

**DISEÑO Y ESTRUCTURA DE UNA GUÍA PARA LA DOCUMENTACIÓN DE UN
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
CON BASE EN LA NORMA ISO / IEC 27001:2005**

**DIANA CATALINA CARDONA ESTRADA
KATERINE VARGAS VIDAL**

**UNIVERSIDAD LIBRE SECCIONAL PEREIRA
FACULTAD CIENCIAS DE ECONOMICAS ADMINISTRATIVAS Y CONTABLE
PROGRAMA DE ADMINISTRACION DE EMPRESAS
PEREIRA
2015**

**DISEÑO Y ESTRUCTURA DE UNA GUÍA PARA LA DOCUMENTACIÓN DE UN
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
CON BASE EN LA NORMA ISO / IEC 27001:2005**

**DIANA CATALINA CARDONA ESTRADA
KATERINE VARGAS VIDAL**

*Trabajo de Investigación para optar al Título de
Profesional Administración de Empresas*

**Asesor
WALTER IVAN GARCÍA MORALES
Especialista Negocios Internacionales**

**UNIVERSIDAD LIBRE SECCIONAL PEREIRA
FACULTAD DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES
PROGRAMA DE ADMINISTRACIÓN DE EMPRESAS**

PEREIRA

2015

Nota de aceptación

Presidente del Jurado

Jurado

Jurado

Pereira, 14 de Enero de 2015

DEDICATORIA

A Dios, por permitirnos cumplir con nuestros sueños, por la vida, por la salud, por la familia y por el amor para seguir adelante sin decaer.

A nuestras madres por creer en nosotras, por su apoyo incondicional, por su motivación constante, porque siempre tienen una voz de aliento y un consejo sabio.

A nuestros hijos(as) porque son nuestro motor de fuerza, por esperarnos cada noche al regreso de la universidad, por todo su amor.

A mi hermana Diana Yury por ser un ejemplo a seguir, que hizo posible que iniciará esta etapa tan importante de mi vida y porque siempre está presente cuando necesito de una mano amiga.

Al nuestro asesor de proyecto de grado por brindarnos todo su conocimiento, por su esmero y paciencia en todo el proceso.

AGRADECIMIENTOS

A Dios, por permitirme llegar a este momento tan especial en mi vida. Por los triunfos y los momentos difíciles que me han enseñado a valorarte cada día más.

A nuestras madres, Por haberme educado y soportar mis errores. Gracias a tus consejos, por el amor que siempre me has brindado, por cultivar e inculcar ese sabio don de la responsabilidad.

¡Gracias por darme la vida!

¡Te quiero mucho!

Gracias a todos los docentes y compañeros del Programa de Administración de Empresas por su tiempo, por su apoyo así como por la sabiduría que me transmitieron en el desarrollo de mi formación profesional.

A la Universidad Libre y en especial a facultad de ciencias económicas, administrativas y contables que me dieron la oportunidad de formar parte de ellas.

¡Gracias!

TABLA DE CONTENIDO

DEDICATORIA	4
AGRADECIMIENTOS	5
LISTA DE TABLAS	10
LISTA DE GRÁFICOS	11
LISTA DE FIGURAS	12
RESUMEN	14
INTRODUCCIÓN	15
1. SINTESIS DEL MARCO TEORICO	16
2. OBJETIVOS DE LA INVESTIGACION	24
3. DISEÑO METODOLOGICO	25
4. LIMITANTES / LIMITACIONES	28
5. DIAGNÓSTICO ORGANIZACIONAL	29
5.1. CHECK LIST CON LOS REQUISITOS EXIGIDOS POR LA ISO/IEC 27001	29
5.2 APLICACIÓN CHECK LIST EN LA ORGANIZACIÓN	37
5.3.1 FACTORES INTERNOS	50
5.3.2 FACTORES EXTERNOS	92
6. REQUERIMIENTOS EXIGIDOS POR LA NORMA ISO 27001	94
6.1 MARCO CONCEPTUAL DE LOS REQUISITOS EXIGIDOS ISO 27001	94
7. METODOLOGÍA PARA DOCUMENTAR LOS PROCESOS CON EL CICLO PHVA110	
7.1 PROCESOS Y REGISTROS PARA CADA REQUISITO DE LA ISO 27001	112
7.2 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN.	150

8. GUÍA DOCUMENTAL	157
8.1 PLAN OPERATIVO PARA EL DESARROLLO DE LA GUÍA	157
8.2 DOCUMENTACIÓN DE LOS PROCESOS EXIGIDOS POR LA ISO 27001	161
8.2.1 Procedimiento de Organización de la Seguridad de la Información	161
8.2.2 Procedimiento Gestión de la Continuidad y Disponibilidad del negocio y de los servicios TI	170
8.2.3 Procedimiento Vinculación, inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación	202
8.2.4 Procedimiento Control de Servicios Contratados Externamente	218
8.2.5 Procedimiento Gestión de activos de información (AI)	226
8.2.6 Procedimiento Seguridad física y del entorno	238
8.2.7 Procedimiento Gestión de comunicaciones y operaciones	253
8.2.8 Procedimiento Control de acceso a la información	281
8.2.9 Procedimiento Adquisición y mantenimiento de sistemas de información	302
8.2.10 Procedimiento Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información	312
8.2.11 Procedimiento Mantenimiento de activos de información	322
8.2.12 Procedimiento Copias de Respaldo	325
8.2.13 Procedimiento Manejo de Medios	335
8.2.14 Procedimiento Gestión de incidentes de seguridad de la información y de servicios TI	339
8.2.15 Procedimiento Gestión de cambios	352
8.2.16 Procedimiento Gestión de las Relaciones con el Negocio y Gestión con los proveedores	364
8.2.17 Procedimiento Gestión de la Capacidad de los servicios TI y de los sistemas de información	373

8.2.18 Instructivo Análisis del impacto en el negocio	380
8.2.19 Instructivo Análisis de riesgos para la continuidad y disponibilidad de los procesos críticos	389
8.2.20 Política de Gestión de la Seguridad de la Información	398
8.3 REGISTROS EXIGIDOS POR LA ISO 27001	399
8.3.1 FO-PRO-07 Registro Lista de chequeo para el control de los servicios contratados externamente	399
8.3.2 FO-PRO-08 Registro Balance del servicio	400
8.3.3 FO-PRO-09 Registro Acuerdo de Confidencialidad	401
8.3.4 RC-DIR-01 Registro del comité de Seguridad de la información	407
8.3.5 Registro FO-DIR-01 Presupuesto para el SGI	408
8.3.6 Registro RC-HUM-16 Acuerdo de confidencialidad de la información y código de buena conducta	409
8.3.7 Registro RC-HUM-25 Roles, responsabilidades y autoridades de SI	419
8.3.8 Registro RC-MEI-05 Mantenimiento a la Infraestructura Interna	420
8.3.9 Registro RC-CAL-01 Plan para realizar la auditoría interna	421
8.3.10 Registro RC-CAL-02 Lista de verificación	422
8.3.11 Registro RC-SIS-32 Matriz del nivel de criticidad de los incidentes	423
8.3.12 Registro RC-SIS-41 Inventario de los activos de información	424
8.3.13 Registro RC-SIS-61 Reporte de vulnerabilidades encontradas	425
8.3.14 Registro RC-SIS-64 Identificación de usuarios y asignación de privilegios	426
8.3.15 Registro RC-SIS-68 Inventario de Sistemas de información.	427
8.3.16 Registro RC-SIS-69 Concesión y Verificación de acceso a los SI.	428
9. CONCLUSIONES	429

10. RECOMENDACIONES	431
BIBLIOGRAFIA	433

LISTA DE TABLAS

	Pág.
Tabla 1 Modelo (PHVA) aplicado a los procesos del SGSI	18
Tabla 2. Check List requisitos ISO 27001 Sin aplicar	29
Tabla 3. Tabla de valores y criterios de calificación para el diagnóstico	38
Tabla 4. Check List requisitos ISO 27001 Aplicado	39
Tabla 5. Tabla de valores y resultados	47
Tabla 6. Anexo A Objetivos de control y controles ISO 27001:2005	96
Tabla 7. Tipo de documento	110
Tabla 8. Nombre del proceso	111
Tabla 9. Matriz de correlación controles ISO de procedimientos o documentos soporte	114
Tabla 10. Listado maestro de documentos para el sistema de gestión de seguridad de la información	158

LISTA DE GRÁFICOS

	Pág.
Gráfico 1. Resultado del cumplimiento de cada fase PHVA	48
Gráfico 2. Sitio principal	181
Gráfico 3: Sitio de recuperación	182

LISTA DE FIGURAS

	Pág.
Figura 1. Ciclo PHVA	18
Figura 2: Mapa de procesos	50
Figura 3. Organigrama	59
Figura 4. Roles y Responsabilidades para la Seguridad de la Información	150
Figura 5. Equipos para ejecutar el plan de continuidad y Disponibilidad	187
Figura 6: Fases de activación del plan de continuidad	188
Figura 7: Registro lista de chequeo para controlar los servicios contratados externamente	399
Figura 8: Registro Balance del servicio	400
Figura 9. Registro del comité de Seguridad de la información	407
Figura 10. Registro Presupuesto del SGI	408
Figura 11. Registro Roles, responsabilidades y autoridades SI	419
Figura 12. Registro Mantenimiento a la infraestructura interna	420

Figura 13. Registro Plan para realizar la auditoría interna	421
Figura 14. Registro Lista de verificación	422
Figura 15. Registro Matriz del nivel de criticidad de los incidentes	423
Figura 16. Registro Inventario de los activos de información	424
Figura 17. Registro Reporte de vulnerabilidades encontradas	425
Figura 18. Registro Identificación de usuarios y asignación de privilegios	426
Figura 19. Registro Inventario de sistemas de información	427
Figura 20. Registro concesión y verificación de acceso a los SI	428

RESUMEN

El presente proyecto pretende dar una adecuada solución de Seguridad de la información a la Organización Cyfo Comunicaciones y Fibra Óptica, tomando como base el estándar internacional ISO/IEC 27001:2005.

En el primer capítulo se realiza un diagnóstico para conocer el estado actual de la organización frente al cumplimiento de los requisitos exigidos por la norma ISO 27001; además se identifican los factores internos como los procedimientos organizacionales, estructura organizativa, funciones de los colaboradores, estructura tecnológica y clientes; y los factores externos como la competencia y proveedores con el objetivo de analizar las necesidades que tiene la organización para gestionar adecuadamente la información tanto interna como de las partes interesadas.

En el segundo capítulo se definen los requerimientos exigidos por la norma ISO 27001:2005, con una breve descripción de los 11 dominios y los controles del anexo A; con los cuales se documentarán los procedimientos y registros que ayudaran a garantizar la seguridad de la información.

En el tercer capítulo, se define una estructura documental de procedimientos y registros necesarios para dar cumplimiento a cada uno de los requisitos de la norma; donde se establecen las actividades a ejecutar y los registros que se deben diligenciar para demostrar la conformidad con el estándar con los cuales se minimizarán los riesgos que puedan afectar la seguridad de la información en la organización.

INTRODUCCIÓN

En Latinoamérica se ha incrementado la preocupación sobre las tendencias en materia de seguridad de la información, debido a que frecuentemente se han evidenciado estafas, ataques tecnológicos e introducción de códigos maliciosos que han generado amenazas contra la confidencialidad e integridad de la información.

En las organizaciones se considera que la seguridad de la información es sólo un problema tecnológico, sin tener en cuenta que es un problema de gestión y organización que puede ocasionar riesgos incalculables desde la pérdida de información hasta el incumplimiento de la legislación colombiana.

La información es poder, y la verdadera ventaja competitiva radica en poder asegurar su confidencialidad, integridad y disponibilidad y es allí en donde las empresas, con el fin de salvaguardar estos activos tan valiosos, implementan estrategias que cubren todos los procesos de la empresa, procesos en donde la información es el primordial activo.

La definición de un modelo de gestión de seguridad de la información implica involucrar a toda la organización en la aplicación de métodos seguros y eficientes que controlen y limiten el acceso a información y a los sistemas que la procesan, estas estrategias deben tener como punto fundamental el establecimiento de políticas, controles de seguridad físicas y de acceso lógico y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger tanto a la información como a los sistemas que la almacenan y administran. De ahí, que se puede considerar a la información, como uno de los activos más valiosos, para cualquier tipo de organización.

1. SINTESIS DEL MARCO TEORICO

PRIMERA VISIÓN

De acuerdo a la visión de Enrique Anton Peregrina: Realidad o Utopía, se evidencia que en la actualidad la Seguridad de la Información es uno de los temas de mayor preocupación de las organizaciones, teniendo en cuenta que la información es uno de los activos más valiosos e importantes, al cual se debe aplicar los controles de seguridad con la finalidad de minimizar los riesgos y evitar así ataques o desastres, pérdida de información crítica hasta la interrupción de las operaciones de la organización. Sin embargo, muchas veces estos esfuerzos no son correctamente encaminados. Bajo este contexto es bueno recordar lo señalado por Jorge Sendra Mas quien indica lo siguiente:

"La Seguridad de la Información ha experimentado una continua evolución durante la última década, desde un enfoque puramente tecnológico, donde las necesidades se cubren mediante la adquisición de herramientas con el fin de mitigar las últimas vulnerabilidades conocidas, hasta un enfoque dominado por la necesidad de justificar las inversiones en seguridad de la información, como un activo esencial. Este enfoque se basa en una gestión continua de los riesgos sustentados en la optimización de ratios empresariales como es el de coste/beneficio."¹

¹ SENDRA, Mas Jorge.- Director del Área de Consultoría de IP Sistemas - La Seguridad TIC, una responsabilidad de todos. [Consulta: 8 junio de 2014]. Disponible en internet: <http://www.monografias.com/trabajos85/seguridad-informacion-realidad-o-utopia/seguridad-informacion-realidad-o-utopia.shtml>

Otro punto importante es señalar como algunas organizaciones creen tener todos los riesgos bajo control y una protección del 100%, de hecho es un error, no hay nada seguro; por esta razón es necesario encontrar soluciones de seguridad aplicables al tipo de organización como estrategia que integra, hardware, software, infraestructura, políticas y procedimientos.

