIZADO. Todo software utilizado por la Contraloría Departamental del Huila es adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Existe un inventario de las licencias de software de la Contraloría Departamental del Huila que permite su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

La Entidad cuenta con otras herramientas, tales como las licencias antivirus y el Firewall con lo cual se minimizan los ataques informáticos. Igualmente, existe un software de filtración de contenidos, que restringe el acceso a algunas páginas de internet.

SERVICIO DE MANTENIMIENTO DE SOFTWARE: Los sistemas de información requieren de mantenimiento y actualizaciones realizadas por sus propietarios de tal manera que aseguren la continuidad de las operaciones evitando el deterioro y riesgo de no desempeñarse de acuerdo a los estándares establecidos, consistente en soporte técnico y actualización de nuevas versiones para optimizar la funcionalidad. Por ello, la entidad anualmente contrata los servicios de mantenimiento o actualización de los Aplicativos SINFA – Sistema de Administración Contable, Financiero y Nomina; al igual que SYSMAN; para la administración de documentos.

Lineamientos para el Mantenimiento de Hardware y Software: Presentar la solicitud de requerimiento de contratación del servicio de mantenimiento Preventivo y Correctivo de la plataforma tecnológica de la entidad.

Presentar el programa anual de mantenimiento preventivo y correctivo de equipos, teniendo en cuenta la evaluación del inventario, para determinar el número de equipos de cómputo, el número de aplicativos y/o el cubrimiento de garantías. Una vez realizado el trámite contractual, coordinar con los contratistas la prestación del servicio, estableciendo cronograma de actividades.

Atender permanentemente los reportes por fallas en los equipos informáticos y coordinar con los contratistas la prestación del servicio, de acuerdo con el F06-F03 Reporte de Mantenimiento.

La firma contratista del servicio de mantenimiento de hardware asignará un técnico para atender el requerimiento señalado en el reporte, quien evaluará la falla, emitiendo un diagnóstico y reparará el equipo, debiendo el usuario demostrar su conformidad, diligenciando para ello el Formato F06-F03 Reporte de Mantenimiento.

Será responsabilidad del servidor público encargado de tecnología supervisar e informar a la Dirección la inadecuada prestación del servicio de mantenimiento preventivo o correctivo o por parte del contratista.

Lineamientos Plan de Seguridad - Elaboración de Backup

El propósito es garantizar la custodia de las bases de datos de los aplicativos que se manejan en la Entidad, indispensables para la reinstalación ante cualquier calamidad, así como también de toda la información que se maneja, en consideración a que ésta es uno de los activos más valiosos de la entidad.

Medios y Datos que se deben preparar

Se disponen de cuatro (4) discos externos de 1 Tb distribuidos en la Oficina Asesora de Planeación y Oficina de Control Fiscal, para el procedimiento de copias de seguridad.

Backup a Sistemas Operativos: Se debe contar con una copia de cada uno de los tipos de Windows instalados en la plataforma tecnológica de la entidad.

Backup a las Bases de Datos: El profesional encargado del manejo de la plataforma tecnológica estará a cargo de la realización de copias de seguridad a las bases de datos de los diferentes aplicativos que se llevan en la entidad y que se encuentran instalados en el servidor de aplicativos. Para ello, de manera mensual ingresará con su clave de acceso y efectuará las respectivas copias, conservándolas en discos externos.

Backup a la Información de los Usuarios: La realización de copias de seguridad estará a cargo de cada usuario, en coordinación con el profesional encargado de tecnología, a través del servidor de copias de seguridad, donde a cada usuario del dominio contraloría.local le ha sido entregado previamente la conexión a una unidad de red, de tal manera que en cada equipo existe una carpeta correspondiente a copia de seguridad, en la que se pueden realizar los Backus necesarios y las veces que se considere conveniente; no obstante, el profesional encargado de tecnología revisará semestralmente que se haya efectuado el backup correspondiente a cada semestre; y efectuará una copia en medio magnético, la cual será debidamente rotulada y conservada en el gabinete designado para ello.

