Superservicios Superintendencia de Servicios Públicos Domiciliarios	**INFORME DE AUDITORÍA A LOS SISTEMAS DE GESTIÓN**	SIGME

FECHA: 29-30/12/2021				**INFORME No.1**			
SISTEMA DE GESTION							
CALIDAD	x	**SG-SST**	x	**SIGESPI**	x	**AMBIENTAL**	x

PROCESO (S) AUDITADO (S): GESTION TECNOLOGIAS DE LA INFORMACION

AUDITOR LÍDER: William Javier Barrera Tamayo

AUDITORE(S) ACOMPAÑANTE(S): María Alejandra Gaviria Valbuena

OBJETIVO DE LA AUDITORIA:
Verificar el cumplimiento de los requisitos establecidos y aplicables de las normas NTC ISO 9001:2015 (Calidad), NTC ISO 14001:2015 (Ambiental), NTC ISO 27001:2013(Seguridad y Privacidad de la Información) y NTC ISO 45001:2018 y los requisitos legales y reglamentarios aplicables al proceso en la Superintendencia de Servicios Públicos Domiciliarios" En la Superintendencia de Servicios Públicos Domiciliarios.

ALCANCE DE LA AUDITORIA:
Aplica para los servicios de vigilancia, inspección y control de la prestación de los servicios públicos domiciliarios, atendiendo los requisitos de sus partes interesadas en Bogotá D.C. (Sede Principal)

PERSONAL ENTREVISTADO:

Daniel Joaquín Rodríguez	Jefe oficina Gestion TICs
David Mauricio Rodríguez	Asesor
Gina Moreno	Asesor
John Redondo	Profesional especializado
Rocio Villanueva	Profesional especializado
Jazmín Flechas	Profesional especializado
Edward Merchán	Profesional especializado
Daniel Sanmiguel	Profesional especializado

DOCUMENTOS ANALIZADOS (CRITERIOS)
SI-M-001 MANUAL DE LINEAMIENTOS TECNICOS
TI-M-002 MANUAL DE SERVICIOS TECNOLÓGICOS
TI-M-003 ESTRATEGIA DE ADOPCIÓN DEL DOMINIO DE USO Y APROPIACION DE LAS TECNOLOGIAS DE INFORMACIÓN
TI-M-006 MANUAL DE GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE LA INFORMACIÓN
TI-PL-001 PLAN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TI-P-001 PROCEDIMIENTO PLANEACIÓN DE LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
TI-P-002 PROCEDIMIENTO GESTIÓN DE LOS SERVICIOS TECNOLÓGICOS
TI-P-003 PROCEDIMIENTO GESTIÓN DE LA INFORMACIÓN E INTELIGENCIA DE NEGOCIO
TI-P-004 PROCEDIMIENTO GESTIÓN DE LOS SISTEMAS DE INFORMACIÓN
TI-I-002 INSTRUCTIVO USO Y APROPIACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
TI-I-003 GESTIÓN DE REQUERIMIENTOS DE LA SOLUCIÓN INFORMÁTICA
TI-I-004 GESTIÓN DE PRUEBAS DE LA SOLUCIÓN INFORMÁTICA
TI-I-005 INSTRUCTIVO GENERAL DE DESARROLLO DE SOFTWARE
TI-I-006 INSTRUCTIVO DE CAMBIOS DE TONERS
TI-I-007 INSTRUCTIVO_PARA_EL_TRATAMIENTO_DE_ID_DUPLICADOS
TI-I-010 INSTRUCTIVO_HERRAMIENTA DE MONITOREO INFRAESTRUCTURA TECNOLOGICA
TI-I-011 INSTRUCTIVO LINEAMIENTOS PARA EL VERSIONAMIENTO DE APLICACIONES
TI-I-012 INSTRUCTIVO PARA LA GESTIÓN DE LICENCIAS DE SOFTWARE
TI-I-013 INSTRUCTIVO GESTION DE USUARIOS
TI-I-014 INSTRUCTIVO DE VALORACIÓN DE ACTIVOS INTANGIBLES GENERADOS INTERNAMENTE
TI-I-015 INSTRUCTIVO PARA USUARIOS DE BITLOCKER
TI-I-016 INSTRUCTIVO GESTIÓN DEL ACCESO A LAS BASES DE DATOS