SEGUNDA VISIÓN

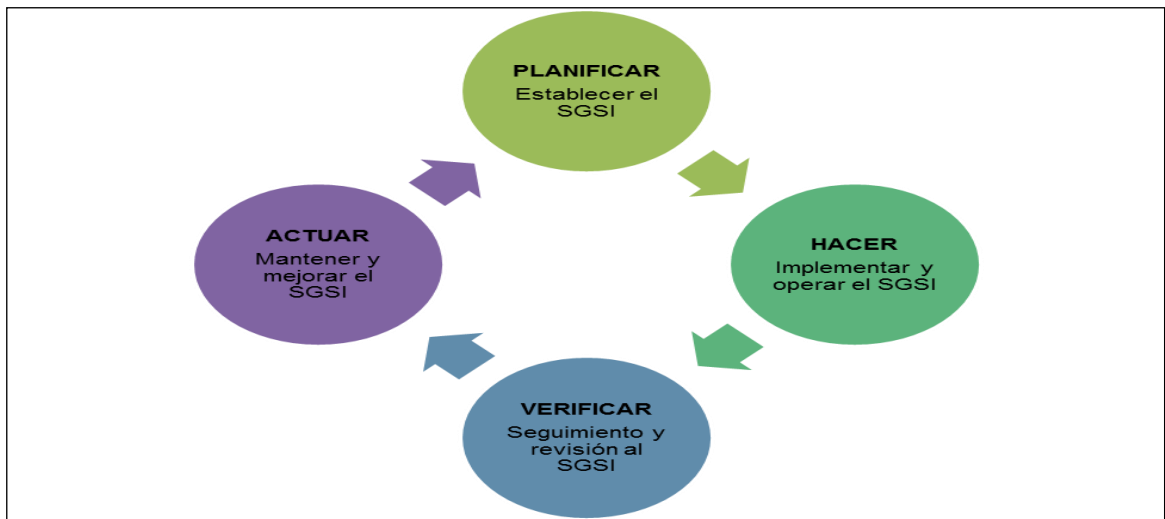
Partiendo del enfoque de Edward W. Deming para la implementación de un sistema de gestión de la seguridad de la información, se requiere desarrollar las actividades en un marco lógico bajo el ciclo PHVA Planificar, hacer, verificar y actuar; como estrategia efectiva para la organización y la documentación que se requiere en este proceso.²

Bajo esta filosofía del mejoramiento continuo, en seguridad de la información es la reevaluación de los controles preventivos, de corrección y evaluación y de mantenimiento; un constante ciclo que no podría terminar

La siguiente figura muestra el modelo basado en los procedimientos esenciales para cada ciclo PHVA.

² UNAD. Ciclo PDCA (Deming Edward) [en línea]. En: Universidad Nacional Abierta y a Distancia. [Consulta: 28 noviembre 2013]. Disponible en internet: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/21_leccion_6_la_organizacion_iso_y_la_familia_de_normas_iso.html

Figura 1. Ciclo PHVA



Fuente: Elaboración propia

Tabla 1 Modelo (PHVA) aplicado a los procesos del SGSI

<u>CICLO PHVA</u>	<u>PROCESOS</u>
Planificar	Establecer el contexto. Alcance y Limites Definir Política del SGSI Definir Enfoque de Evaluación de Riesgos Identificación de riesgos Análisis y Evaluación de riesgos Evaluar alternativas para el Plan de tratamiento de riesgos Aceptación de riesgos Declaración de Aplicabilidad

Continuación Tabla 1

<p>Hacer</p>	<p>Implementar plan de tratamiento de riesgos Implementar los controles seleccionados Definir las métricas Implementar programas de formación y sensibilización Gestionar la operación del SGSI Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad</p>
<p>Verificar</p>	<p>Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI</p>
<p>Actuar</p>	<p>Implementar las mejoras identificadas para el SGSI Implementar las acciones correctivas y preventivas pertinentes. Comunicar acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.</p>

Fuente: Elaboración propia

TERCERA VISIÓN

La importancia de contar con un sistema de gestión de la seguridad de la información en el mundo se ha robado la atención en los últimos años, en la Jornada Internacional de ISMS Forum Spain; allí Lukas Alarcon, profesional en seguridad de la información explicó que a pesar de que muchas personas asocian la idea de protección informática con los hackers, siendo esto un error debido a que la seguridad informática tienen muchos frentes. La tecnología es solo un aspecto de la seguridad que deben de tenerse en cuenta, el cual indica:

“Actualmente hay varias formas de encarar el tema de la seguridad de la información. Un ejemplo podría tener políticas de seguridad de información cuyo contenido y estructura refleje el ámbito cultural de la propia empresa y su dinámica respecto a su quehacer, una arista mas es la implementación efectiva de las políticas en las que los elementos técnicos que me ayudan en la implementación estén de acuerdo a mis objetivos.”³

Las organizaciones no solo se enfrentan al reto de controlar los riesgos de seguridad sino también a cumplir con las normas vigentes de gestión de seguridad de la información para proteger sus datos desde adentro, debido a que son los propios empleados quienes pueden manipular indebidamente la información.

“Según el estudio realizado entre más de 3.000 profesionales, seis de cada diez encuestados apunta que ha perdido datos sensibles como resultado de una negligencia por parte de los empleados de la compañía. Además, otro dato destacable de este estudio resalta que tres de cada diez encuestados afirma haber sufrido el robo de datos sensibles por parte de sus propios empleados.”⁴

³ ISMS FORUM SPAIN (Alarcon Lukas). La necesidad de la certificación ISO 27001 acaparó la atención de la 1 jornada de internacional de ISMS Forum Spain [en línea]. En: Asociación Española para el fomento de la seguridad de la información. [Consulta: 15 enero de 2014]. Disponible en internet: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/21_leccion_6_la_organizacin_iso_y_la_familia_de_normas_iso.html

⁴ Seguridad informática (Gonzáles Encarna). Los empleados, cada vez un mayor riesgo para la seguridad de las empresas. Disponible en internet: <https://seguinfo.wordpress.com/category/riesgos/page/12/>

ARTICULACIÓN DE LOS ASPECTOS

El objetivo principal de una empresa es la generación de dinero ahora y en el futuro; esta es una premisa bien conocida en las actuales teorías financieras y de valoración de empresas; sin embargo, esto no es suficiente, lo realmente importante es encontrar la metodología adecuada para lograrlo de una manera segura y confiable respecto al uso y buen manejo de la información, independientemente del soporte en el que se encuentre, de tal manera que se pueda asegurar la continuidad de las actividades de la organización y minimizar el perjuicio y/o daño que se pudiera causar así como maximizar el rendimiento del capital invertido.

Se caracteriza por preservar:

- ✓ Confidencialidad.
- ✓ Integridad.
- ✓ Disponibilidad.

No cabe ninguna duda que actualmente nos enfrentamos a mundo globalizado donde las comunicaciones no tienen fronteras y esto conlleva a un sinnúmero de riesgos y nuestro principal desafío es encontrar la manera de controlar las amenazas a los que está expuesta la información dentro del contexto de los riesgos globales del negocio de la organizacional.

Al abarcar la Gestión de la Seguridad de la Información, la Gestión de Riesgos tiene como objetivos principales proteger la información; la reputación de la marca, la administración de los controles, la promoción de las acciones correctivas y preventivas, el cumplimiento de la normatividad y la definición de los procesos de gestión de la Seguridad de la Información que se requieran.

Para la estandarización de los controles de seguridad y diseño de un SGSI se debe realizar teniendo en cuenta el ciclo PHVA, (planear, hacer, verificar y actuar) con el fin de evidenciar de manera secuencial y lógica las actividades que se llevarán a cabo. Dentro del contexto de un Sistema de Seguridad de la información, el PHVA es un ciclo dinámico que puede desarrollarse dentro de cada proceso de la organización, tomando como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios promueve resultados de seguridad de la información que cumplen estos requisitos y expectativas.

Para enfrentar la Seguridad de la Información en la organización se debe establecer y documentar una serie de reglas, normas y controles de seguridad que se pueden estandarizar en documentos como: Políticas, Planes, Registros, Formatos, Manuales y Procedimientos. Sin embargo esto no es suficiente, la Alta Dirección debe promover una cultura transparente y orientada a proteger los principios de confidencialidad, integridad y disponibilidad de la información y lograr que los colaboradores se han conscientes de los riesgos y que participen activamente en su control y gestión. Consecuente con lo anterior, es de gran importancia que los colaboradores asuman en forma permanente, en todas sus actuaciones la práctica de los controles de seguridad.

Los colaboradores de todos los niveles de la organización deben ser entrenados continuamente en materia de seguridad de la información, buscando así cerrar las brechas de información que son originados por “Errores humanos” como son: el plagio de contraseñas, datos sin encriptar, error en el envío de información a un correo electrónico, falta de conocimientos en informática, cohecho, entre otros.

En conclusión un Sistema de Gestión de Seguridad de la información debe ser aplicable y estandarizado de acuerdo a las necesidades de la organización, bajo el ciclo PHVA y aplicado a todos sus activos como son: la información, la infraestructura física y tecnológica y el recurso humano.

2. OBJETIVOS DE LA INVESTIGACION

OBJETIVO GENERAL

Diseñar y estructurar una guía para la documentación de un Sistema de Seguridad en la Información basada en la norma ISO/IEC 27001:2005.

OBJETIVOS ESPECÍFICOS

- Elaborar un diagnóstico de la situación actual de organización frente a la documentación requerida para la seguridad de la información.
- Identificar cuáles son los procesos, procedimientos y metodología necesarios para documentar los controles de seguridad de la información.
- Proponer y estructurar una guía documental bajo la norma ISO/IEC 27001:2005, para el Sistema de Seguridad en la Información.

3. DISEÑO METODOLOGICO

- TIPO DE INVESTIGACIÓN

Descriptiva:

Con base en el propósito de esta investigación se requirió la utilización de un enfoque de investigación, que garantizara el aspecto científico y la objetividad del estudio tratado. En tal sentido, la investigación está enmarcada dentro de la modalidad de campo.

La investigación de campo es aquella donde se recogen los datos en forma directa, mediante el trabajo concreto del investigador, estos datos son llamados primarios ya que son de primera mano, originales, producto de la investigación en curso, sin intermediarios de ninguna naturaleza.

A objeto de ampliar y profundizar el conocimiento de las variables que constituyen el eje del estudio, la investigación de campo, se apoyó en las investigaciones de carácter descriptivo y documental. En tal sentido, la investigación está enmarcada dentro de la modalidad descriptiva. En la investigación descriptiva, los únicos elementos que manipula el investigador son los métodos de observación y descripción.

- MÉTODO DE INVESTIGACIÓN

Análisis y Síntesis

En atención al objeto y los fines planteados en esta investigación, fue necesario formular un procedimiento concreto que proporcionará y garantizará resultados válidos, confiables y coherentes. Las técnicas que se utilizaron para la recopilación de la información precisa y veraz, permitió

estudiar con detalle los procedimientos asociados a cada proceso, la forma como se lleva a cabo cada proceso y cómo se produce la interrelación entre ellos, para luego desarrollar mejoras al sistema y cumplir con los objetivos propuestos.

Por esta razón, la investigación se llevara a cabo de acuerdo a las etapas que a continuación se describen:

Etapa 1: Conocer la situación actual de la compañía con el fin de aprovechar la estructura procedimental, organizacional y tecnológica existente.

Etapa 2: Realizar un diagnóstico sobre la situación actual de la empresa frente al cumplimiento de los requisitos exigidos por la norma ISO 27001 del sistema de gestión de seguridad de la información.

Etapa 3: Definir y establecer la documentación necesaria para la organización que den cumplimiento a cada uno de los requisitos exigidos por la norma ISO soportados en la estructura organizacional y documental existente.

- INFORMACIÓN PRIMARIA
Cyfo Comunicaciones y Fibra Óptica

- INFORMACIÓN SECUNDARIA
 - ✓ Icontec
 - ✓ Internet
 - ✓ Cyfo Comunicaciones y Fibra Óptica

- POBLACIÓN Y MUESTRA

Población: Cyfo Comunicaciones y Fibra Óptica

Muestra: 3 Personas del área administrativa (Gerente General, Coordinador TIC y Coordinador SGI)

4. LIMITANTES / LIMITACIONES

Para el desarrollo de una guía documental con base en la norma ISO 27001 sistema de Gestión de Seguridad de la Información se tuvieron los siguientes limitantes:

- Dificultades para la consecución de la información necesaria para realizar el diagnóstico organizacional
- Desorganización del área de tecnología
- Información descentralizada en lo que respecta al área de tecnología
- Desconocimiento de las normas de seguridad de la información
- Falta de concientización de la parte directiva sobre la importancia de la seguridad de la información.

5. DIAGNÓSTICO ORGANIZACIONAL

5.1. CHECK LIST CON LOS REQUISITOS EXIGIDOS POR LA ISO/IEC 27001

Se establece un check list considerando los requisitos definidos en el estándar ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información basado en el ciclo Planear-Hacer-Verificar-Actuar (P-H-V-A) con el fin de conocer la situación actual de organización frente a la documentación requerida para la seguridad de la información

Tabla 2. Check List requisitos ISO 27001 sin aplicar

REQUISITO ISO	CICLO PROCESO	VARIABLE	ESTADO ACTUAL	CALIFICACIÓN
4.2.1	Planear	ESTABLECIMIENTO Y GESTION SGSI		
4.2.1.a	Planear	ALCANCE Y LIMITES DEL SGSI		
4.2.1.a	Planear	¿Están definidas las características del negocio?		
4.2.1.a	Planear	¿Están definidos los Objetivos y necesidades de la Organización?		
4.2.1.a	Planear	¿Está definida la Estructura y recursos en la Organización para implantar SGSI?		
4.2.1.a	Planear	¿Se han seleccionado las áreas/procesos a involucrar en el SGSI?		
4.2.1.a	Planear	¿Están definidos los requisitos y expectativas de seguridad?		
4.2.1.a	Planear	¿Están definidas las actividades, sedes físicas, tecnología a incluir/excluir en el SGSI?		

Tabla 2. (Continuación)

4.2.1.a	Planear	¿Se han estimado los recursos humanos, técnicos y económicos para implantar SGSI?		
4.2.1.a	Planear	¿Existe un Documento Alcance y Límites SGSI?		
4.2.1.b	Planear	POLITICA DE SEGURIDAD		
4.2.1.b	Planear	¿Se ha definido una política de seguridad y objetivos globales?		
4.2.1.b	Planear	¿Existe declaración de la Dirección para el apoyo de objetivos y principios de seguridad?		
4.2.1.b	Planear	¿Existe una definición de responsabilidades generales y específicas en cada rol?		
4.2.1.b	Planear	¿Están definidos los activos que se protegen, de quién/qué y por qué?		
4.2.1.b	Planear	¿Se han establecido los criterios para gestión de riesgos y selección de objetivos de control y controles?		
4.2.1.b	Planear	¿Se han seleccionado las medidas de seguridad a implementar?		
4.2.1.b	Planear	¿Se han establecido los criterios de actuación ante incidentes de seguridad?		
4.2.1.b	Planear	¿Se han establecido los procesos de revisión periódica, ante incidentes de seguridad o ante cambios estructurales en la organización?		
4.2.1.b	Planear	¿Se ha publicado y aprobado por parte de la Dirección?		
4.2.1.b	Planear	¿Está disponible para consulta?		
4.2.1.b	Planear	¿Existe Documento Política de Seguridad?		
4.2.1.a	Planear	ORGANIZACIÓN DE LA SEGURIDAD		
4.2.1.a	Planear	¿Se ha seleccionado al responsable de la seguridad?		
4.2.1.a	Planear	¿Se ha nombrado al Comité de Dirección?		
4.2.1.a	Planear	¿Se ha nombrado al Comité de Gestión?		
4.2.1.a	Planear	¿Se han tomado medidas frente a terceros para proteger la información?		