Este procedimiento debe ser realizado con periodicidad de seis meses, o cuando se requiera por necesidad del servicio, ya sea que el usuario sea reemplazado en el cargo por otro, o por fallas de los mismos equipos. De todas formas, el encargado de tecnología deberá coordinar y estar pendiente del backup de esta información.: En el caso de no encontrar respuesta positiva con algún usuario sobre el cumplimiento de la copia semestral se registrará este incumplimiento a través del Formato F06-F05 Reporte de Incumplimiento Copias de Seguridad.

Backup de Hardware: El profesional encargado de tecnología tendrá identificados los equipos que podrán ser utilizados como equipos de emergencia o de respaldo.

Resultados Esperados: La información de respaldo se encontrará disponible para ser usada en cualquier momento que se presente la falla y/o contingencia, y ante cualquier evento la recuperación rápida a partir del último Backup que se encuentra en el servidor y en las copias en medio magnético conservadas en el gabinete especial que se halla debidamente rotulada con el nombre del usuario y fecha correspondiente. En el caso de bases de datos de los aplicativos, el restablecimiento de la información, se efectuará en coordinación con los propietarios de los aplicativos.

Aseguramiento de Equipos: Como parte de la protección de los activos institucionales, anualmente se contrata el seguro contra todo riesgo para la plataforma tecnológica de la entidad.

CONFORMACIÓN DE EQUIPOS DE CONTINGENCIA

Con el fin de ejercer permanentemente control y reglamentación a los procesos informáticos, la Contraloría Departamental del Huila mediante Resolución No. 0537 de diciembre 12 de 2013 creó el Comité de Gobierno en Línea y de Informática, integrado por los siguientes:

- Contralor Departamental - Líder del Comité GEL-T.
- Jefe de la Oficina Administrativa y Financiera
- Jefe de la Oficina Asesora de Planeación
- Jefe de la Oficina de Participación Ciudadana
- Funcionario responsable de Sistemas y/o Tecnología

Dicho Comité, además de estar obligado a llevar a cabo la implementación de la Estrategia de Gobierno en Línea, tiene asignado las siguientes funciones:

- Apoyar y asesorar a la Contraloría, en la adquisición de tecnologías de software y hardware para el apoyo a la infraestructura de la entidad.

- Recomendar políticas de alcance general que permitan el manejo consistente e integral de la información para el funcionamiento de los procesos administrativos, facilitando a su vez la toma de decisiones.

- Recomendar políticas y estrategias para el fomento del uso de nuevas tecnologías de informática y telecomunicaciones en el ejercicio del control fiscal.

- Aprobar el Plan Anual de Desarrollo Tecnológico y Plan Anual de Seguridad y Contingencia de la Entidad elaborado por el área de sistemas.

- Aprobar la Evaluación a los Planes de Desarrollo Tecnológico y de Seguridad y Contingencia al finalizar cada vigencia.

- Elaborar y gestionar el presupuesto anual necesario para el desarrollo de los planes trazados.

El órgano de control cuenta con el Comité de Salud Ocupacional, conformado por los Jefes de las Oficinas Administrativa y Financiera; Planeación y Talento Humano; cuya función primordial es velar por la seguridad de los funcionarios de la Contraloría Departamental e informar la existencia de cualquier factor de riesgo y sugerir las medidas de control.

IV. POLITICAS DE SEGURIDAD Y CONTINGENCIA PARA LA VIGENCIA

POLITICA 1: ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas y pasantes que laboran para la Contraloría Departamental del Huila deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la Contraloría Departamental del Huila, el Contralor y Jefes de Oficina, deben autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

Para que un funcionario público, contratista o pasante tenga acceso a los servicios y recursos tecnológicos dispuestos por la Contraloría Departamental del Huila, se requiere que el Contralor y/o Jefes de Oficina soliciten a la Oficina Asesora de Planeación mediante un oficio, la activación de dichos servicios con el perfil requerido y las restricciones de algunos servicios.