ASPECTOS RELEVANTES
4.1 Se identifican los lineamientos inherentes al proceso del análisis del contexto interno y externo y se identifican las partes interesadas y sus requisitos pertinentes, que impactan el cumplimiento de los propósitos misionales, los resultados previstos en el SIGME y la capacidad institucional desde los sistemas de calidad, ambiental, SST y seguridad de la información.
Se establece en el documento DE-F-003 Contexto estratégico institucional, en el cual se identifican los factores y se clasifican de acuerdo al proceso de Tecnologías de la Información.
4.2 Se identifican las partes interesadas para calidad, ambiental, SST y seguridad de la información desde el documento "DF-002 Identificación de partes interesadas" en donde se evidencian como partes directamente relacionadas al proceso como MINTIC, funcionarios y contratistas, entidades de control nacional y distrital como la contraloría
4.3 Se ubica el alcance del sistema alineado con el proceso de Gestion de la información y el conocimiento con respecto a los requisitos de las normas NTC ISO 14001:2015, NTC ISO 45001:2018, NTC ISO/IEC 27001:2013 y NTC ISO 9001:2015. Se ubican el alcance en el Manual del sistema
4.4 Se tiene identificada la descripción del proceso con sus entradas y salidas de calidad, SST, ambiental y seguridad de la

información en el aplicativo SIGME. TI-PR-01. Versión 12
5/ 5.1 Existe compromiso y liderazgo por parte de la Alta Dirección y se determinan las responsabilidades y autoridades para calidad, SST, ambiental y seguridad de la información.
Se establecen las responsabilidades y autoridades desde la “Matriz de Roles, Responsabilidades y autoridades” en el documento “DE-R-004” desde el SGC;
5.2 Se establecen, se conocen y se ubican las políticas para el sistema de gestión de calidad, ambiental, SST y seguridad de la información como también las políticas complementarias al proceso; Estas están establecidas en la página institucional a través del aplicativo SIGME.
5.2.2 Se realiza la validación de saber dónde están ubicadas dentro de las cuales se encuentra la página web en Quienes somos, también indican que de manera física en las instalaciones
5.3 Se establecen los roles y responsabilidades y autoridades para las normas NTC ISO 9001:2015, ISO 14001:2015, ISO 45001:2018 y NTC ISO 27001:2013 (Seguridad y Privacidad de la Información)
Se establecen las responsabilidades y autoridades del personal desde la “Matriz de Roles, Responsabilidades y autoridades” DE-R-004.
Se verifica para
Jazmín Argenis Flechas Muñoz
Rol: Enlace de dependencia
Rol: Profesional de seguridad Informática
5.4 (ISO 45001) Se conoce de la existencia de los comités de Copasst y convivencia, se les comunica a través de correo electrónico y se participa por parte de los funcionarios de la elección de los mismos.
Se los han comunicado también a través del infórmate y comunicaciones de Gestión Humana.
6. Se planifica el sistema de gestión de calidad, ambiental, SST y de seguridad de la información, considerando las cuestiones internas y externas revisadas en el contexto de la entidad a partir de allí se desarrolla una metodología de identificación de riesgos.
6.1 Se desarrolla la metodología de identificación de riesgos teniendo en cuenta:
● Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública V4 de octubre de 2018.
Se identifican los riesgos del proceso
Calidad:
-Obsolescencia de la infraestructura tecnológica
Ambiental:
-Disposición de residuos
-Deterioro de los recursos naturales
SST:
-Químicos, biomecánicos, desastres naturales, biológicos
8.2 (ISO 27001) Seguridad de la información:
-Posibilidad de la afectación de la confidencialidad, integridad y disponibilidad de la información de los datos almacenados en los sistemas de información (capa de aplicación). Por fallas en otorgar accesos a los sistemas de información administrados por la OTIC debido a 1) Dar de alta usuarios sin contar con un Aranda y formato TI-F-034, 2) Dar de alta a un sistema de información no especificado en el formato TI-F-034 3) No dar de baja un usuario en algún sistema de información que ha sido reportado por el formato TI-F-034 4) La OTIC no es informada de que un usuario ya no debe tener acceso a un sistema de información.
-Perdida de confidencialidad, perdida de integrada
6.1.1 Se cuenta con tratamientos para los riesgos identificados en los sistemas de calidad, ambiental, SST y seguridad de la información así:
Calidad:
Obsolescencia de la infraestructura tecnológica
-Tratamiento: Seguimiento trimestral, donde realizan la identificación de la cantidad de elementos de infraestructura y el nivel de obsolescencia.
Posible aumento de siniestralidad en riesgos laborales que afectan la salud y seguridad de los colaboradores
Tratamiento: inspecciones y programa de prevención de los desórdenes musculoesquelesticos.
Ambiental: Disposición de residuos
Tratamiento: Baja de computadores y baterías con el área administrativa para la disposición final.
Deterioro de los recursos naturales
Tratamiento: campañas para el uso adecuado de los recursos
SST: Químicos, biomecánicos, desastres naturales, biológicos
Tratamiento: Uso del tapabocas, lavado de manos, pausas activas,
Seguridad de la información:
-Posibilidad de la afectación de la confidencialidad, integridad y disponibilidad de la información de los datos almacenados en los sistemas de información (capa de aplicación). Por fallas en otorgar accesos a los sistemas de información administrados por la OTIC debido a 1) Dar de alta usuarios sin contar con un Aranda y formato TI-F-034, 2) Dar de alta a un sistema de información no especificado en el formato TI-F-034 3) No dar de baja un usuario en algún sistema de información que ha sido reportado por el formato TI-F-034 4) La OTIC no es informada de que un usuario ya no debe tener acceso a un sistema de información.
Tratamiento: Acceso de usuarios
Tratamiento: Registro y cancelación de usuarios. Se inactivan usuarios que no han utilizado la plataforma por 90 días
Tratamiento: a través de la mesa de ayuda por parte de los supervisores remiten la información de bloqueos de usuarios para contratistas que terminan las actividades.
- PERDIDA DE CONFIDENCIALIDAD, PERDIDA DE INTEGRIDA
Tratamiento: Controles de redes
Tratamiento: Controles contra códigos maliciosos
Tratamiento: Toma de conciencia mínimo una vez al mes realiza divulgación de temas de seguridad de la información
Tratamiento: Tratamiento de datos personales y cláusula de confidencialidad para empleados y contratistas.
6.1.2 (ISO 14001) Se identifican los aspectos ambientales más relevantes para la entidad y se aplica la sensibilización del buen uso de recursos como el agua, energía y residuos.
6.1.2/6.1.3 (ISO 27001) La entidad define y aplica un proceso de valoración de riesgos de la seguridad de la información e