Tabla 2. (Continuación)

4.2.1.a	Planear	¿Existe Documento Organización de la Seguridad?		
4.2.1.a	Planear	SENSIBILIZACION Y FORMACION DEL PERSONAL		
4.2.1.a	Planear	¿Existe una campaña para divulgar los avances del SGSI en toda la organización?		
4.2.1.a	Planear	¿Se ha capacitado al personal encargado de la SGSI para enfrentar sus nuevas actividades?		
4.2.1.a	Planear	¿Existe Documento sensibilización y formación del personal?		
4.2.1.d	Planear	IDENTIFICACION DE ACTIVOS		
4.2.1.d	Planear	¿Se ha definido alguna metodología para identificar activos?		
4.2.1.d	Planear	¿Existe inventario de activos (descripción-localización-propietario-grado de seguridad)?		
4.2.1.d	Planear	¿Están incluidos los activos intangibles (Imagen Organizacional)?		
4.2.1.d	Planear	¿Se ha determinado el ciclo de vida útil de los activos?		
4.2.1.d	Planear	¿Existe análisis o árbol de dependencia entre activos?		
4.2.1.d	Planear	¿Existe Documento Inventario de activos?		
4.2.1.d	Planear	VALORACION DE ACTIVOS		
4.2.1.d	Planear	¿Existe valoración de activos según la importancia e impacto ante una incidencia basado en CID (cuantitativa y/o cualitativa)?		
4.2.1.d	Planear	¿Qué Método es empleado para valorar activos (entrevista, encuesta)?		
4.2.1.d	Planear	¿Existe Documento valoración de activos?		

Tabla 2. (Continuación)

4.2.1.d	Planear	IDENTIFICACION DE RIESGOS		
4.2.1.d	Planear	¿Se ha identificado áreas que requieren medidas de seguridad?		
4.2.1.d	Planear	¿Existe identificación de riesgos y están asociados a los activos inventariados?		
4.2.1.d	Planear	¿Existe identificación de riesgos asociados a los activos más críticos?		
4.2.1.d	Planear	¿Hay Amenazas identificadas que afectan los activos inventariados?		
4.2.1.d	Planear	¿Existe Análisis de vulnerabilidades de los activos inventariados?		
4.2.1.d	Planear	¿Se conoce el impacto por la ocurrencia de un riesgo?		
4.2.1.e	Planear	¿Se ha determinado la probabilidad de ocurrencia de un riesgo?		
4.2.1.d	Planear	¿Este proceso considera los recursos de la organización?		
4.2.1.d	Planear	¿Existe Análisis de medidas de seguridad ya implantadas?		
4.2.1.d	Planear	¿Hay Participación de las diversas áreas de la compañía?		
4.2.1.d	Planear	¿Existe Documento identificación de riesgos?		
4.2.1.c	Planear	ENFOQUE PARA VALORACION DE RIESGOS		
4.2.1.c	Planear	¿Se ha definido alguna metodología para valorar riesgos?		
4.2.1.c	Planear	¿Se han estimado los niveles para los riesgos?		
4.2.1.c	Planear	¿Existe un Documento enfoque para valorar riesgos?		
4.2.1.f	Planear	GESTION DEL RIESGO		
4.2.1.f	Planear	¿Se han definido acciones frente a los riesgos identificados y valorados?		

Tabla 2. (Continuación)

4.2.1.f	Planear	¿Se ha determinado el riesgo residual para cada riesgo identificado y valorado?		
4.2.1.c,e	Planear	¿Existen criterios definidos para tomar riesgo aceptable?		
4.2.1.f	Planear	¿Hay Aprobación por dirección para los riesgos aceptable?		
4.2.1.f	Planear	¿Existe Documento de Aprobación Dirección Gestión de Riesgos?		
4.2.1.h	Planear	¿Existe Documento de Aprobación Dirección Riesgos residuales?		
4.2.1.f	Planear	¿Existe Documento matriz de riesgos?		
4.2.1.g	Planear	SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES		
4.2.1.g	Planear	¿Existe Análisis de controles existentes?		
4.2.1.g	Planear	¿Existe Análisis y selección de los dominios, objetivos y controles a implantar?		
4.2.1.g	Planear	¿Se Cumplen los requisitos definidos en procesos de tratamiento de riesgos?		
4.2.1.g	Planear	¿Se hacen Inversiones en controles proporcionales al impacto del riesgo?		
4.2.1.g	Planear	¿Existen Controles documentados en procedimientos?		
4.2.1.g	Planear	¿Hay disponibilidad de recursos para implementar los controles?		
4.2.1.g	Planear	¿Existe justificación para los objetivos y controles seleccionados y no seleccionados?		
4.2.1.j	Planear	¿Existe Documento declaración de aplicabilidad?		
4.2.1.i	Planear	AUTORIZACION PARA IMPLEMENTAR Y OPERAR SGSI		
4.2.1.i	Planear	¿Existe Documento de aprobación por dirección para implementar y operar el SGSI?		

Tabla 2. (Continuación)

4.2.1	Planear	GESTION DE LA CONTINUIDAD DEL NEGOCIO (PCN)		
4.2.1	Planear	¿Están identificados los procesos críticos a recuperar progresivamente?		
4.2.1	Planear	¿Existe PCN extraído de gestión de riesgos críticos?		
4.2.1	Planear	¿Se ha puesto a prueba el PCN (cuánto es el tiempo de recuperación mínimo, los ANS se conservan)?		
4.2.1	Planear	¿Existe comité de emergencia para solucionar las crisis?		
4.2.1	Planear	¿Existen procedimientos (relacionados a cada situación) establecidos para aplicar en las crisis (indica acciones y sugerencias)?		
4.2.1	Planear	¿Los procedimientos han sido divulgados y puestos a prueba?		
4.2.1	Planear	¿Existen registros que documentan la reacción ante la crisis y su respectivo análisis?		
4.2.1	Planear	Fases PCN: Definición del proyecto (alcance y objetivos de peor escenario) - Análisis de impacto (riesgos, impacto económico) - Selección de estrategias (recursos-salvaguardas a usar) - Desarrollo - Pruebas periódicas y mantenimiento		
4.2.2	Hacer	IMPLEMENTACION Y OPERACIÓN SGSI		
4.2.2.a,b	Hacer	PLAN DE TRATAMIENTO DE RIESGOS		
4.2.2.a,b	Hacer	¿Existe guía de ejecución del plan para tratamiento de riesgos?		
4.2.2.h	Hacer	¿Se han definido Procedimientos y controles adicionales para detectar y reaccionar ante incidentes de seguridad en esta fase?		
4.2.2.a,b	Hacer	¿Existe documento informe de plan para tratamiento de riesgos?		
4.2.2.c	Hacer	IMPLANTACION DE CONTROLES		
4.2.2.c	Hacer	¿Se han definido los responsables de los controles técnicos?		

Tabla 2. (Continuación)

4.2.2.c	Hacer	¿Se han definido los responsables de los controles administrativos?		
4.2.2.d	Hacer	¿Se han definido los indicadores para cada control implantado?		
4.2.2.d	Hacer	¿Existe un método para medir la eficacia de los controles implantados?		
4.2.2.h	Hacer	¿Se han implantado controles adicionales ante incidentes de seguridad detectados en esta fase?		
4.2.2.e	Hacer	¿Se ha hecho sensibilización y divulgación?		
4.2.2.c	Hacer + Dominios 1-15	¿Existen los procedimientos de los controles del anexo A, correspondientes a 133 controles?		
4.2.3	Verificar	SEGUIMIENTO Y REVISION SGSI		
4.2.3	Verificar	PROCEDIMIENTOS SEGUIMIENTO Y REVISION		
4.2.3.a,c	Verificar	¿Se hace un análisis periódico de indicadores y su eficacia?		
4.2.3.b,e	Verificar	¿Se realizan auditorías internas/externas al sistema?		
4.2.3.b,e	Verificar	¿Se hace revisión por Dirección de las auditorias?		
4.2.3.a	Verificar	¿Se hace revisión por Dirección del informe Comité de Gestión?		
4.2.3.a	Verificar	¿Se hace revisión por Dirección del informe Responsable Seguridad?		
4.2.3.d	Verificar	¿Se hace revisión periódica por Dirección de valoración de riesgos, riesgo residual, riesgo aceptable?		
4.2.3.b,e	Verificar	¿Existe un documento auditorías internas?		
4.2.3.a,b,c,d,e	Verificar	¿Existe un documento de revisión por dirección?		
4.2.4	Actuar	MANTENIMIENTO Y MEJORA SGSI		
4.2.4.a,b	Actuar	¿Se ejecutan acciones correctivas, preventivas, mejora?		
4.2.4.a,b	Actuar	¿Se hace la actualización de riesgos y controles?		

Tabla 2. (Continuación)

14	4.2.4.d	Actuar	¿Se hace la medición de eficacia de acciones implementadas?		
14	4.2.4.c	Actuar	¿Existe un documento informe de ejecución de acciones correctivas-preventivas?		

Fuente: Elaboración propia

5.2 APLICACIÓN CHECK LIST EN LA ORGANIZACIÓN

La aplicación de la lista de chequeo se realiza a los siguientes cargos: Coordinador TIC, Coordinadora de los Sistemas de Gestión y el Gerente General con el fin de obtener datos verídicos y exactos del estado real de la organización frente a la Seguridad de la información.

A continuación se muestra la tabla 3, que abarca todos los puntos requeridos por el estándar ISO/IEC 27001 en las fases PHVA para identificar el nivel de avance o implementación que tiene la organización:

Planear que corresponde al capítulo 4.2.1 “Establecimiento del SGSI”, a esta fase se tienen definidos 74 ítems, para una suma total de 370 puntos, se asigna un porcentaje total del 25% debido a que es una de las etapas con un número de ítems considerables, los cuales se deben planificar para la implementación en la fase del Hacer.

Hacer que corresponde al capítulo 4.2.2 “Implementación y Operación SGSI” y el Anexo A de la norma ISO 27001, a esta fase se tiene definidos 10 ítems, para una suma total de 50 puntos. Se asigna un porcentaje total del 35% debido a que es una de las etapas más complejas, donde se debe definir e implementar los requisitos de la fase planear y establecer los procedimientos con los controles de seguridad considerando el Anexo “A”.

Verificar que corresponde al capítulo 4.2.3 “Seguimiento y Revisión SGSI”, se tienen definidos 8 ítems, para una suma total de 40 puntos. Se asigna un porcentaje total del 20% debido a que en esta etapa, los ítems son más pocos y las actividades que allí se solicitan son repetitivas y no complejas.

Actuar que corresponde al capítulo 4.2.4 “Mantenimiento y Mejora SGSI”, se tienen definidos 4 ítems, para una suma total de 20 puntos. Se asigna un porcentaje total del 20% debido a que en esta etapa, los ítems son más pocos y no corresponden a controles de Seguridad.

Tabla 3. Tabla de valores y criterio de calificación para diagnóstico.

TABLA VALORES POR ÍTEM		
CICLO	# ÍTEMS	VALOR %
Planear	74	25
Hacer	10	35
Verificar	8	20
Actuar	4	20
CRITERIO DE CALIFICACIÓN PARA DIAGNÓSTICO		
Calificación	Concepto	
0	No existe avance	
1	Se tiene conocimiento del ítem	
2	En inicio	
3	Se han avanzado moderadamente en el control	
4	Se tiene documentado	
5	Se tiene implementado	

Fuente: Elaboración propia

Tabla 4. Check List requisitos ISO 27001 Aplicado

REQUISITO ISO	CICLO PROCESO	VARIABLE	ESTADO ACTUAL	CALIFICACIÓN
4.2.1	Planear	ESTABLECIMIENTO Y GESTION SGSI		
4.2.1.a	Planear	ALCANCE Y LIMITES DEL SGSI		
4.2.1.a	Planear	¿Están definidas las características del negocio?	Está definido el alcance, el marco estratégico. La estructura organizacional, roles, misión, visión, valores, objetivos corporativos y de calidad están planteados y aprobados.	2
4.2.1.a	Planear	¿Están definidos los Objetivos y necesidades de la Organización?	Se planteó una matriz DOFA para la identificación de necesidades. De ahí salieron las estrategias y los Objetivos corporativos. DA: Proyección estratégica corporativa.	2
4.2.1.a	Planear	¿Está definida la Estructura y recursos en la Organización para implantar SGSI?	Se tiene aprobado un presupuesto para la implementación del SGSI. En la Proyección estratégica 2014 está planteada la implementación del SGSI.	2
4.2.1.a	Planear	¿Se han seleccionado las áreas/procesos a involucrar en el SGSI?	Todos los procesos están incluidos en el mapa de procesos del SGC.	2
4.2.1.a	Planear	¿Están definidos los requisitos y expectativas de seguridad?	No se ha definido.	0
4.2.1.a	Planear	¿Están definidas las actividades, sedes físicas, tecnología a incluir/excluir en el SGSI?	No.	0
4.2.1.a	Planear	¿Se han estimado los recursos humanos, técnicos y económicos para implantar SGSI?	Se tiene aprobado un presupuesto para la implementación del SGSI. (Asesor y auditor externo) están definidos.	2
4.2.1.a	Planear	¿Existe un Documento Alcance y Límites SGSI?	Se tiene un alcance planteado para el SGC , no se tiene para el SGSI	2
4.2.1.b	Planear	POLITICA DE SEGURIDAD		

Tabla 4. (Continuación)

4.2.1.b	Planear	¿Se ha definido una política de seguridad y objetivos globales?	Se cuenta con directriz para la política de calidad, no se tienen definidos principios de seguridad.	2
4.2.1.b	Planear	¿Existe declaración de la Dirección para el apoyo de objetivos y principios de seguridad?	No.	0
4.2.1.b	Planear	¿Existe una definición de responsabilidades generales y específicas en cada rol?	Están definidas las responsabilidades para el SGC pero no se tiene definidas las del sistemas SGSI	2
4.2.1.b	Planear	¿Están definidos los activos que se protegen, de quién/qué y por qué?	Hay un seguro contra todo riesgo que cubre todos los activos de la empresa. La administrativa define qué proteger.	1
4.2.1.b	Planear	¿Se han establecido los criterios para gestión de riesgos y selección de objetivos de control y controles?	Sobre gestión de riesgos no se ha hecho nada al respecto.	0
4.2.1.b	Planear	¿Se han seleccionado las medidas de seguridad a implementar?	No.	0
4.2.1.b	Planear	¿Se han establecido los criterios de actuación ante incidentes de seguridad?	No.	0
4.2.1.b	Planear	¿Se han establecido los procesos de revisión periódica, ante incidentes de seguridad o ante cambios estructurales en la organización?	No hay nada documentado, algunos de estos procesos son iniciativa únicamente de cada responsable.	0
4.2.1.b	Planear	¿Se ha publicado y aprobado por parte de la Dirección?	No.	0
4.2.1.b	Planear	¿Está disponible para consulta?	No.	0
4.2.1.b	Planear	¿Existe Documento Política de Seguridad?	No.	0
4.2.1.a	Planear	ORGANIZACIÓN DE LA SEGURIDAD		
4.2.1.a	Planear	¿Se ha seleccionado al responsable de la seguridad?	Se encargó al personal de sistemas de esta responsabilidad, pero no hay nada documentado oficialmente ni tareas totalmente definidas.	1
4.2.1.a	Planear	¿Se ha nombrado al Comité de Dirección?	Existe comité de calidad que se realiza bimestralmente para revisar el SGC.	2