Cada vez que se recibe un computador de escritorio o portátil para darle acceso a los servicios tecnológicos que brinda la entidad a los usuarios, es necesario, requerido y obligatorio entregar el equipo con todos los servicios instalados, configurados y en operación. Esto es, verificación y última actualización de parches de seguridad del sistema operativo, instalación del último Services pack del sistema operativo, instalación del último antivirus utilizado por la entidad, instalación y configuración del mensajero interno, configuración del servicio de red e inclusión en el directorio activo del servidor, verificación e instalación de herramienta para comprimir, verificación e instalación de herramientas para gestionar archivos pdf, verificación e instalación de herramientas para quemar cd y DVD con previa autorización del Jefe de Oficina.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Todos los privilegios para el uso de los sistemas de información de la entidad deben terminar inmediatamente después que el trabajador deja de laborar en la entidad o finaliza su práctica universitaria.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal.

POLITICA 2: ADMINISTRACION DE CAMBIOS

Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios responsables de la información y aprobado formalmente por la Oficina Asesora de Planeación, con el visto bueno del jefe de la Oficina.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

POLITICA 3: SEGURIDAD DE LA INFORMACION

Los funcionarios públicos, contratistas y pasantes de la Contraloría Departamental del Huila son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para proteger y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios públicos, contratistas y pasantes no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica (Anexo 2. Índice de Información Clasificada y Reservada)

Después que el funcionario deja de prestar sus servicios a la Entidad, éste se compromete entregar toda la información respectiva de su trabajo realizado al supervisor o jefe inmediato según sea el caso y avala el recibido de la información. Una vez retirado el funcionario, contratista, y/o pasante de la Contraloría Departamental del Huila debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros. Así mismo, los funcionarios públicos que detecten el mal uso de la información están en la obligación de reportar el hecho al grupo de control interno disciplinario.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

POLITICA 4: SEGURIDAD PARA LOS SERVICIOS TECNOLÓGICOS

El sistema de correo electrónico y servicios tecnológicos prestados por la Contraloría Departamental del Huila debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas y pasantes.

La entidad se reserva el derecho de acceder y develar todos los mensajes recibidos y enviados por medio del correo electrónico en caso de requerirse para ello la entidad podrá realizar las revisiones y/o auditorías respectivas directamente o a través de terceros.

Los funcionarios públicos, contratistas y pasantes no deben utilizar versiones escaneadas de firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmado por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el funcionario, contratista o pasante se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Contraloría Departamental del Huila. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.

Los funcionarios públicos, contratistas y pasantes que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet implantadas por la Dirección.

La Contraloría Departamental del Huila prohíbe el servicio de internet en la plataforma tecnológica a través de otras empresas prestadoras de servicio de internet haciendo uso de dispositivos inalámbricos diferentes al servicio disponible propio; con el fin de minimizar el riesgo a la integridad de la información y la seguridad de los sistemas de información corporativos.

En cualquier momento que un funcionario, contratista o pasante publique un mensaje en un grupo de discusión de internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la entidad.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la Oficina Asesora de Planeación (funcionaria encargada de la administración de la plataforma), no utilizar el computador y desconectarlo de la red.

La Oficina Asesora de Planeación debe proveer material y charlas para recordar regularmente a los funcionarios, contratistas y pasantes acerca de sus obligaciones con respecto a la seguridad de la plataforma y los servicios tecnológicos.

POLITICA 5: SEGURIDAD EN RECURSOS INFORMATICOS

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

Administración de Usuarios: Establece cómo deben ser utilizadas las claves de ingreso a los servicios tecnológicos.

Rol de Usuario: Los controladores de dominio, y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, precisando las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el control de usuarios.

El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario, bien sea controlado y administrado por directorio o una herramienta similar que cumpla con esta tarea.

Las palabras claves o contraseñas de acceso a los servicios tecnológicos, que designen los funcionarios públicos, contratistas y pasantes de la Contraloría Departamental del Huila son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de respaldo para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los Jefes de Oficina, en conjunto con la el funcionario encargado de tecnología, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

POLITICA 6: SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.

Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la entidad, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de ciframiento y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

Los computadores de la Contraloría Departamental del Huila se conectarán de manera directa con computadores de entidades externas, conexiones seguras, previa autorización del área de seguridad informática y/o la Oficina Asesora de Planeación.