incluye riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información. Se cuenta con los registros de tratamiento a cada uno de los riesgos identificados.
6.1.3 y 6.1.4 (ISO 14001) Se identifican los requisitos legales para identificar los aspectos ambientales, se tiene acceso a los mismos y se toman las acciones teniendo en cuenta los aspectos ambientales significativos y requisitos legales y otros requisitos.
6.2 Para el logro de los objetivos se tiene en cuenta las sensibilizaciones en los documentos aplicables al proceso, capacitaciones y divulgaciones a través de correos institucionales, pagina web, boletines e inducción.
6.3 Se verifica la identificación de las necesidades de cambios para el Sistema de Integrado de Gestión considerando su propósito, consecuencias potenciales, integridad del sistema, disponibilidad de recursos y asignación o reasignación de responsabilidades y autoridades.
Catarsis: Se verifica la aplicación en Adquisición de bienes y servicios en donde se evidencian las aplicaciones de los pasos definidos: empatía, definición, ideación.
Innovación Cerrada: identificación de reto, crear equipos, reconocimientos:
7 /7.1 Se garantizan los recursos para la entidad para mantener sus sistemas de calidad, ambiental, SST y seguridad de la información y se presenta resolución SSPD20211000000045 de 4 de enero de 2021 de Aceptación de presupuesto 2021.
7.1.2 actualmente se tienen 904 empleos (hoja de cálculo que administra el Grupo Administración de Personal).Se cuenta con el personal para la ejecución de las actividades del proceso en los temas de calidad, SST, ambiental y seguridad de la información: El proceso cuenta con personal Contratista, Prestadores y Directivos.
7.1.5/ 7.1.5.1 Se cuenta con las programaciones y realización de pruebas de seguridad, validación y verificación de aplicaciones y software como recursos de seguimiento y medición
7.1.6 Se realizan actividades de conocimiento a través de las rutas de:
Catarsis e Innovación Cerrada para mantener y tener disponible el conocimiento y la innovación de la entidad.
- Instructivos técnicos con paso a paso de las actividades
- Documentar y divulgar la información del proceso
- Rotación de roles
- Instructivo de la gestión de conocimiento.