Tabla 4. (Continuación)

4.2.1.a	Planear	¿Se ha nombrado al Comité de Gestión?	Sí se ha nombrado, faltaría incorporar al líder de sistemas para analizar los ítems de seguridad de la información.	2
4.2.1.a	Planear	¿Se han tomado medidas frente a terceros para proteger la información?	Se toman las medidas básicas intuitivas, pero no hay nada documentado.	1
4.2.1.a	Planear	¿Existe Documento Organización de la Seguridad?	No.	0
4.2.1.a	Planear	SENSIBILIZACION Y FORMACION DEL PERSONAL		
4.2.1.a	Planear	¿Existe una campaña para divulgar los avances del SGSI en toda la organización?	No.	0
4.2.1.a	Planear	¿Se ha capacitado al personal encargado de la SGSI para enfrentar sus nuevas actividades?	No.	0
4.2.1.a	Planear	¿Existe Documento sensibilización y formación del personal?	No.	0
4.2.1.d	Planear	IDENTIFICACION DE ACTIVOS I		
4.2.1.d	Planear	¿Se ha definido alguna metodología para identificar activos?	Hay un plan para el mantenimiento y calibración de los equipos, tanto para los que inciden en la calidad como los que no.	1
4.2.1.d	Planear	¿Existe inventario de activos (descripción-localización-propietario-grado de seguridad)?	En una hoja de Excel se maneja todo el inventario. Falta establecer la descripción-localización-propietario-grado de seguridad	1
4.2.1.d	Planear	¿Están incluidos los activos intangibles (Imagen Organizacional)?	No.	0
4.2.1.d	Planear	¿Se ha determinado el ciclo de vida útil de los activos?	Sí se maneja el ciclo de vida de los activos desde la parte contable, pero no hay Documentación.	1
4.2.1.d	Planear	¿Existe análisis o árbol de dependencia entre activos?	No.	0
4.2.1.d	Planear	¿Existe Documento Inventario de activos?	La hoja de Excel.	1

Tabla 4. (Continuación)

4.2.1.d	Planear	VALORACION DE ACTIVOS		
4.2.1.d	Planear	¿Existe valoración de activos según la importancia e impacto ante una incidencia basado en CID (cuantitativa y/o cualitativa)?	No.	0
4.2.1.d	Planear	¿Qué Método es empleado para valorar activos (entrevista, encuesta)?	No hay nada documentado, se valoran por el personal gerencial.	0
4.2.1.d	Planear	¿Existe Documento valoración de activos?	No.	0
4.2.1.d	Planear	IDENTIFICACION DE RIESGOS		
4.2.1.d	Planear	¿Se ha identificado áreas que requieren medidas de seguridad?	No	0
4.2.1.d	Planear	¿Existe identificación de riesgos y están asociados a los activos inventariados?	No.	0
4.2.1.d	Planear	¿Existe identificación de riesgos asociados a los activos más críticos?	No.	0
4.2.1.d	Planear	¿Hay Amenazas identificadas que afectan los activos inventariados?	No.	0
4.2.1.d	Planear	¿Existe Análisis de vulnerabilidades de los activos inventariados?	No.	0
4.2.1.d	Planear	¿Se conoce el impacto por la ocurrencia de un riesgo?	No.	0
4.2.1.e	Planear	¿Se ha determinado la probabilidad de ocurrencia de un riesgo?	No.	0
4.2.1.d	Planear	¿Este proceso considera los recursos de la organización?	No.	0
4.2.1.d	Planear	¿Existe Análisis de medidas de seguridad ya implantadas?	No.	0
4.2.1.d	Planear	¿Hay Participación de las diversas áreas de la compañía?	No.	0
4.2.1.d	Planear	¿Existe Documento identificación de riesgos?	No.	0

Tabla 4. (Continuación)

4.2.1.c	Planear	ENFOQUE PARA VALORACION DE RIESGOS		
4.2.1.c	Planear	¿Se ha definido alguna metodología para valorar riesgos?	No.	0
4.2.1.c	Planear	¿Se han estimado los niveles para los riesgos?	No.	0
4.2.1.c	Planear	¿Existe un Documento enfoque para valorar riesgos?	No.	0
4.2.1.f	Planear	GESTION DEL RIESGO		
4.2.1.f	Planear	¿Se han definido acciones frente a los riesgos identificados y valorados?	No.	0
4.2.1.f	Planear	¿Se ha determinado el riesgo residual para cada riesgo identificado y valorado?	No.	0
4.2.1.c,e	Planear	¿Existen criterios definidos para tomar riesgo aceptable?	No.	0
4.2.1.f	Planear	¿Hay Aprobación por dirección para los riesgos aceptable?	No.	0
4.2.1.f	Planear	¿Existe Documento de Aprobación Dirección Gestión de Riesgos?	No.	0
4.2.1.h	Planear	¿Existe Documento de Aprobación Dirección Riesgos residuales?	No.	0
4.2.1.f	Planear	¿Existe Documento matriz de riesgos?	No.	0
4.2.1.g	Planear	SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES		
4.2.1.g	Planear	¿Existe Análisis de controles existentes?	No.	0
4.2.1.g	Planear	¿Existe Análisis y selección de los dominios, objetivos y controles a implantar?	No.	0
4.2.1.g	Planear	¿Se Cumplen los requisitos definidos en procesos de tratamiento de riesgos?	No.	0
4.2.1.g	Planear	¿Se hacen Inversiones en controles proporcionales al impacto del riesgo?	No.	0
4.2.1.g	Planear	¿Existen Controles documentados en procedimientos?	No.	0
4.2.1.g	Planear	¿Hay disponibilidad de recursos para implementar los controles?	No.	0
4.2.1.g	Planear	¿Existe justificación para los objetivos y controles seleccionados y no seleccionados?	No.	0

Tabla 4. (Continuación)

4.2.1.i	Planear	AUTORIZACION PARA IMPLEMENTAR Y OPERAR SGSI		
4.2.1.i	Planear	¿Existe Documento de aprobación por dirección para implementar y operar el SGSI?	Existe un documento aprobado por la Dirección para la implementación y operación solo del SGC	2
4.2.1	Planear	GESTION DE LA CONTINUIDAD DEL NEGOCIO (PCN)		
4.2.1	Planear	¿Están identificados los procesos críticos a recuperar progresivamente?	No.	0
4.2.1	Planear	¿Existe PCN extraído de gestión de riesgos críticos?	No.	0
4.2.1	Planear	¿Se ha puesto a prueba el PCN (cuánto es el tiempo de recuperación mínimo, los ANS se conservan)?	No.	0
4.2.1	Planear	¿Existe comité de emergencia para solucionar las crisis?	No.	0
4.2.1	Planear	¿Existen procedimientos (relacionados a cada situación) establecidos para aplicar en las crisis (indica acciones y sugerencias)?	No.	0
4.2.1	Planear	¿Los procedimientos han sido divulgados y puestos a prueba?	No.	0
4.2.1	Planear	¿Existen registros que documentan la reacción ante la crisis y su respectivo análisis?	No.	0
4.2.1	Planear	Fases PCN: Definición del proyecto (alcance y objetivos de peor escenario) - Análisis de impacto (riesgos, impacto económico) - Selección de estrategias (recursos-salvaguardas a usar) -Desarrollo - Pruebas periódicas y mantenimiento	No.	0
4.2.2	Hacer	IMPLEMENTACION Y OPERACIÓN SGSI		
4.2.2.a,b	Hacer	PLAN DE TRATAMIENTO DE RIESGOS		
4.2.2.a,b	Hacer	¿Existe guía de ejecución del plan para tratamiento de riesgos?	No.	0
4.2.2.h	Hacer	¿Se han definido Procedimientos y controles adicionales para detectar y reaccionar ante incidentes de seguridad en esta fase?	No.	0

Tabla 4. (Continuación)

4.2.2.a,b	Hacer	¿Existe documento informe de plan para tratamiento de riesgos?	No.	0
4.2.2.c	Hacer	IMPLANTACION DE CONTROLES		
4.2.2.c	Hacer	¿Se han definido los responsables de los controles técnicos?	No.	0
4.2.2.c	Hacer	¿Se han definido los responsables de los controles administrativos?	No.	0
4.2.2.d	Hacer	¿Se han definido los indicadores para cada control implantado?	No.	0
4.2.2.d	Hacer	¿Existe un método para medir la eficacia de los controles implantados?	No.	0
4.2.2.h	Hacer	¿Se han implantado controles adicionales ante incidentes de seguridad detectados en esta fase?	No.	0
4.2.2.e	Hacer	¿Se ha hecho sensibilización y divulgación?	No.	0
4.2.2.c	Hacer + Dominios 1-15	¿Existen los procedimientos de los controles del anexo A, correspondientes a 133 controles.	No.	0
4.2.3	Verificar	SEGUIMIENTO Y REVISION SGSI		
4.2.3	Verificar	PROCEDIMIENTOS SEGUIMIENTO Y REVISIÓN		
4.2.3.a,c	Verificar	¿Se hace un análisis periódico de indicadores y su eficacia?	No.	0
4.2.3.b,e	Verificar	¿Se realizan auditorías internas/externas al sistema?	Están establecidas las bases para hacerlas para el SGC.	2
4.2.3.b,e	Verificar	¿Se hace revisión por Dirección de las auditorías?	Falta incorporar lo referente a SGSI.	2
4.2.3.a	Verificar	¿Se hace revisión por Dirección del informe Comité de Gestión?	Falta incorporar lo referente a SGSI.	2
4.2.3.a	Verificar	¿Se hace revisión por Dirección del informe Responsable Seguridad?	Falta incorporar lo referente a SGSI.	2
4.2.3.d	Verificar	¿Se hace revisión periódica por Dirección de valoración de riesgos, riesgo residual, riesgo aceptable?	Falta incorporar lo referente a SGSI.	2
4.2.3.b,e	Verificar	¿Existe un documento auditorías internas?	Procedimiento PR-SGC03 Auditorías Internas de Calidad. Falta incorporar lo referente a SGSI.	2

Tabla 4. (Continuación)

4.2.3.a,b, c,d,e	Verificar	¿Existe un documento de revisión por dirección?	Agenda previa y acta de la revisión por la dirección. Falta incorporar lo referente a SGSI	2
4.2.4	Actuar	MANTENIMIENTO Y MEJORA SGSI		
4.2.4.a,b	Actuar	¿Se ejecutan acciones correctivas, preventivas, mejora?	No.	0
4.2.4.a,b	Actuar	¿Se hace la actualización de riesgos y controles?	No.	0
4.2.4.d	Actuar	¿Se hace la medición de eficacia de acciones implementadas?	No.	0
4.2.4.c	Actuar	¿Existe un documento informe de ejecución de acciones correctivas-preventivas?	No.	0

Fuente: Elaboración propia

5.3 ANÁLISIS DE LA INFORMACIÓN OBTENIDA EN EL CHECK LIST

Para realizar el análisis de los resultados se completó la tabla de valores así:

Tabla 5. Tabla de valores y resultados.

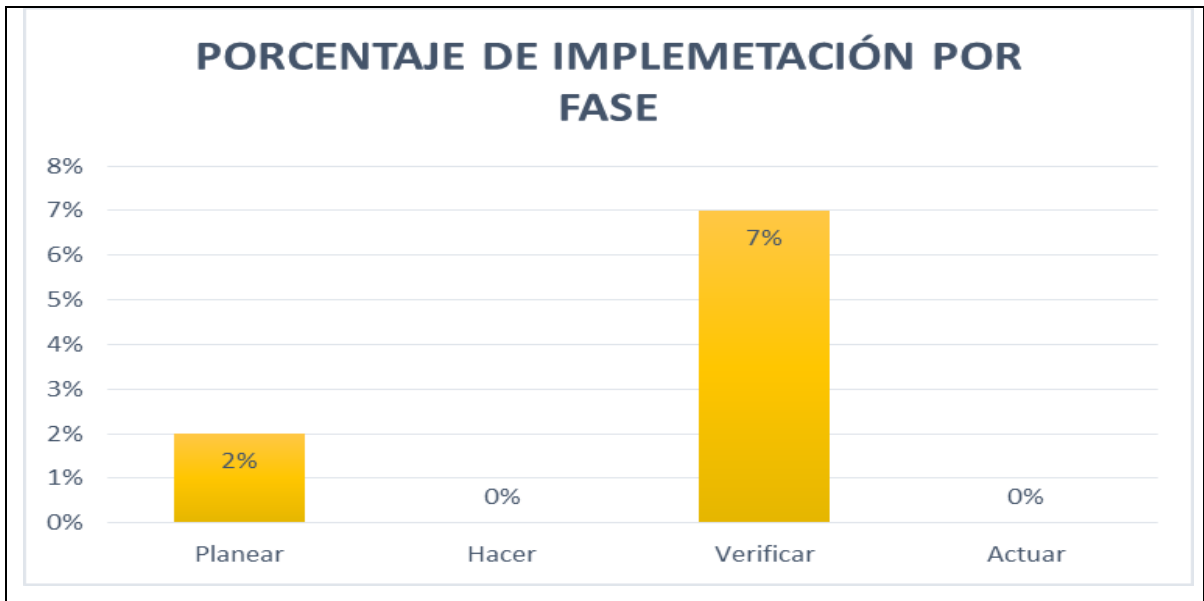
TABLA VALORES Y RESULTADOS						
VALOR % POR FASE	CICLO	# ÍTEMS	SUMA MÁXIMA DE CADA FASE	RESULTADO (suma calificación por ítems)	RESULTADO PROMEDIO	PORCENTAJE DE IMPLEMETACIÓN POR FASE
25%	Planear	74	370	29	0,39	2%
35%	Hacer	10	50	0	0,00	0%
20%	Verificar	8	40	14	1,75	7%
20%	Actuar	4	20	0	0,00	0%
TOTAL						9%

Fuente: Elaboración propia

-Se realizó la sumatoria de las calificaciones obtenidas para cada fase de los ciclos Planear, Hacer, Verificar y Actuar

- Para determinar el promedio de cada ciclo, se toma el resultado de la suma de la calificación por ítem y se divide por el # de ítems; analizando el resultado se puede evidenciar que el nivel de implementación es menor a 2, esto quiere decir que se ha iniciado con el proceso, pero aún no está documentado ni implementado.

Gráficos 1. Resultado del cumplimiento de cada fase PHVA



Fuente: Elaboración propia

De acuerdo con la figura anterior se puede evidenciar el porcentaje de cumplimiento de los requisitos en cada fase de la norma ISO 27001 así:

Para determinar el porcentaje de implementación de cada ciclo del Planear, Hacer, Verificar y Actuar, se utilizó una regla de tres, donde se cogió la suma calificación por ítems y se multiplicó por el valor porcentual asignado al ciclo y se dividió por el valor de la suma máxima del ciclo.