POLITICA 7: SEGURIDAD PARA USUARIOS TERCEROS

Los dueños de los Recursos tecnológicos e informáticos que no sean propiedad de la Contraloría Departamental del Huila y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente, debe definir un documento de acuerdo oficial entre las partes.

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de la Contraloría Departamental del Huila para el funcionamiento de recursos que no sean propios de la entidad y

que deban ubicarse en sus instalaciones, los recursos serán administrados por la Oficina Asesora de Planeación del órgano de control.

Los usuarios terceros tendrán acceso a los servicios y recursos tecnológicos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el Jefe inmediato o coordinador.

La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada por la Oficina Asesora de Planeación, con el fin de no comprometer la seguridad de la información interna de la entidad.

Los equipos de usuarios terceros que deban estar conectados a la red, deben cumplir con todas las normas de seguridad informática vigentes en la Entidad.

Como requisito para interconectar la red de la Contraloría Departamental del Huila con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por el ente de control. La entidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La entidad se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la Contraloría Departamental del Huila.

POLITICA 8: SOFTWARE UTILIZADO

Todo software que utilice la Contraloría Departamental del Huila será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la entidad o reglamentos internos.

Todo el software de manejo de datos que utilice la Contraloría Departamental del Huila dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la entidad que garantice el conocimiento por parte de los funcionarios públicos, contratistas y pasantes de las implicaciones que tiene el instalar software ilegal en los computadores de la Contraloría Departamental del Huila.

Existirá un inventario de las licencias de software de la Contraloría Departamental del Huila que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

POLITICA 9: ACTUALIZACIÓN DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la Contraloría Departamental del Huila (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización de la Oficina Asesora de Planeación.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado de la Oficina Asesora de Planeación.

Los equipos tecnológicos instalados en la Plataforma Tecnológica (PC, servidores, LAN, Router, Antenas, etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, Jefe o coordinador de la Oficina Asesora de Planeación

POLITICA 10: ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática de la Contraloría Departamental del Huila deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

La entidad definirá la custodia de los respaldos de la información que se realizará externamente con una compañía especializada en este tema.

El almacenamiento de la información deberá realizarse interna y/o externamente a la Contraloría Departamental del Huila, esto de acuerdo con la importancia de la información para su operación.

Los funcionarios públicos, contratistas y pasantes de un área dueña de la información, serán los responsables de respaldar la información producida por esta área, siguiendo el procedimiento definido por la entidad. La Oficina Asesora de Planeación será la autorizada para realizar el seguimiento y control de esta política.