7.2 Se conoce y se tiene la competencia para el personal integrante de la superintendencia de servicios.
Manual de funciones
Profesional especializado 2028 – 19
Infraestructura
7.3 La toma de conciencia en temas cómo los riesgos, políticas, objetivos integrales se dan a conocer a través de correo electrónico enviado fecha 17/08/2021 sensibilizaciones en temas de riesgos ambientales, de SST del proceso, a través de la inducción en la cual se trabaja con 11 con módulos.
7.4 Para la gestión de divulgación de la información, se cuenta con diferentes canales, entre correos electrónicos y plataformas tecnológicas, bajo la administración de funcionarios y contratistas conforme a los perfiles de acceso relacionados a continuación.
Intranet, correo de comunicación interna, boletín virtual infórmate, carteleras digitales, pagina Web, redes sociales, portal SUI, correos de comunicación externa.
Te resuelve (PQRS)
7.5/ 7.5.1/ 7.5.2/7.5.3 Se crea, actualiza y se controla la información documentada del proceso y requerida por las normas NTC ISO 9001:2015 (Calidad), NTC ISO 14001:2015 (Ambiental), NTC ISO 27001:2013 (Seguridad y Privacidad de la Información) y NTC ISO 45001:2018.
8/ 8.1 Se cuenta con un plan estratégico PETI el cual prioriza las necesidades del proceso.
PRESUPUESTOS:
Se tiene establecido el presupuesto en 3 grandes productos que son
1. Desarrollo y mejoras para el SUI: contratos de adquisición de licenciamiento, perfiles de desarrollo
2. Infraestructura: actualización de redes, servidores, seguridad
3. Planificación estrategia de TI: Estudio de tecnologías, nuevas políticas.

Se tiene planificación de adquisiciones e inversiones del proceso, se tiene el control del mismo y se reporta en SIGME.
Se aporta en el tema de contratación en la alineación de requisitos de desarrollo o de personal.
Contrato de desarrollo: Portales WEB contrato 534, se identifica la necesidad desde el estudio previo para dar cumplimiento de políticas de gobierno digital, se tienen en cuenta los requisitos legales aplicables y los requisitos del manual de requerimientos técnicos, cuenta con acuerdos de nivelo de servicio, análisis de riesgos, Versionamiento, ambientes de trabajo, También se tiene la programación del ambiente de pruebas.
Contrato de personal: Contrato para seguridad de la información contrato 256 de 2021 con informe de febrero de supervisión.
SERVICIOS:
Se cuenta con acuerdo marco de servicios, se programa desde COMSISTELCO, los mantenimientos preventivos, contrato 562 del 2021, el seguimiento se registra en la aplicación de ARANDA SERVICE DESK con cada mantenimiento. Se verifica requerimiento 182925 con su revisión por la entidad de cumplimiento, se cuenta con el formato de mantenimiento de equipos de cómputo TI-F-040 para este equipo con código de identificación número 1PC7-230-17732. El cual significa ubicación, área y placa de identificación inventario.
Se identifica mantenimientos correctivos caso 175789.
Se cuenta con documento línea base de OTIC con el registro de mantenimientos equipos, serial, características, placa entre otros.
Se maneja manuales de equipos para acceder a los mismos, Marca COMPUMAX Línea Corporativo Procesador AMD Ryzen™ 5 2400G con Gráficos Radeon™ RX Vega 11, Caché 4M, 3.60 GHz, 15 Núcleos (4 CPU + 11 GPU), 8 Hilos. Arquitectura de 64 Bits Fecha de lanzamiento Q2-2018 Referencia SATURNO-RZ5-0001 Factor de Forma All in one.
DUVULGACION EN SUI:
Surge de la necesidad de establecer formularios en búsqueda de la recolección de información de los prestadores de servicios.
Evidencia de Solicitud creación de formato: A través de aplicativo “ARANDA” se tramita la solicitud, se crea la tarjeta y se asigna a un ingeniero desarrollador, se somete a pruebas y finalmente se somete a pruebas funcionales para aprobación y aceptación del usuario. Una vez se pone en producción termina el ciclo de desarrollo.