En la Fase Planear: Se tiene un 2% de ítems implementados, esto debido a que el Sistema de Gestión de Calidad ISO 9001 contempla requisitos comunes con la norma ISO 27001 en cuanto a:

- La definición de objetivos estratégicos
- Estructura organizacional
- Identificación de procesos

- Definición de responsabilidades
- Asignación de recursos y responsabilidades

Fase Hacer: Se evidencia un 0% en el nivel de cumplimiento de los requisitos de la ISO 27001

Fase Verificar: Se tiene un 7% de ítems implementados, esto debido a que se cuenta con:

- La definición de las Auditorías internas
- Se han definido los mecanismos para la revisión por la Dirección

Fase Actuar: Se evidencia un 0% en el nivel de cumplimiento de los requisitos de la ISO 27001

Esto indica que la organización aunque tiene implementado un Sistema de Gestión de Calidad, éste solo aporta un 9% de cumplimiento de requisitos al Sistema de Seguridad de la Información, es decir que la Organización requiere es documentar disposiciones para definir los controles de la norma con el fin de minimizar los riesgos de seguridad de la información, y cumplir así con el objeto del presente documento.

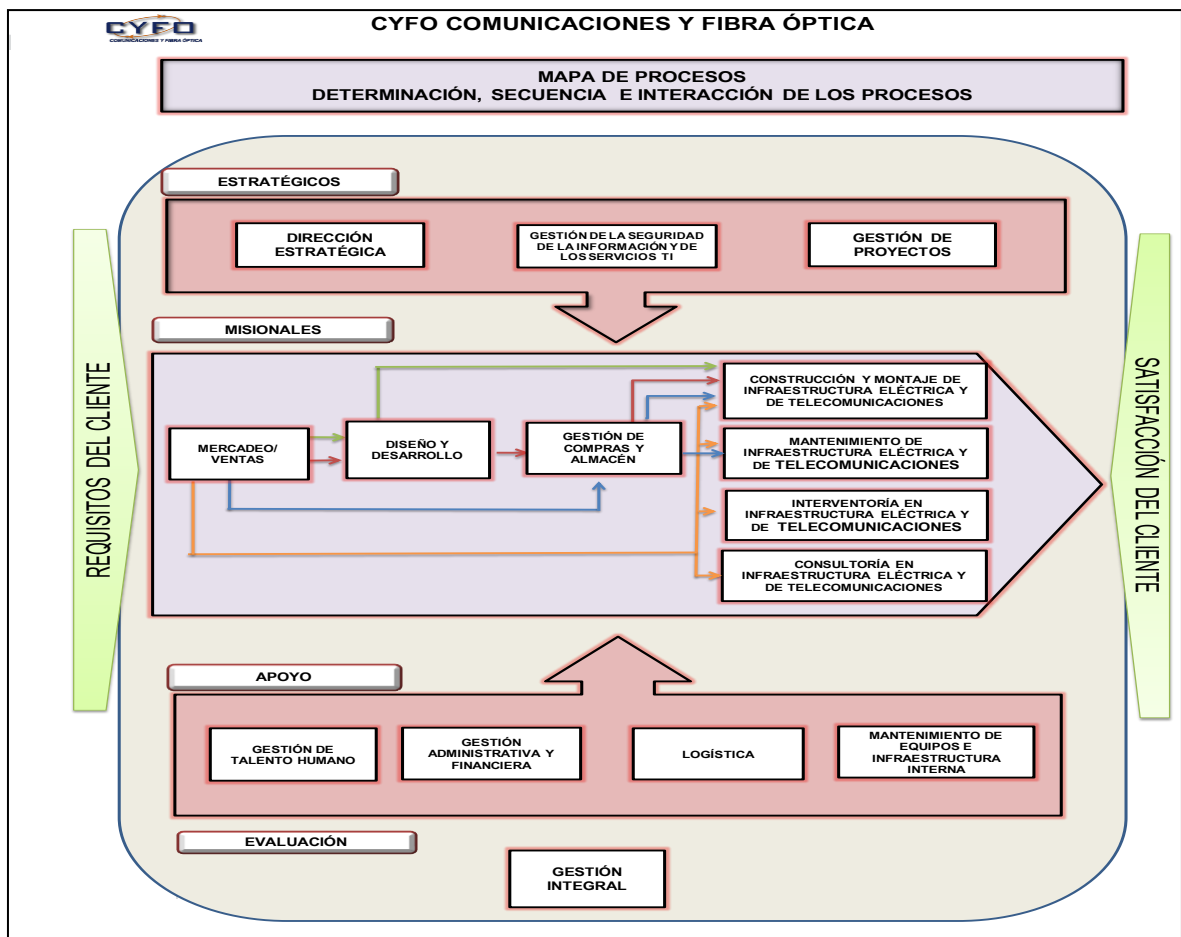
Además de la información recogida en el check List, se identifican los factores internos y externos que se requieren para conocer ampliamente el estado de la organización:

5.3.1 FACTORES INTERNOS

PROCESOS ORGANIZACIONALES

Cyfo Comunicaciones tiene establecido quince (15) procesos que soportan la operación y administración de sus servicios de acuerdo al siguiente mapa

Figura 2: Mapa de procesos.



Fuente: Cyfo Comunicaciones y Fibra Óptica

Los servicios misionales que presta la organización son:

- El diseño y la construcción de redes de fibra óptica, que involucra los estudios preliminares para los diseños, el diseño final y la Construcción de redes de Fibra Óptica bien sea canalizadas o aéreas (utilizando líneas de Alta, Media y Baja Tensión); en infraestructura nueva o existente.
- El Mantenimiento de Redes de Fibra Óptica que comprende las actividades de diagnóstico, mantenimiento preventivo y correctivo a redes de fibra óptica tanto aéreas como canalizadas; ya sea en estado operativo o pasivo de los enlaces.

- Asesoría y Capacitación

Se tiene la capacidad técnica para capacitar y/o asesorar en los campos relacionados con la tecnología de la fibra óptica y cableado estructurado

- Interventoría para Proyectos

Se ejecuta Interventoría a proyectos relacionados con la construcción de redes de fibra óptica (aéreas o canalizadas) y cableado estructurado en todas y cualquiera de sus fases de diseño y construcción.

Para soportar las operaciones de la organización se cuenta con 15 procesos de acuerdo al siguiente esquema:

3 procesos Estratégicos:

- ✓ Dirección Estratégica
- ✓ Gestión de Proyectos
- ✓ Gestión de la Seguridad de la Información y de los Servicios TI

7 procesos Misionales:

- ✓ Mercadeo y Ventas
- ✓ Gestión de Compras y Almacén
- ✓ Diseño de infraestructura eléctrica y de telecomunicaciones
- ✓ Construcción y montaje de infraestructura eléctrica y de telecomunicaciones
- ✓ Mantenimiento de infraestructura eléctrica y de telecomunicaciones
- ✓ Interventoría a infraestructura eléctrica y de telecomunicaciones
- ✓ Consultoría a infraestructura eléctrica y de telecomunicaciones

4 procesos de Apoyo:

- ✓ Gestión del Talento Humano
- ✓ Gestión Administrativa y Financiera
- ✓ Logística
- ✓ Mantenimiento de equipos e infraestructura Interna

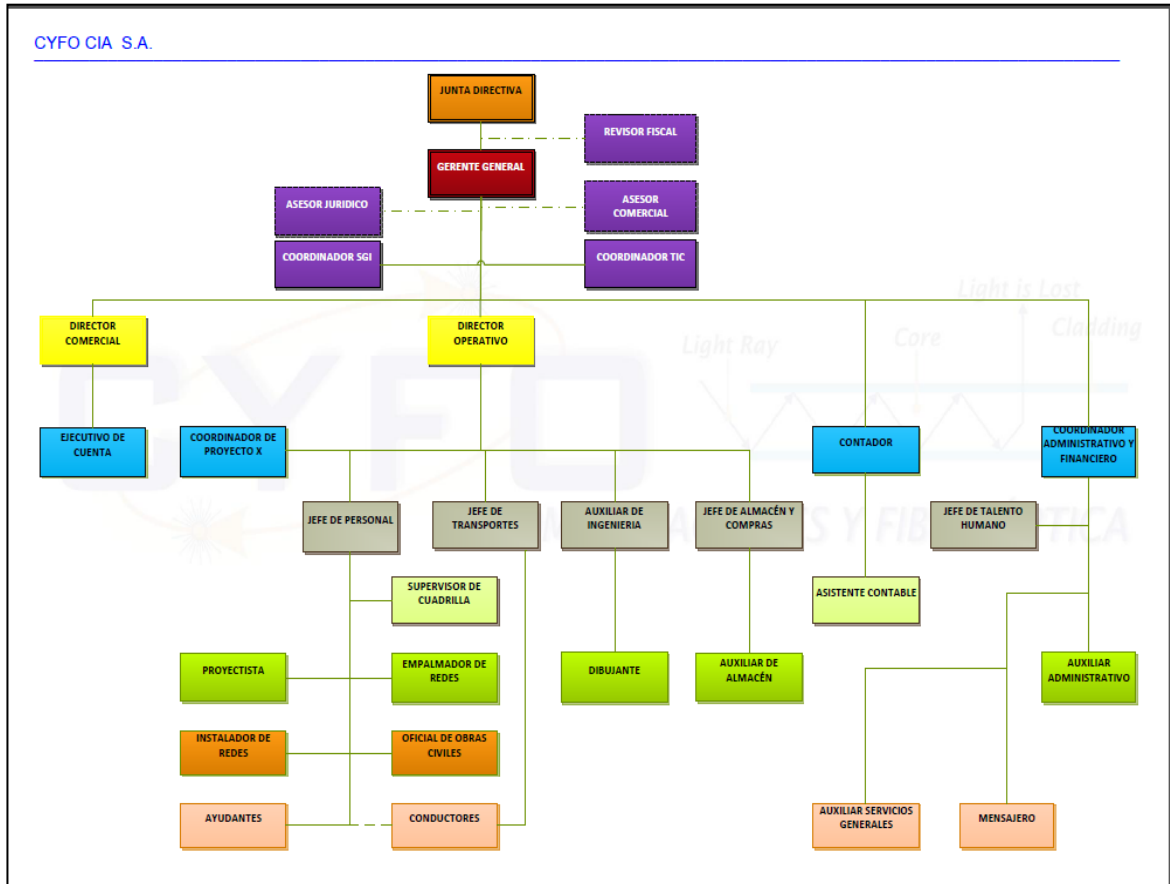
1 proceso de Evaluación:

- ✓ Gestión de Calidad

ESTRUCTURA ORGANIZATIVA

La organización actualmente cuenta con 122 colaboradores entre personal administrativo (24) y personal operativo (98)

Figura 3. Organigrama



Fuente: Cyfo Comunicaciones y Fibra Óptica

A continuación se describen las funciones de cada uno de los cargos del organigrama en:

MANUAL DE FUNCIONES DEL PERSONAL DE LA EMPRESA

a) Gerente General

NOMBRE DEL CARGO: Gerente General

OBJETIVO GENERAL DEL CARGO: Ejecución de labores de dirección, planeación, evaluación y control en la administración, con el fin de garantizar el cumplimiento de las políticas organizacionales, el desarrollo de las actividades y el logro de los objetivos generales de la organización.

CARGO DEL JEFE INMEDIATO: Junta Directiva

PROCESO: Dirección Estratégica

DESCRIPCIÓN DE FUNCIONES

1. Controlar que se ejecute adecuadamente la planeación de las actividades para la ejecución de los Proyectos.
2. Programar y efectuar la gestión para disponer de los recursos necesarios para la ejecución de los proyectos.
3. Aprobar presupuesto pre acordado por los Gerentes Administrativos y Financieros.
4. Presentar las políticas generales de funcionamiento y de las prioridades a atender en cada ejercicio financiero para el cumplimiento de las metas programadas, conforme a la misión y visión Organizacional.
5. Establecer los lineamientos para la elaboración del Plan Operativo de la Organización y para los distintos niveles gerenciales bajo su adscripción.
6. Control de liquidación de gastos de los proyectos ejecutado y en ejecución, indicando las utilidades del mismo.
7. Supervisar las estrategias de ejecución de los distintos programas operativos.
8. Controlar las actividades de carácter financiero y administrativo de la Organización.

9. Crear y mantener buenas relaciones con los clientes, gerentes corporativos y proveedores para mantener el buen funcionamiento de la Organización.
10. Promover el proceso continuo de mejoramiento de la calidad de la Organización.
11. Seleccionar, nombrar y remover a los Colaboradores de acuerdo a su nivel de competencia.
12. Ejercer las demás atribuciones que le concede la Junta Directiva.
13. Responsabilidad en su proceso por el sistema de gestión de calidad (SGC).
14. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

b) Director Operativo

NOMBRE DEL CARGO: Director Operativo

OBJETIVO GENERAL DEL CARGO: Planificar, organizar, dirigir, evaluar y supervisar los programas de operación y gestión, el mantenimiento y expansión de las infraestructuras de telecomunicaciones y eléctricas.

CARGO DEL JEFE INMEDIATO: Gerencia General

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Pre aprobar solicitudes de Gastos de los Coordinadores de Proyectos, Esto teniendo siempre en cuenta la rentabilidad de la Organización.
2. Supervisar y Aprobar las diferentes cotizaciones y licitaciones del Departamento de Licitaciones.
3. Atender las recomendaciones de la Gerencia General
4. Tomar las medidas necesarias para el Cuidado de los Equipos, Materiales y herramientas involucradas en el desarrollo de las actividades de la Compañía, procurando su uso racional y siempre teniendo como meta el beneficio de la Compañía.

5. Vigilar la rentabilidad de todos los proyectos y actividades de la Compañía: antes, durante y luego de su ejecución.
6. Realizar evaluaciones periódicas acerca del cumplimiento de las funciones de los departamentos a su cargo.
7. Gestionar los recursos para la buena realización de los proyectos.
8. Establecer políticas y procesos continuos para la mejora permanente en el desarrollo de los proyectos.
9. Crear y mantener buenas relaciones con los clientes, gerentes corporativos y proveedores para mantener el buen funcionamiento de la empresa.
10. Crear un ambiente en el cual las personas puedan lograr las metas, optimizando los recursos disponibles. En síntesis, propender por que CYFO sea una empresa seductora, tanto para los empleados, como para clientes.
11. Proponer a la Gerencia General, cambios en la estructura administrativa que lleven a lograr los objetivos del Plan Estratégico, optimizando el recurso humano.
12. Supervisar constantemente los indicadores de las actividades a su cargo con el fin de tomar decisiones adecuadas, encaminadas a lograr el óptimo desempeño de la empresa.
13. Investigar nuevos procedimientos, insumos y productos afines con las actividades de la Compañía para ofrecer tecnología de punta a nuestros clientes
14. Proponer vinculación o desvinculación de personal de acuerdo a su rendimiento.
15. Supervisar la adecuada Custodia y Almacenamiento de la Documentación de los diferentes proyectos.
16. Conservar registro de Actas de reuniones de su Dirección.

c) Director Comercial

NOMBRE DEL CARGO: Director Comercial.