Anexo 1

AUTORIZACIÓN SALIDA DE COMPUTAODRES PORTÁTILES

Ciudad y Fecha _____

Marca. _____

No. del Equipo _____

No. de Batería: _____

No. del Cargador: _____

Con Mouse: SI _____ NO ____

OBSERVACIONES: _____

_____

_____

QUIEN AUTORIZA LA SALIDA QUIEN RECIBE

Nombre: _____ Nombre: _____

Cargo: _____ Cargo: _____

Firma: _____ Firma: _____

Anexo 2

INDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA

Nombre o título de la Categoría de la Información la Categoría de la información	Nombre o Título de la Información	Idioma	Indice de la Información	Medio de Condervación y Soporte	Fecha de generación de la Información	Nombre del responsable de la producción de la información	Nombre del responsable de la información	Objetivo Legímo de la Excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción total o parcial	Fecha de la calificación	Plazo de la clasificación o reserva
OFICINA ASESORA JURÍDICA													
Proceso Disciplinario	Proceso Disciplinar	Español	Reservada	Físico	Cada vez que se aperture y emita actuaciones procesales	Oficina Asesora Jurídica	Oficina Asesora Jurídica	Amparar derechos fundamentales como el buen nombre, la intimidad	Artículo 95 de la Ley 734 DE 2002	Artículo 209, en concordancia articulo 3º de la Ley 1437 de 2011. Y art. 74 C.N. - derecho	Parcial	Fecha de auto de apertura	Fecha pliego de cargos o archivo definitivo
OFICINADE TALENTO HUMANO													
Historias Laborales	Historias Laborales	Español	Clasificada	Físico	Fecha de vinculación del funcionario	Oficina de Talento Humano	Oficina de Talento Humano	Proteger el Derecho a la intimidad	Artículo 15 Constitución Política de Colombia	Ley 1437 de 2011, Art. 24, Numeral 4	Parcial	Cuando haya autorización del titular o por solicitud judicial o administrativa	Indefinido
Nómina	Nómina	Español	Clasificada	Fisico-Electrónica	Periódica	Oficina de Talento Humano	Oficina de Talento Humano	Proteger el Derecho a la intimidad	Ley Estatutaria 1266 de 2008 Título IV, Ley 1581 de 2012	Ley Estatutaria 1266 de 2008 Título IV, Ley 1581 de 2013	Parcial	Cuando haya autorización del titular o por solicitud judicial o	Indefinido
OFICINADE RESPONSABILIDAD FISCAL													
Expediente de Indagaciones Preliminares	Expediente de Indagaciones Preliminares	Español	Reservada	Físico	Apertura auto de indagación preliminar	Oficina de Responsabilidad Fiscal	Oficina de Responsabilidad Fiscal	Proteger las Garantias Procesales de los Investigados	Articulo 20 de la Ley 610 del 2000	Articulo 20 de la Ley 610 del 2000	Parcial	6 Meses	6 Meses
Procesos de Responsabilidad Fiscal	Procesos de Responsabilidad Fiscal	Español	Reservada	Físico	Fecha de apertura del proceso	Oficina de Responsabilidad Fiscal	Oficina de Responsabilidad Fiscal	Proteger las Garantias Procesales de los Investigados	Articulo 20 de la Ley 610 del 2000	Articulo 20 de la Ley 610 del 2000	Parcial	Fecha del Auto de Imputación	Indefinido
Expediente de Cuaderno de Medidas Cautelares Cautelares	Expediente de Cuaderno de Medidas Cautelares	Español	Reservada	Físico	Fecha de apertura del proceso	Oficina de Responsabilidad Fiscal	Oficina de Responsabilidad Fiscal	Proteger las Garantias Procesales de los Investigados	Articulo 20 de la Ley 610 del 2000	Articulo 20 de la Ley 610 del 2000	Parcial	Fecha del Auto de Imputación	Indefinido
Procesos de Juridicción Coactiva	Procesos de Juridicción Coactiva	Español	Reservada	Físico	Inicia con mandamiento de pago	Oficina de Responsabilidad Fiscal	Oficina de Responsabilidad Fiscal	Proteger las Garantias Procesales de los Investigados	Articulo 20 de la Ley 610 del 2000	Articulo 20 de la Ley 610 del 2000	Parcial	Fecha del Auto de Imputación	Indefinido
Proceso Administrativo Sancionatorio	Proceso Administrativo Sancionatorio	Español	Reservada	Físico	Inicia con el auto de apertura	Oficina de Responsabilidad Fiscal	Oficina de Responsabilidad Fiscal	Proteger las Garantias Procesales de los Investigados	Artículos 15 y 29 de la Constitución Política y principios establecidos en el artículo 3 de la Ley 1437 de 2011	Artículos 15 y 29 de la Constitución Política y principios establecidos en el artículo 3 de la Ley 1437 de 2011	Parcial	Hasta que se profiera el acto administrativo que decida el fondo del hecho investigado	Una vez se notifique el acto administrativo personalmente o por aviso
OFICINADE PARTICIPACIÓN CIUDADANA													
Denuncia	Denuncia	Español	Reservada	Físico	La presentación de la Denuncia	Oficina de Participación Ciudadana	Oficina de Participación Ciudadana	Derecho a la Privacidad y Buen Nombre	Artículo 15 Constitución Política de Colombia	Artículo 15 Constitución Política de Colombia	Parcial	Cuando haya autorización del titular o por solicitud judicial o	Indefinido