Norma 20161300013835 de 2016 se toma verificación de la creación de" Formulario registro de estaciones de transferencia", se verifica modelo SI-F-014 con las especificaciones sometidas a revisión.
Proyecto Aseo 178142 Suscriptores beneficiarios del incentivo a la separación en la fuente DINC 5/08/202, resolución CRA7120. Acta de revisión de viabilidad 4/06/2021, se realizan las pruebas y en la herramienta MANTIS código DINC 18841, pruebas de aceptación G-DF-063 del 13/09/2021, TI-F-14 suscriptores beneficiarios de DINC.
ESTRATEGIA DE ADOPCIÓN DEL DOMINIO DE USO Y APROPIACION DE LAS TECNOLOGIAS DE INFORMACIÓN
Se desarrolla una estrategia de capacitación y entrenamiento, se parte de la matriz de comunicaciones código MI-R-002. Por ejemplo, noticias de "seguridad de la información y gestión de usuarios" a través de Boletín Infórmate, 15/10/2021 numero 036. Capacitación e tema "SIGME"
8.1.4 (ISO 45001) Se provee la información a través de los TDR, contratos, cartas de inicio como también con los diferentes comunicados de seguimiento o terminación de servicios.
8.1.5 (ISO 45001) El proceso se asegura la conformidad de los procesos, productos y servicios suministrados externamente a través de su participación en el establecimiento de los requisitos de los mismos.
8.1.6 (ISO 45001) Se provee la información a través de los TDR, contratos, cartas de inicio como también con los diferentes comunicados de seguimiento o terminación de servicios.
Se participa en el establecimiento de los controles el cual es ejecutado por el proceso de adquisición de bienes y servicios
8.2.1 Se cumplen los requisitos de capacitación, bienestar, nomina, competencias y salud y seguridad en el trabajo teniendo en cuenta la legislación aplicable y su cumplimiento en la entidad.
8.2 (ISO 14001/45001)
Conocen el plan de emergencia de la sede CIVIS, los brigadistas y conocen los puntos de ubicación.
8.3 (ISO 27001) Se evidencia la protección de la información en correos electrónicos, accesos, manejo de SIGME, solicitud de acceso y retiros de SIGME.
El tele trabajador Lo funcionarios se comprometen al cumplimiento de las políticas complementarias de seguridad y privacidad de la información publicadas en la plataforma SIGME
http://sigmecalidad.superservicios.gov.co/SSPD/Isodoc/contenido.nsf/0/713dd3a984b077bc052582b900595386?OpenDocument, a lo establecido en el Formato GH-F-105 Confidencialidad y tratamiento de datos personales para funcionarios y al uso adecuado del(os) equipo(s) y herramienta(s) proporcionada(s) por la Superservicios para utilizarlas exclusivamente, con fines laborales definidos.
Gestion de acceso: LA Directora de Talento Humano hace las solicitudes de accesos o eliminación de los mismos. Formato TI-F-034 Administración de usuarios.
Claves: Se verifica el establecimiento de contraseñas seguras. Se cambia la contraseña cada 3 meses.
Funciones de Activación de cuentas: Se activan las funciones de doble autenticación en las cuentas o canales que lo permitan.
Abrir: Se abren las plataformas o correo en equipos (computador, tableta, celular, otros) que cuenten con software y buscador de red (Chrome, Firefox, Bing, u otros) actualizados y protegidos contra virus.
Cerrar: Se cierran las sesiones de plataformas y correos cada vez que se finalice la sesión de trabajo. Al dejarla abierta puede ser accedida por un tercero.
No abrir No se abre las plataformas y correos en sitios públicos de internet. En caso de ser necesario ingresar en sitio público, se recomienda utilizar ventana de incognito y asegurarse de cerrar y eliminar la cuenta de acceso al terminar la sesión de trabajo
No digitar: No se digitan las contraseñas en momentos en que puede ser captada por terceros. - Evitar abrir enlaces que parezcan sospechosos.
Revisar: Se revisan los permisos de aplicaciones y eliminar aquellas que no se utilizan. - Al usar WiFi pública tener presente: Utilizar una VPN (red privada virtual) para cifrar la conexión, dar protección a la información y evitar la entrada de intrusos.
Desactivar el WiFi: se Desactiva el WIFI cuando no se esté usando.
Gestión de incidentes de seguridad: Se conoce el procedimiento y el formato de reporte en caso de presentarse un incidente
Gestión ante robo o pérdida de equipos. Se conoce el procedimiento en caso de presentarse un robo de equipo.
Discos duros externos y carpetas en drive: Se dispone de discos duros externos y carpetas de drive para el almacenamiento de los archivos que se producen en desarrollo de las actividades propias de la gestión.
8.4.1 El proceso se asegura la conformidad de los procesos, productos y servicios suministrados externamente a través de su participación en el establecimiento de los requisitos de los mismos.
8.4.2 Se participa en el establecimiento de los controles el cual es ejecutado por el proceso de adquisición de bienes y servicios
8.4.3 Se provee la información a través de los TDR, contratos, cartas de inicio como también con los diferentes comunicados de seguimiento o terminación de servicios.
8.5 Se cuenta con implementación de servicios de Talento Humano bajo condiciones controladas así:
ANEXOS DE CONTROL:
ANEXO A (5 AL 18).
A5: Políticas de seguridad: Se tienen políticas de seguridad de la información y otras políticas aprobadas y revisadas anualmente.
Se evidencia revisión de la política en SIGME EN 2021
A6 Organización de la seguridad de la Información: Se cuenta con matriz de roles y responsabilidades, Oficial de seguridad, profesional de seguridad informática
A partir del decreto 137 se determinan las funciones de tecnologías de la información separando las funciones del oficial de seguridad y profesionales de seguridad.
Se tiene actualizado listado de autoridades de seguridad de la información y se tiene convenios con entidades como policía nacional, defensa civil , ministerio de telecomunicaciones,
Se tiene listado de partes interesadas, proveedores, autoridades nacionales, la CRAFT entre otros
Dentro de direccionamiento estratégico se establece documento para la gestión de proyectos DE-P-001. Gestion de proyectos de inversión.
Se cuenta con política de manejo de dispositivos móviles D-EM-004 5.11 y teletrabajo 5.7 y 5.8 trabajo remoto.
Se tiene formato de control de entrada y salida de equipos móviles GA-F-008, se tiene establecido instructivo GI-C-004
Gestion de incidentes de la seguridad de la información. Fecha 27/10/2021 jefe Daniel Rodríguez