OBJETIVO GENERAL DEL CARGO: Mostrar la compañía frente a los entes comerciales que puedan tener posible interés en relaciones comerciales, así como atender las consultas técnicas que surjan de los clientes como de los líderes de los procesos de la organización.

CARGO DEL JEFE INMEDIATO: Gerente General.

PROCESO: Mercadeo y Ventas

DESCRIPCIÓN DE FUNCIONES

1. Uso de información necesaria para la presentación de la compañía, como Brochure, Catálogos de los servicios de la compañía.
2. Con base en las visitas con clientes, sugerir actualizaciones, modificaciones y adiciones al Brochure de la Compañía, página web y cualquier otro medio de difusión de información comercial.
3. Efectuar los contactos con nuevos clientes potenciales para determinar condiciones necesarias afín de iniciar relaciones comerciales.
4. Asesorar la Negociación con clientes y aquellos asuntos que puedan generar beneficios para la compañía.
5. Programar y Ejecutar reuniones con Clientes actuales para conservar y mejorar las relaciones comerciales existentes.
6. Asesorar al área de licitaciones en la presentación y elaboración de ofertas comerciales.
7. Asesorar en la programación de proyectos.
8. Negociación con clientes y proveedores, de asuntos que puedan generar beneficios para la compañía, con aprobación previa de la Gerencia General.
9. Identificar las necesidades de capacitación del personal en su área; así como programar, gestionar y ejecutar las capacitaciones que sean necesarias para el mejor funcionamiento de la Compañía en su área.

10. Ejecutar la estrategia de mercadeo de la compañía compuesta por sus procesos de investigación y participación de mercadeo, licitaciones, comercialización así como las estrategias de mercadeo, de posicionamiento y permanencia.
11. Coordinar la investigación de mercados según lo dispuesto en el PR-MER-01.
12. Responsabilidad en su proceso por el sistema de gestión de calidad (SGC).
13. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

d) Coordinadora Administrativa y Financiera

NOMBRE DEL CARGO: Coordinador Administrativo y Financiero

OBJETIVO GENERAL DEL CARGO: Optimizar el proceso administrativo y financiero de la Organización

CARGO DEL JEFE INMEDIATO: Gerente General

PROCESO: Gestión Administrativa y Financiera

DESCRIPCIÓN DE FUNCIONES

1. Planificar, dirigir y administrar las labores realizadas en el área.
2. Planificar, gestionar y realizar los pagos generados por las distintas actividades y compromisos contraídos por la organización
3. Planificar en función de los recursos asignados en el presupuesto anual y disponibilidad de recursos para la ejecución de actividades, control y evaluación de la disponibilidad financiera de la organización para sus distintas operaciones.
4. Firmar y tramitar documentos con firmas autorizadas a nivel bancario para la apertura de cuentas
5. Elaborar informes técnicos requeridos por la junta directiva sobre las actividades a su cargo y el análisis financiero sobre el patrimonio de la organización.
6. Mantener actualizados los avalúos de los bienes inmuebles y otras patrimoniales de la organización.
7. Trámites y documentación para préstamos realizados por CYFO

8. Análisis y trámite para para préstamos con entidades financieras
9. Elaboración informes de costos de proyectos
10. Asignación y control de tareas a recepción, mensajero y oficios generales
11. Responsabilidad en su proceso por el sistema de gestión de la calidad
12. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial
13. Responsabilidad de todos los activos de la compañía
14. Responsable por la estabilidad y buen funcionamiento de la Infraestructura
15. Responsable por la salud financiera de la Compañía.
16. Tramites de importación y exportación de equipos.
17. Responsabilidad de la Compra y Venta de Activos de la Compañía.

e) Contador

NOMBRE DEL CARGO: Contadora

OBJETIVO GENERAL DEL CARGO: Dirigir el proceso contable de la organización, de tal forma que se cuente con información veraz y confiable. Elaboración y análisis de los estados financieros y ajustes correspondientes de acuerdo a las políticas establecidas y lineamientos estratégicos, dando cumplimiento a la normatividad vigente.

CARGO DEL JEFE INMEDIATO: Gerente General

PROCESO: Gestión Administrativa y Financiera

DESCRIPCIÓN DE FUNCIONES

1. Revisar las conciliaciones bancarias mensuales
2. Controlar cuentas por pagar y por cobrar
3. Gestionar el proceso de facturación
4. Preparar y presentar las declaraciones tributarias del orden nacional y municipal
5. Analizar y depurar las cuentas de balance
6. Generar ajustes mensuales (depreciación, amortización de diferidos, rendimientos financieros, etc.).

7. Elaborar y presentar estados financieros de la compañía
8. Generar y liquidar la nómina mensual, provisiones de prestaciones y pago de aportes a la seguridad social en Sistema UNO (SIESA)
9. Revisar y actualizar del informe de cuentas semanalmente (cuentas por pagar - flujo de caja - cuentas por cobrar - pagos semanales)
10. Generar informes anuales (súper sociedades)
11. Presentar información exógena
12. Suministrar información para el Director Administrativo y financiero para realizar informe de ejecución de proyectos
13. Enviar información del proceso contable a los clientes que la soliciten (Telmex)
14. Realizar la encuesta trimestral y anual de servicios del DANE
15. Presentar informes contables y administrativos
16. Actualizar constantemente el archivo de control de Activos Fijos
17. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
18. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

f) Coordinador TIC

NOMBRE DEL CARGO: Coordinador TIC

OBJETIVO GENERAL DEL CARGO: Dirigir el proceso de programación e implementación de sistemas de información, así mismo mantener estándares para el análisis, diseño y pruebas de sistemas de información de acuerdo a las metodologías establecidas, realizando actividades de actualización y/o mantenimiento de los sistemas de información.

CARGO DEL JEFE INMEDIATO: Gerente General

PROCESO: Gestión Seguridad de la Información

DESCRIPCIÓN DE FUNCIONES

1. Mantener actualizado el antivirus e informar a la Compañía de los virus que se encuentren afectando las redes y las medidas para contrarrestarlos.

2. Realizar el mantenimiento preventivo y correctivo de los equipos de cómputo de la Organización o en su defecto, gestionar su realización por terceros.
3. Mantener actualizada la página de internet de la compañía, de acuerdo a las indicaciones de la gerencia técnica y/o de operaciones.
4. Efectuar la creación y eliminación de las cuentas de correo, de acuerdo a las solicitudes de la administración general
5. Mantener bajo su custodia los equipos accesorios de computación y /o medios informáticos como: discos duros, DVD's de respaldo, software, drivers, cables y otros.
6. Gestionar los insumos necesarios para los equipos de impresión de la organización, como: tonner, cintas, tintas, CD's, DVD's, Stickers y otras; manteniendo un stock mínimo.
7. Llevar informe semanal de eventos presentados en los equipos de cómputo y las actividades realizadas para su reparación.
8. Efectuar las sugerencias para el uso de equipos de cómputo y software, buscando la mayor conveniencia para la Organización.
9. Realizar reporte de las llamadas realizadas nacional e internacionalmente por la línea telefónica IP
10. Realizar copia de seguridad semanal de las grabaciones tomadas en las cámaras de seguridad
11. Revisar el correcto funcionamiento o velar por las mejores opciones de backups para mejorar el rendimiento de la red
12. Atender las inquietudes o problemas técnicos que se le presenten a cualquier departamento de la CIA
13. Velar por el óptimo rendimiento de la red (Internet, equipos, telefonía, entre otros), ya sea internamente o tratando con terceros.
14. Velar por el correcto funcionamiento de las redes de voz de la CIA.
15. Ser el soporte de terceros que requieran realizar labores técnicas en la CIA (UNE, Darsoftware, Sip telecomunicaciones, entre otras)
16. Responsabilidad en su proceso por el sistema de gestión de la calidad

17. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial

g) Coordinador del SGI

NOMBRE DEL CARGO: Coordinador del Sistema de Gestión Integral

OBJETIVO GENERAL DEL CARGO: Estructurar y mantener debidamente actualizado y en operación el sistema integral de gestión de la calidad con base en los requisitos establecidos en las normas ISO 9001, 2007 Y 20000-1 generando acciones que permitan el mejoramiento de la eficacia de los procesos productivos y administrativos, conducentes a lograr la satisfacción del cliente final.

CARGO DEL JEFE INMEDIATO: Gerente General

PROCESO: Gestión de la Calidad

DESCRIPCIÓN DE FUNCIONES

1. Liderar los procesos de revisión por la dirección, reportando al comité de calidad periódicamente, mediante informes ejecutivos, el desempeño del SGC y las necesidades de mejora.
2. Participar o liderar grupos interdisciplinarios del S.G.C., como evaluación y selección de proveedores y evaluación de la competencia del personal.
3. Liderar los procesos de auditoria interna, manteniendo la competencia como "auditor líder" y formando y entrenando cuando se requiera a los auditores internos de calidad
4. Liderar o "ser facilitador" de las actividades para establecer, implementar, mantener y mejorar los procesos del SGC.
5. Concientizar a todos los niveles de la organización en el cumplimiento de los requisitos del cliente, los legales y los organizacionales
6. Liderar las actividades o "ser facilitador" de los "grupos de mejora"
7. Coordinar las actividades para el control de los documentos internos, externos y registros de calidad de todos los procesos del SGC.

8. Coordinar las actividades para que todos los procesos tomen las acciones correctivas, preventivas y de mejora necesarias para lograr la eficacia del SGC, incluida las peticiones, quejas y reclamos de los clientes.
9. Realizar actividades de seguimiento y medición del plan estratégico (Objetivos corporativos), del plan estratégico de la calidad (Objetivos de calidad) y de la satisfacción del cliente.
10. Responsabilidad en su proceso por el sistema de gestión de la calidad
11. Presentar al Comité de calidad, los informes de la revisión de los resultados de la satisfacción de los clientes internos y externos
12. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial

h) Ejecutivo de cuentas

NOMBRE DEL CARGO: Ejecutivo de cuentas

OBJETIVO GENERAL DEL CARGO: Obtener del mercado la mayor cantidad posible de solicitudes de ofertas (por parte de los clientes habituales y de los potenciales); que sean susceptibles de ser presentadas de manera oportuna y que puedan ser elaboradas, presentadas, evaluadas, ejecutadas y financiadas por la Organización.

CARGO DEL JEFE INMEDIATO: Director Comercial

PROCESO: Mercadeo y Ventas

DESCRIPCIÓN DE FUNCIONES

1. Entregar cuentas de gastos efectuados, como máximo 3 días después de haber llegado de viaje
2. Verificar que todo su grupo porte los documentos de identidad, especialmente carnet y aportes parafiscales
3. Asesorar a los directores de proyecto para negociar condiciones de ejecución, determinar y gestionar requisitos necesarios para el inicio de los trabajos, como garantías, pólizas, etc.

4. Asesorar al área de licitaciones respecto a la calificación de la compañía ante los proveedores
5. Asesorar el proceso de búsqueda, lectura de pliegos y realización de las cotizaciones de acuerdo a las solicitudes del cliente y las indicaciones de su superior. Lo anterior a través del control de ofertas y de las obras en ejecución.
6. Buscar licitaciones en internet, prensa y /o llamadas a los contactos comerciales.
7. Calificación de la Organización ante todos los proveedores potenciales.
8. Control de los contratos, tanto para clientes como para proveedores (con copia a contabilidad) llevando archivo físico y adjuntando las pólizas correspondientes a cada uno de ellos.
9. Coordinar el proceso de búsqueda, lectura de pliegos y realización de las cotizaciones de acuerdo a las solicitudes del cliente y las indicaciones de su superior. Lo anterior a través del control de ofertas y de las obras en ejecución.
10. Efectuar los contactos con el cliente para negociar condiciones de ejecución, determinar y gestionar requisitos necesarios para el inicio de los trabajos, como garantías, pólizas, etc.
11. Entrega de información de ofertas adjudicadas y / o aprobadas a contabilidad
12. Establecer los modelos y efectuar la revisión de los informes finales de ejecución de obra.
13. Llevar el control de las ofertas a presentar, presentadas y adjudicadas.
14. Manejo de información necesaria para la ejecución de las ofertas, como brochure, certificaciones de obra y documentos legales
15. Manejo de los archivos magnéticos e impresos de las licitaciones presentadas y ejecutadas
16. Mantener actualizado el brochure de la compañía
17. Negociación de los valores y condiciones finales de las ofertas, previa consulta e instrucciones de la presidencia
18. Presentación de la oferta y registro de la recepción de las mismas

19. Realizar las licitaciones y cotizaciones menores a las cuales aplica la compañía, reuniendo la documentación legal y cálculo de precios.
20. Revisar las actividades para la planeación y ejecución de los proyectos, de manera conjunta con los directores de proyecto
21. Revisión documental para determinar si la Organización aplica a las ofertas que presenta
22. Seguimiento a las ofertas y fechas de adjudicación
23. Solicitud y gestión ante el cliente para la emisión de certificaciones de obra y mantener comunicación con el cliente para recibir retroalimentación sobre satisfacción, una vez concluidos los trabajos
24. Subsanación de documentos y aclaración de inquietudes de las ofertas presentadas
25. Tramitar pólizas y documentos necesarios para la firma de contratos
26. Responsabilidad en su proceso por el Sistema de Gestión de la Calidad
27. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial

i) Jefe de Talento Humano

NOMBRE DEL CARGO: Jefe de Talento Humano

OBJETIVO GENERAL DEL CARGO: Seleccionar, reclutar y administrar los recursos humanos que participan en la operación de la Organización, así como velar por su capacitación, seguridad y bienestar a fin de lograr el desarrollo integral de todos los colaboradores.

CARGO DEL JEFE INMEDIATO: Coordinadora Administrativa y Financiera

PROCESO: Gestión Administrativa y Financiera

DESCRIPCIÓN DE FUNCIONES

1. Llevar a cabo el procedimiento de contratación de personal: Convocar, seleccionar, realizar pruebas de aptitud cuando aplique, entrevista, verificar el

cumplimiento de la documentación requerida (hoja de vida con soportes) y verificar las referencias.

2. Realizar el proceso de contratación del personal: Realizar afiliaciones de ARP, EPS, AFP, Parafiscales, seguro de accidentes personales y vida grupo.
3. Establecer y dirigir programas de inducción, entrenamiento y capacitación tanto al personal que se encuentra vinculado como al que ingresa.
4. Velar por el cumplimiento de las normas de seguridad industrial y salud ocupacional establecidos por la ley y por la empresa: Programa de S.O, Panorama de Factores de Riesgo, Planes de Acción, Comité Paritario de S.O, Reglamento de Higiene y Seguridad, Políticas de salud ocupacional.
5. Diseñar y ejecutar el programa anual de capacitación.
6. Mantener actualizado el manual de funciones de la compañía con las respectivas descripciones de cargos.
7. Realizar análisis de competencias cuando se vincula un colaborador a la compañía y anualmente.
8. Evaluar la eficiencia de las capacitaciones.
9. Promover campañas de promoción y prevención a todos los colaboradores con apoyo de las EPS.
10. Exigir a los subcontratistas el cumplimiento de las normas establecidas en seguridad industrial y salud ocupacional: Afiliaciones al SGS, programas de inducción y capacitación, permisos y estándares de seguridad.
11. Realizar la evaluación de las condiciones de trabajo.
12. Gestionar la evaluación de desempeño anual para cada uno de los colaboradores en compañía con los jefes inmediatos.
13. Realizar actividades de gestión ambiental: Programa de reciclaje de residuos.
14. Conformar brigadas de emergencia: Incendios, primeros auxilios y evacuación y rescate.
15. Realizar controles periódicos de los afiliados al S.G.S.S.S para evitar inconsistencias en el momento de solicitar los servicios a las diferentes EPS por parte de los empleados.

16. Tramitar ante el área contable las incapacidades de los empleados para solicitar el respectivo pago ante las EPS.
17. Reportar las novedades al proceso contable.
18. Velar por el bienestar laboral de todos los empleados de la Compañía.
19. Implementar y entregar formatos, registros y estadísticas para toma de decisiones.
20. Enviar información del proceso de Talento Humano a los clientes que la soliciten.
21. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
- 22 Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

j) Jefe de Personal

NOMBRE DEL CARGO: Jefe de Personal

OBJETIVO GENERAL DEL CARGO: Planificar, organizar, dirigir, controlar, evaluar y supervisar el talento humano operativo de la compañía a fin de dar cumplimiento a los objetivos propuestos en la ejecución de los proyectos.

CARGO DEL JEFE INMEDIATO: Director Operativo

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Funciones Permanentes

01. Planificar y dimensionar el talento humano operativo requerido o necesario para la ejecución de los proyectos.
02. Proponer la vinculación o desvinculación de personal de acuerdo a su rendimiento o de acuerdo a las necesidades de la compañía.
03. Hacer seguimiento a las funciones de los colaboradores subalternos y tomar acciones correctivas de ser necesario.
04. Solicitar capacitaciones al personal que según su criterio requiera elevar o mejorar sus competencias para el desarrollo de sus funciones.

05. Mantener informado constantemente a la dirección operativa del estatus o novedades del personal operativo.
06. Controlar permanentemente el ingreso y salida del personal operativo y asegurar el diligenciamiento del formato de ausentismo en los casos que aplican.
07. Registrar permanentemente el tiempo causado por cada colaborador operativo según los centros de costo.
08. Administrar y controlar la utilización de tiempo extra el personal para la ejecución del proyecto.
09. Registrar en forma permanente el tiempo extraordinario causado por cada colaborador de la compañía y presentar periódicamente un informe con el tiempo que se deberá compensar a cada colaborador ya sea en dinero o en especie.
10. Gestionar en conjunto con la Jefatura de Talento humano, las solicitudes de vacaciones, permisos y tiempos compensatorios del personal operativo.
11. Programar y organizar permanentemente las labores a ejecutar diariamente por el personal operativo.
12. Realizar diariamente la liquidación o cierre de las ejecuciones de obras civiles locales, recibir formatos de campo diligenciados, chequear las cantidades de obra cotizados vs. Las ejecutadas, resolver imprevistos y entregar a la coordinación de los proyectos la información precisa para la liquidación de las actas de entrega de servicios en proyectos locales.
13. Controlar y validar la ejecución de obras adicionales para proyectos locales.
14. Hacer interventoría interna a los proyectos locales antes de hacer entrega al cliente.
15. Llevar un registro fotográfico de la ejecución y producto final de los proyectos locales.
16. Hacer veeduría permanente en la entrega y devolución de materiales (asegurar el correcto despacho y devolución de materiales a almacén).
17. Gestionar por medio de la jefatura de compras y almacén, las herramientas, equipos, materiales e insumos que a su juicio sean necesarios para la ejecución de los proyectos.

18. Tomar las medidas necesarias para el Cuidado de los Equipos, Materiales y herramientas involucradas en el desarrollo de las actividades de la Compañía, procurando su uso racional y siempre teniendo como meta el beneficio de la Compañía.
19. Ejecutar las actividades, procedimientos y disposiciones del sistema de gestión de la calidad, salud ocupacional y seguridad industrial.
20. Mantener un ambiente de trabajo seguro y adecuado para la ejecución del proyecto, exigiendo la utilización de los EPP.
21. Mantener el orden y aseo en los lugares de trabajo y áreas afectadas por los mismos.
22. Reportar oportunamente tanto accidentes como incidentes de trabajo al Gestión del Talento Humano y a la ARP respectiva.
23. Responsabilidad en su proceso por el sistema de Gestión de la Calidad.
24. Llevar un control diario de los PNC, hacer seguimiento, archivado, procesamiento y cierre de todos los PNC que surjan.
25. Responsabilidad en su proceso por la salud Ocupacional y seguridad industrial
26. Hacer reuniones periódicas con el personal operativo con el fin de transmitir las políticas y directrices de la dirección operativa, evaluar el desempeño de los proyectos y escuchar las peticiones de los colaboradores.

k) Jefe de Transporte

NOMBRE DEL CARGO: Jefe de Transporte

OBJETIVO GENERAL DEL CARGO: Velar por el excelente estado mecánico y el uso eficiente de los medios de transporte así como de su disponibilidad.

CARGO DEL JEFE INMEDIATO: Director Operativo

PROCESO: Logística

DESCRIPCIÓN DE FUNCIONES

1. Administrar de acuerdo a prioridades y disponibilidad, las solicitudes de asignación de vehículos.
2. Llevar bitácora de la asignación de vehículos y sus incidencias.
3. Realizar la gestoría de los trámites fiscales relativos al equipo de transporte.
4. Mantener un registro individualizado de cada vehículo que muestre los servicios, reparaciones, kilometraje y en caso de siniestros (Hoja de vida de cada equipo automotor)
5. Realizar los trámites necesarios para la adquisición de vales de gasolina y llevar un registro de su uso.
6. Efectuar la asignación (despachos) de vehículos, equipos y herramientas necesarias para su normal funcionamiento.
7. Recepción de vehículos, equipo y herramientas.
8. Informar de malos tratos o situaciones que afecten el equipo especial o vehículos, de manera inmediata a su recepción.
9. Informar directamente a la gerencia, en caso de que algún superior pretenda pasar por alto cualquiera de las funciones encomendadas al cargo o el uso indebido de equipo y /o vehículos de la Compañía.
10. Realizar mantenimiento preventivo a los vehículos de la flotilla de la Organización periódicamente.
11. Ejecutar de manera eficiente y rápida, el mantenimiento correctivo de vehículos de la compañía; en el evento en el que éstos resulten afectados, debe informar al administrador general de manera inmediata.
12. Gestionar las compras y/o servicios necesarios para la ejecución de los mantenimientos preventivos y correctivos de los vehículos.
13. Mantener control del vencimiento de seguros y certificados de revisiones técnico mecánicas; programando su renovación, por lo menos con 8 días de anterioridad al vencimiento e informando a los Jefes de área que tengan estos vehículos bajo su responsabilidad.
14. Apertura y cierre de la bodega en los horarios programados.
15. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).

16. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

I) Jefe de Compras y almacén

NOMBRE DEL CARGO: Jefe de Almacén y Compras

OBJETIVO GENERAL DEL CARGO: Atender los requerimientos de las diferentes áreas de la organización, supervisar el proceso de almacenamiento y despacho de materiales, suministros y equipos, revisando, organizando y distribuyendo los mismo, a fin de mantener los niveles de inventarios necesarios para garantizar un servicio eficiente a la Organización.

CARGO DEL JEFE INMEDIATO: Director Operativo

PROCESO: Gestión de Almacén y compras

DESCRIPCIÓN DE FUNCIONES

1. Llevar el inventario general de la bodega: equipo, herramienta y material; reportando periódicamente cualquier diferencia entre las existencias y el inventario general.
2. Despacho de equipo, herramienta y material de acuerdo a las solicitudes diarias.
3. Recepción de equipo, herramienta y material de acuerdo a las solicitudes diarias.
4. Informar de malos tratos o situaciones que afecten el equipo, herramienta o material, de manera inmediata al momento de su recepción.
5. Informar directamente a la Gerencia o Dirección Operativa, en caso de que algún superior pretenda pasar por alto cualquiera de las funciones encomendadas al cargo o el uso indebido de equipo, herramienta y materiales de la Compañía.
6. Llevar inventario de cables con el respectivo abscisado y el registro de la obra en la cual fue utilizado.
7. Mantener en buen estado los equipos, herramientas y material a su cargo en la bodega.

8. Gestionar la relación, el contrato o convenio y el rendimiento de los proveedores.
9. Elaboración de órdenes de compras y entrada de facturas de las compras autorizadas en comité de compras.
10. Búsqueda continua de nuevos proveedores que ofrezcan mayores ventajas competitivas.
11. Legalización de consumos por parte de los grupos de mantenimiento.
12. Análisis de intención de consumo, interpretación de compras a realizar y manejo de stocks.
13. Coordinar con el gerente general las compras internacionales.
14. Legalización de facturas externas.
15. Cumplir con las disposiciones contenidas en los contratos que firme CYFO con sus clientes, en cuanto al almacenamiento, manejo y control de materiales, herramientas y equipos.
16. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
17. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

m) Auxiliar de Ingeniería

NOMBRE DEL CARGO: Auxiliar de Ingeniería

OBJETIVO GENERAL DEL CARGO: Servir de apoyo al Director de Proyecto en la coordinación de todos los trabajos relacionados con el tendido de redes tanto de fibra óptica como conductores eléctricos de media, alta y extra-alta tensión en cualquier parte del mundo.

CARGO DEL JEFE INMEDIATO: Director Operativo

PROCESO: Diseño y Desarrollo

DESCRIPCIÓN DE FUNCIONES

1. Programar con el Director de Proyecto las visitas de obra.

2. Apoyar la planificación de los proyectos en cuanto a logística, transporte, comunicaciones, materiales, herramientas y talento humano, así como cualquier recurso adicional para la culminación de los trabajos y lleva un registro de la misma en el formato establecido.
3. Elaborar los cronogramas de ejecución del proyecto, mantenerlos actualizados, proponer acciones correctivas si es necesario y mantenerlos disponibles tanto para el cliente como para los jefes.
4. Calcular la provisión necesaria en dinero para la ejecución y terminación de la obra y presentarla al Director de Proyecto.
5. Efectuar constante seguimiento de las actividades realizadas durante la ejecución del proyecto.
6. Apoyar la gestión de permisos para la intervención de espacios públicos y privados ante entidades gubernamentales/privadas.
7. Hacer seguimiento a los sub-contratistas para la ejecución de obras civiles.
8. Verificar y controlar la utilización de tiempo extra el personal para la ejecución del proyecto.
9. Velar constantemente por la correcta utilización de herramientas y equipos tanto del personal subalterno como las asignadas al cargo.
10. Legalizar los gastos causados durante o por la ejecución del proyecto de acuerdo a las instrucciones de contabilidad.
11. Hacer seguimiento de los proyecto en lo referente a facturación, ejecución y programación de obras.
12. Mantener el orden y aseo en los lugares de trabajo y áreas afectadas por los mismos.
13. Elaborar los informes de Costos Vs Facturación de los proyectos ejecutados y entregarlos al Directo de Proyecto.
14. Ejecutar periódicamente la copia de respaldo (Backus) de la información generada durante el cumplimiento de las funciones. Este respaldo se realiza en el ordenador - servidor de las instalaciones principales y de acuerdo a las instrucciones de análisis de sistemas.

15. Mantener un ambiente de trabajo seguro y adecuado para la ejecución del proyecto, exigiendo la utilización de los EPP.
16. Mantener informado al Director de Proyecto, del avance o estado del proyecto en ejecución.
17. Ejecutar las actividades, procedimientos y disposiciones del sistema de gestión de la calidad, salud ocupacional y seguridad industrial.
18. Mantener una buena comunicación con el representante del cliente y proponer soluciones a los problemas presentados.
19. Revisar y validar todos los documentos establecidos en el proceso de ejecución.
20. Responsabilidad en su proceso por el sistema de Gestión de la Calidad (SGC).
21. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

n) Asistente de Contabilidad

NOMBRE DEL CARGO: Asistente Contable

OBJETIVO GENERAL DEL CARGO: Efectuar asientos de las diferentes cuentas, revisando, clasificando y registrando documentos a fin de mantener actualizados los movimientos contables que se realizan en la Organización. Apoyar en la elaboración de informes contables y financieros de manera veraz y eficiente de acuerdo a lo señalado por la normatividad vigente y que sean solicitados por la Contadora y/o demás dependencias.

CARGO DEL JEFE INMEDIATO: Contadora

PROCESO: Gestión Administrativa y Financiera

DESCRIPCIÓN DE FUNCIONES

1. Manejar y controlar de la caja menor administrativa
2. Digitar los documentos contables como recibos de caja, comprobantes de egreso, legalizaciones, notas contables
3. Liquidar la nómina en Excel

4. Manejar y archivar los documentos del proceso contable
5. Generar y entregar los desprendibles de nómina
6. Actualizar el archivo de cuentas por pagar
7. Controlar el movimiento de las cuentas bancarias
8. Conciliar las pólizas de accidentes personales y vida grupo
9. Apoyar la depuración y análisis de las cuentas de balance
10. Gestionar el cobro y recaudo de cartera
11. Generar, entregar y verificar los cheques para el pago a proveedores y terceros
12. Realizar conciliaciones bancarias
13. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
14. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

ñ) Auxiliar de almacén

NOMBRE DEL CARGO: Auxiliar de Almacén

OBJETIVO GENERAL DEL CARGO: Asistir en las actividades de almacén, recibiendo, revisando y organizando los materiales y equipos, a fin de despachar oportunamente los requerimientos de las áreas de la Organización.