Se tiene acceso a plataformas y aplicaciones de la entidad con claves y doble autenticación.
A7 Seguridad de los Recursos Humanos: Se cuenta con procedimiento de selección de personal, se definen términos y condiciones del empleo y se definen roles y responsabilidades, se cuenta con procedimiento de toma de conciencia, educación y formación en la seguridad de la información y se toman medida de accesos y restricción de los mismos una vez es retirado el personal.
A8 Política de Gestión de Activos: Se cuenta con procedimientos de manejo de activos, en donde se establece inventario, propiedad, clasificación, devolución, etiquetado y manejo.
A9 Control de acceso: Se cuenta con política de la seguridad física 5.1.
Se maneja doble autenticación en sistemas de información mediante asteriscos o puntos negros cuando se digita, a nivel correo se adelanta campaña desde el segundo trimestre del año para utilización de la doble autenticación.
Se maneja a través de los privilegios que se dan al acceso
Se crea caso con documento TI-F-34 Para retiro o ajuste
Se establece en la política 5.9 literal a Dentro de OTIC se maneja repositorio de código fuente svn-suBVERSION y el GIT-GITLAB se solicita usuario y contraseña para acceso a los repositorios y se debe hacer solicitud a través de ARANDA.
A10 Criptografía: Se cuenta con controles criptográficos y política 5.2 certificados generados con vigencia de tres meses.
La protección está con manejo del contratista, los token de un año.
A11 Seguridad física y del entorno: Se identifican las áreas de seguridad y el Perímetro de seguridad física prevenir acceso no autorizado a instalaciones de procesamiento de información. Ingreso biométrico y llave.
OBS: Es conveniente establecer un control de llaves, copias y cambios de las mismas.
Acceso biométrico.
No se utiliza carnet como acceso
Dentro del plan de emergencias, se establece protección de los servidores, utilización de EPP y elementos contra incendios para daños eléctricos. Procedimiento GH-PL-001 Plan de preparación de emergencias
Existe demarcación de la zona de despacho y carga la cual requiere identificación.
Se cuenta con planta de energía y UPS.
Se cuenta con Limpieza y borrado seguro de equipos obsoletos.
Se identifica el equipo a darse de baja por obsolescencia, se entrega a almacén sin información con aplicación de Software DEVIA el cual toma 3 o 4 horas de borrado, con el resultado el técnico toma evidencias y vuelve e inventarios.se tiene caso 780751 equipo placa 150218 del 23/09/2021, caso 180754 equipo placa 14933 del 23/09/2021.
DE-M-004 Política de pantalla limpia y escritorio limpio número 5.3 se evidencia en equipo 21927.
OBS: Es conveniente establecer protocolo de robo de equipos por perdida de equipo mes de enero y no reportado al proceso de Gestion TICs.A12 Seguridad de las operaciones
Se cuenta con los procedimientos de operacionales y responsabilidades actividades de T.I. y de seguridad de la información
Se determinan la Gestion del cambio a través de la aplicación de procedimiento de MI-F-005 Manual de servicios tecnológicos y se utiliza el formatoTI-F-033 Solicitud de cambio RFC. Se verifica cambio 1613 reportado en ARANDA para solución de incidente de seguridad en donde se detalla la serie de actividades. Con cierre 5/11/2021, 8.14 p.m.
S verifica la capacidad para LINUX, WINDOWS, por hiperconvergencia, para proyección de capacidad teniendo en cuenta máquinas, capacidad de procesamiento y a través de herramienta de monitoreo. rvtools_export_all_2021-11-19_14.04.53
Se cuenta con la separación de los ambientes de desarrollo, pruebas y operación establecidos en las especificaciones de los servicios de desarrollo o actualización de aplicaciones y software. Se cuenta con formato SI-F-008 Requerimientos de infraestructura para determinar la capacidad en suministro de infraestructura sujeto a comité de cambios.
Se cuenta con formato SI-F-008 Requerimientos de infraestructura para determinar la capacidad en suministro de infraestructura sujeto a comité de cambios.
Se trabajan de manera que se pueden convertir en un requerimiento o desarrollo programado.
A13 Seguridad de las comunicaciones: Se cuenta con métodos de clasificación y divulgación de la información y maneja y controla través del proceso de Comunicaciones, se cuenta con Separación en las Redes Transferencia de Información acuerdos con partes externas, Políticas y procedimientos de transferencia de información, acuerdos de confidencialidad o de no divulgación.
A14 Adquisición, Desarrollo y Mantenimiento de Sistemas: Se cuenta con política de desarrollo seguro bajo lineamientos de ITIL, se cuenta con instructivo TI-I-005 INSTRUCTIVO GENERAL DE DESARROLLO DE SOFTWARE, s tienen lineamientos para la ejecución de pruebas no funcionales, y ejecución de pruebas funcionales.
A15 Relaciones con los proveedores: Se tienen establecidos los acuerdos de nivel de servicios (ANS) con proveedores, también se cuenta con política de proveedores, se tienen acuerdos de seguridad.
A16 Gestión de Incidentes de la Seguridad de la Información: Se cuenta con procedimientos de Gestión de Incidentes de Seguridad de la Información y se tienen establecidas las responsabilidades y procedimientos para asegurar una respuesta rápida, se cuenta con los reportes, evaluación y respuesta de eventos de seguridad de la información, se tiene respuesta a Incidentes de seguridad de acuerdo al Procedimiento para la gestión de incidentes
A través de sensibilizaciones se retroalimenta el aprendizaje obtenido de los incidentes de seguridad de la información.
A17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocio: Se cuenta con manual de continuidad de negocio DE-M-006.
Se está trabajando en la planificación de la continuidad de negocio y en el plan de recuperación de desastres.
Se tienen estrategias DRP con proyección en SIGME, SUI y ORFEO.
Se tienen requerimientos de máquinas, espacios, velocidad y capacidad de almacenamiento. Busca pasar de respaldo físico a respaldo a la nube.
Se cuenta con herramienta de disponibilidad de procesamiento de información a través de las ANS con directrices de cumplimiento de disponibilidad de servicio.
A18 Cumplimiento: Check list de protección de seguridad de la información, actividades de revisión de vulnerabilidades, accesos y Gestion de usuarios. Se cuenta con informes de vulnerabilidad de outsorsing Comsistelco (contrato 562) en septiembre de 2021 en temas de malware, fireware, mensualmente sobre 200 sistemas operativos con mediciones de vulnerabilidades altas 115 medias 457 y bajas 8. También herramientas como FORTI 100, FORTI MEIT para detectar tráficos.
Revisión de proceso con respecto al cumplimiento de ISO 27001:2013 a través de auditoria internas
Revisión de las políticas de seguridad y normas de seguridad
Pruebas de ética hacking y phishing con ingeniero interno a aplicaciones web, análisis a infraestructura tecnológica (servidores) antifraude, validación y comportamiento de usuario, fecha 13 agosto de 2021. Se cuenta sensibilización con

Boletín Infórmate número 29 del 27 de agosto. Datos Phishing "Gran Feria de Beneficios"
Se verifica la aplicación y conocimiento de los programas de:
Ambiental: GA-PG-001 Programa Manejo de Residuos Sólidos, GA-PG-002 Programa Gestión Eficiente de La Energía, GA-PG-003 Programa Uso Eficiente del Agua y GA-PG-004 Programa Buenas Prácticas Sostenibles, en donde se tienen las evidencias de la participación de comunicaciones y ejecuciones de aplicabilidad de las mismas.
Salud y seguridad en el trabajo: GH-PG-002 Programa Entorno Laboral Saludable y GH-PG-005 Programa Prevención Desordenes Musculo Esquelético en donde se evidencias las pausas activas y sensibilizaciones en temas de ergonomía, en noviembre de 2020, 27 de octubre de 2021.
Seguridad de la información: Se evidencia la protección de la información en correos electrónicos, accesos, manejo de SIGME, solicitud de acceso y retiros de SIGME.
8.5.4 La información se preserva en medio digital en ORFEO;SISGESTION y SIGEP
9/9.1/9.1.1 Se tiene seguimiento y medición del proceso mediante indicadores de:
- SOLICITUDES SOLUCIONADAS SOPORTE NIVEL 1 -2021
Periodicidad: Mensual
- TIEMPO PROMEDIO DE ATENCIÓN DE HABILITACIONES SUI - SOPORTE NIVEL 2 – 2021
Periodicidad: Mensual
- NIVEL DE SATISFACCIÓN DE USUARIOS (MANTENIMIENTOS) – 2021
Periodicidad: Trimestral
- INCIDENTES DE SEGURIDAD SOLUCIONADOS
Periodicidad: Semestral
- MANTENIMIENTO DE ACTIVOS TI
Periodicidad: Semestral
9.1.2 Se cuenta con análisis en cada uno de los indicadores del proceso.
9.1.3 Cada indicador tiene su análisis y rangos de medición los cuales están ligados a acciones inmediatas o preventivas o correctivas de no cumplir en los porcentajes esperados.
9.2 Se realizó la auditoria en 2020 a los sistemas de gestión de calidad, ambiental, SST y seguridad de la información;
En el proceso de auditoría interna de 2020 tuvieron 2 no conformidades.
AC-TI-031
Actualización de la matriz y roles y responsabilidades
Fecha de cierre: 21/06/2021
C-TI-017
Copias de respaldo
Fecha de cierre: 11/12/2021
9.3 La alta dirección revisa el sistema de gestión de la calidad, ambiental, SST y seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación, eficacia y alineación continuas con la dirección estratégica de la organización.
La frecuencia de realización dela Revisión por la Dirección es anual con corte 01 de junio.
Se incluyen las entradas de las normas NTC ISO 9001:2015 (Calidad), NTC ISO 14001:2015 (Ambiental), NTC ISO 27001:2013 (Seguridad y Privacidad de la Información) y NTC ISO 45001:2018 junto con el Decreto 1072 del 2015 y la Resolución 0312 del 2019 (Seguridad y Salud en el Trabajo)
Actualmente se encuentra en revisión.
10/ 10.1 La entidad ha determinado y seleccionado las oportunidades de mejora e implementado las acciones necesarias para cumplir con los requisitos del cliente y mejorar su satisfacción.
10.2/ 10.3 Se tienen 2 acción correctivas abiertas a la fecha.
AC-TI-032 –. Para cumplimiento el 31/12/2021
AC-TI-030 -. Para cumplimiento el 31/12/2021
AC-TI-028- Para cumplimiento el 30/09/2022
Actualmente no hay acciones de mejora y preventivas abiertas.

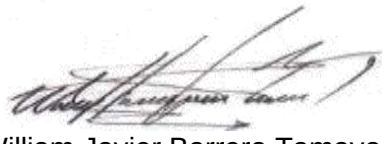
RIESGOS DEL PROCESO (bajo criterio de los auditores, el grado de riesgo que puede tener un proceso frente al cumplimiento total o parcial de los requisitos auditados):
Fallas en los servicios de energía, servicios de conexión, falta de disponibilidad de la información, demoras o fallas en el funcionamiento en las herramientas de consulta de la entidad.

OPORTUNIDADES DE MEJORA	REQUISITO NORMA
Es conveniente establecer un control de llaves, copias y cambios de las mismas.	A11 ISO 27001:2013
Es conveniente establecer protocolo de robo de equipos y gestión de incidentes, por perdida de equipo mes de enero y no reportado al proceso de Gestion TICs.	A.11.2 Equipos

No.	NO CONFORMIDAD	REQUISITO NORMA	PROCESO
	No hay o conformidades		No aplica

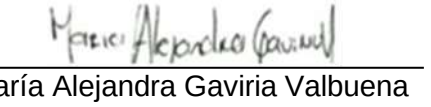
CONCLUSIONES DE AUDITORÍA
El equipo auditor llega a la conclusión de que el proceso ha establecido, mantenido y mejorado su sistema de gestión integral de acuerdo a los requisitos de la(s) norma(s), NTC ISO 9001:2015 (Calidad), NTC ISO 14001:2015 (Ambiental), NTC ISO 27001:2013(Seguridad y Privacidad de la Información) y NTC ISO 45001:2018 de igual manera el proceso ha demostrado la capacidad del sistema para lograr que se cumplan los requisitos para los servicios incluidos en el alcance, así como las políticas y los objetivos de la Organización desde el proceso de Gestion Tecnologías de la Información.

No. DE NO CONFORMIDADES HALLADAS	**0**
No. DE NO CONFORMIDADES CERRADAS DURANTE LA AUDITORIA	**0**
No. DE NO CONFORMIDADES PENDIENTES	**0**
No. DE CONFORMIDADES	**0**



William Javier Barrera Tamayo
AUDITOR LÍDER

David Mauricio Rodríguez Escobar
AUDITADO



María Alejandra Gaviria Valbuena
AUDITOR