CARGO DEL JEFE INMEDIATO: Jefe de Almacén y Compras

PROCESO: Gestión de Compras y Almacén

DESCRIPCIÓN DE FUNCIONES

1. Reportar al jefe de almacén y compras si se agotan suministros y posibles daños en la herramienta
2. Mantener en buen estado las herramientas y estar pendiente de los mantenimientos
3. Mantener el control de salidas y préstamos temporales diariamente
4. Legalización de consumos por parte de los grupos de mantenimiento en el momento en que el jefe de almacén este realizando otras actividades

5. Llevar el inventario general de la bodega: equipo, herramienta y material; reportando diariamente cualquier diferencia entre las existencias y el inventario general
6. Reportar semanalmente el estado de las existencias de material y efectuar los pedidos (quincenales), de acuerdo al stock mínimo establecido y a las instrucciones del superior.
7. Efectuar despachos de equipo, herramienta y material para obras externas; de acuerdo a las solicitudes escritas
8. Despacho de equipo, herramienta y material; de acuerdo a las solicitudes diarias.
9. Recepción de equipo, herramienta y material; de acuerdo a las solicitudes diarias.
10. Informar de malos tratos o situaciones que afecten el equipo, herramienta o material, de manera inmediata a su recepción.
11. Informar directamente a la presidencia, en caso de que algún superior pretenda pasar por alto cualquiera de las funciones encomendadas al cargo o el uso indebido de equipo, herramienta y materiales de la compañía.
12. Llevar inventario de cables con el respectivo abcisado y el registro de la obra para la cual fue utilizado
13. Mantener en buen estado los equipos, herramientas y material a su cargo en la bodega.
14. Programación del mantenimiento preventivo de equipo y herramienta, de acuerdo a las recomendaciones del fabricante
15. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
16. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

o) Auxiliar Administrativo

NOMBRE DEL CARGO: Auxiliar Administrativa

OBJETIVO GENERAL DEL CARGO: Brindar soporte administrativa para el correcto funcionamiento de los procesos operativos y administrativos de la compañía

CARGO DEL JEFE INMEDIATO: Coordinadora Administrativa y Financiera

PROCESO: Gestión Administrativa y Financiera

DESCRIPCIÓN DE FUNCIONES

1. Operar la central telefónica, trasmitiendo los mensajes oportunamente y dejar registro.
2. Recibir, revisar, radicar y registrar la documentación que ingrese y que salga de la compañía.
3. Mantener actualizado los datos personales (Dirección, teléfonos y correos) del personal activo de la Organización.
4. Actualizar y verificar la base de datos proveedores.
5. Gestión de los registros fotográficos (Descargar y enviar a los interventores de Telmex).
6. Distribuir los materiales, útiles y elementos necesarios.
7. Digitalizar control de actividades diarias del personal operativo.
8. Coordinar y realizar las reservas para tiquetes aéreos.
9. Elaborar correspondencia como certificados laborales, remites, etc.
10. Gestionar proyectos de tipo administrativo entre las diferentes entidades estatales.
11. Orientar al usuario que acuda a la recepción, con buen trato y calidez.
12. Mantener adecuada discrecionalidad en el manejo de la información y los documentos a su cargo.
13. Realizar un back Up con toda la información actualizada en la computadora.
14. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).

15. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

p) Servicios Generales

NOMBRE DEL CARGO: Auxiliar de servicios generales

OBJETIVO GENERAL DEL CARGO: Realizar tareas de apoyo y mantenimiento de la infraestructura en lo relativo a la higiene y conservación de las instalaciones de la organización, necesarios para el buen funcionamiento de la Organización.

CARGO DEL JEFE INMEDIATO: Coordinadora Administrativa y financiera

PROCESO: Gestión Administrativa y Financiera

DESCRIPCIÓN DE FUNCIONES

1. Aseo integral de las oficinas, mezanine, zona de parqueo, almacén, recepción, cocina, áreas comunes, fachada y antejardín.
2. Aseo integral de los baños.
3. Limpieza total de los vidrios, puertas, ventanas y cielo raso.
4. Limpieza permanente de sillas, muebles y demás elementos de la organización.
5. Preparación de bebidas (café, aromáticas, jugos).
6. Velar por unas condiciones óptimas en cuanto a orden y aseo de las oficinas.
7. Realizar tareas que le sean asignadas por su jefe inmediato y así garantizar un trabajo de calidad
8. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
9. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

q) Mensajero

NOMBRE DEL CARGO: Mensajero

OBJETIVO GENERAL DEL CARGO: Atender los requerimientos oportunamente en los trámites administrativos y diversas encomiendas dentro y fuera de la

Organización, utilizando los medios adecuados para cumplir con la entrega oportuna y en forma segura.

CARGO DEL JEFE INMEDIATO: Coordinadora Administrativa y Financiera

PROCESO: Gestión Administrativa y Financiera

DESCRIPCIÓN DE FUNCIONES

1. Realizar las diligencias de la manera más rápida y eficiente posible.
2. Realizar pagos y consignaciones.
3. Gestionar trámites diversos.
4. Entregar facturas a clientes.
5. Realizar encuestas de satisfacción al cliente.
6. Entregar licitaciones en otras ciudades cuando se requiera.
7. Apoyar actividades administrativas.
8. Conducir de manera adecuada y cuidar el vehículo asignado para el cumplimiento de sus funciones.
9. Realizar el control pre operativo del vehículo.
10. Diligenciar el registro "Control de actividades diarias y/o vehículos" y entregarlo al Jefe de Transporte.
11. Verificar el estado del vehículo al iniciar y al finalizar la jornada, verificando especialmente: nivel de gasolina (1/4 mínimo), nivel de aceite, batería y llantas.
12. Informar con dos semanas de anterioridad, del vencimiento de los documentos necesarios para la movilización del vehículo.
13. Informar de cualquier daño o avería del vehículo de manera inmediata al Jefe de Transporte.
14. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
15. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

r) **Coordinador de Proyectos**

NOMBRE DEL CARGO: Coordinador de Proyectos

OBJETIVO GENERAL DEL CARGO: Coordinar todos los trabajos relacionados con el tendido de redes tanto de fibra óptica como conductores eléctricos de media, alta y extra-alta tensión en cualquier parte del mundo.

CARGO DEL JEFE INMEDIATO: Director Operativo

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Programación con los representantes del cliente las visitas de obra.
2. Planificar los proyectos externos en cuanto a logística, transporte, comunicaciones, materiales, herramientas y talento humano, así como cualquier recurso adicional para la culminación de los trabajos y lleva un registro de la misma en el formato establecido.
3. Elaborar los cronogramas de ejecución del proyecto, mantenerlos actualizados, tomar acción correctiva si es necesario y mantenerlos disponibles tanto para el cliente como para los jefes.
4. Gestionar el talento humano: definir la competencia, documentación requerida, Equipo de Protección Personal (EPP) y hacer la solicitud a Gestión del Talento Humano
5. Preparar la provisión necesaria en dinero para la ejecución y terminación de la obra y enviarla por escrito a la dirección operativa y/o a la gerencia.
6. Gestionar por medio de la jefatura de compras y almacén las herramientas, equipos operativos, repuestos, materiales e insumos necesarios para la ejecución del proyecto.
7. Efectuar constante seguimiento de las actividades realizadas durante la ejecución del proyecto.
8. Gestión de permisos para la intervención de espacios públicos y privados ante entidades gubernamentales/privadas.
9. Búsqueda y negociación con sub-contratistas para la ejecución de obras civiles.
10. Administrar y controlar la utilización de tiempo extra el personal para la ejecución del proyecto y llevar registro detallado del mismo.

11. Velar constantemente por la correcta utilización de herramientas y equipos tanto del personal subalterno como las asignadas al cargo.
12. Legalizar los gastos causados durante o por la ejecución del proyecto de acuerdo a las instrucciones de contabilidad.
13. Continúa comunicación con los funcionarios del cliente en lo referente a facturación, ejecución y programación de obras.
14. Hacer seguimiento a las funciones de los colaboradores subalternos y tomar acción correctiva de ser necesario.
15. Mantener el orden y aseo en los lugares de trabajo y áreas afectadas por los mismos.
16. Elaborar los informes de Costos Vs Facturación de los proyectos ejecutados y entregarlos a la dirección operativa.
17. Reportar oportunamente tanto accidentes como incidentes de trabajo al Gestión del Talento Humano y a la ARP respectiva del proyecto en ejecución.
18. Ejecutar periódicamente la copia de respaldo (Backus) de la información generada durante el cumplimiento de las funciones. Este respaldo se realiza en el ordenador - servidor de las instalaciones principales y de acuerdo a las instrucciones de análisis de sistemas.
19. Mantener un ambiente de trabajo seguro y adecuado para la ejecución del proyecto, exigiendo la utilización de los EPP.
20. Mantener informado constantemente al representante del cliente y a la dirección operativa del avance o estado del proyecto en ejecución.
21. Ejecutar las actividades, procedimientos y disposiciones del sistema de gestión de la calidad, salud ocupacional y seguridad industrial
22. Mantener una buena comunicación con el representante del cliente y solucionar los problemas presentados.
23. Revisar y validar todos los documentos establecidos en el proceso de ejecución.
24. Responsabilidad en su proceso por el sistema de Gestión de la Calidad (SGC).

25. Responsabilidad en su proceso por la salud ocupacional y seguridad de la industrial.

s) Supervisor de cuadrillas

NOMBRE DEL CARGO: Supervisor de cuadrilla

OBJETIVO GENERAL DEL CARGO: Coordinar y supervisar las actividades necesarias para la ejecución de montajes y mantenimientos y el uso eficiente de los recursos.

CARGO DEL JEFE INMEDIATO: Coordinador de proyectos

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Supervisar y controlar las actividades del personal a cargo.
2. Establecer técnicas adecuadas para el asegurar la buena ejecución de los montajes
3. Manejar, en todo momento relaciones cordiales con los clientes, brindándoles solución a sus inquietudes y circunstancias particulares
4. Efectuar el levantamiento de información de las redes tendidas
5. Diligenciar el Acta de entrega a satisfacción y hacerla firmar por el cliente una vez terminado el proyecto.
6. Indicar al cliente de manera clara, los tiempos aproximados de las actividades a desarrollar y los procedimientos que debe seguir.
7. Coordinar las actividades de ejecución de obra civil
8. Distribuir el personal operativo de acuerdo a la programación de actividades diaria
9. Supervisar la entrega de materiales, herramientas, vehículos para la ejecución de los proyectos
10. Hacer replanteos para los proyectos de montaje cuando sea necesario

11. Supervisar la instalación de cable aéreo, canalizado
12. Realizar registro fotográfico de las obras ejecutadas
13. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC)
14. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

t) Proyectistas

NOMBRE DEL CARGO: Proyectista

OBJETIVO GENERAL DEL CARGO: Realizar proyecciones de montajes y replanteos a fin de contribuir con el desarrollo de los proyectos.

CARGO DEL JEFE INMEDIATO: Coordinador de Proyectos

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Ejecución de los dibujos que indican las características y rutas de las obras a ejecutar para la conexión de los clientes.
2. Realizar los dibujos, cálculos de material y mano de obra, necesarios para la ejecución de las obras civiles, instalación de cables y empalmes de fibra óptica que se requieren para la conexión de cada cliente.
3. Realizar los site survey para la proyección del montaje
4. Realizar los replanteos de los tendidos de redes que se proyectan ejecutar así como el levantamiento de la información después de su ejecución.
5. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGS).
6. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

u) Dibujante

NOMBRE DEL CARGO: Dibujante

OBJETIVO GENERAL DEL CARGO: Realizar dibujos especializados, diseñando planos, mapas, gráficos, cuadros y demás dibujos, a fin de contribuir con el desarrollo de los proyectos.

CARGO DEL JEFE INMEDIATO: Coordinador de Proyectos

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Actualizar la base de datos gráfica a medida que se interviene la red.
2. Efectuar dibujos con base en los replanteos hechos para proyectos de montaje de redes.
3. Efectuar dibujos con base en los tendidos hechos para proyectos de montaje y mantenimiento
4. Digitar las memorias de replanteos y tendidos de los proyectos de montaje y mantenimiento
5. Diligenciar el registro de actividades diarias
6. Responsabilidad en su proceso por el Sistema de Gestión de la Calidad (SGS).
7. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

v) Empalmador de redes

NOMBRE DEL CARGO: Empalmador de redes

OBJETIVO GENERAL DEL CARGO: Realizar tendido de cable aéreo y/o canalizado, preparar y fusionar fibra óptica asegurando la atenuación dentro de los parámetros permitidos, manejo y control de equipo de medición.

CARGO DEL JEFE INMEDIATO: Coordinador de Proyectos

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Entregar cuentas de gastos efectuados, como máximo 8 días después de haber llegado de viaje
2. Mantenimiento y cuidado de la herramienta y material. La herramienta se debe limpiar luego de cada trabajo
3. Realizar el check list de equipos, accesorios, herramientas y material, antes de salir de la bodega y antes de abandonar el sitio de trabajo.
4. Mantenimiento y cuidado de la empalmadora, los accesorios y materiales para los empalmes.
5. La empalmadora y la herramienta se debe limpiar luego de cada trabajo (a diario)
6. Reportar funcionamiento anormal de la máquina y /o accesorios para empalmes, así como deterioro de los mismos, de manera inmediata.
7. Embalaje y transporte de la empalmadora y los accesorios, de manera que se evite cualquier daño de la misma en cualquier circunstancia bien sea o golpes, humedad, polvo o extravío de la misma.
8. Verificación de labores a ejecutar durante el día y solicitud de herramienta y materiales necesarios para llevarlas a cabo.
9. Verificación de sitios de empalme, abscisas de los cables a empalmar y fusiones a ejecutar
10. Seteo o configuración de la empalmadora, de acuerdo a las características de las fibras ha empalmar
11. Ejecución de fusiones y acomodamiento dentro de las bandejas porta empalmes
12. Llevar registro de actividades ejecutadas durante el día, incluyendo cantidad de fusiones, sitios, cables, resultados de pruebas y cualquier otra información de campo exigida por el superior.
13. Devolución de herramienta y materiales a la bodega, una vez finalizada la jornada laboral

14. Realizar informe diario o semanal (según indique el Superior) de las actividades ejecutadas, incluyendo fechas y horas respectivas.
15. Tomar registro fotográfico de actividades terminadas y/o que impliquen importancia para la Organización.
16. Diligenciar actas de entrega de recepción del proyecto y certificado de obra y hacerlas firmar por el cliente, una vez terminado el proyecto
17. Comprobar las longitudes de cable necesarias para cada instalación y corte del cable en bodega
18. Embalaje y transporte tanto de herramienta como de material necesario para las actividades a ejecutar
19. Instalación y desinstalación de cable aéreo y canalizado
20. Bajada e inspección de puntas del cable, verificando el estado y correcto ingreso a la estructura.
21. Instalar fibra óptica o canalizada
22. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC)
23. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

w) Instalador de redes

NOMBRE DEL CARGO: Instalación de fibra óptica

OBJETIVO GENERAL DEL CARGO: Realizar la instalación de fibra óptica de acuerdo a las normas de instalación, optimizando los materiales que se utilicen durante la instalación.

CARGO DEL JEFE INMEDIATO: Supervisor de cuadrilla

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Mantenimiento y cuidado de la herramienta y material.
2. Comprobar las longitudes de cable necesarias para cada instalación y corte del cable en bodega

3. Bajada e inspección de puntas del cable, verificando el estado y correcto ingreso a la estructura.
4. Apertura de las cámaras de empalme y limpieza de las mismas antes de su cierre
5. Instalación de fibra óptica, herrajes, retenciones o suspensiones, enchaquetado y adosado de cajas de empalme
6. Embalaje y transporte tanto de herramienta como de material necesario para las actividades a ejecutar
7. Brindar soluciones a los inconvenientes técnicos presentados durante la instalación o desinstalación.
8. Asegurar buen manejo de materiales y recursos en la ejecución
9. Cumplir con la programación y actividades dadas por el Coordinador de proyectos o Director Operativo
10. Devolución de Herramienta y Materiales a la bodega, una vez finalizada la jornada laboral
11. Instalación y desinstalación de Cable Aéreo y Canalizado
12. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
13. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

x) Oficial de obra civil

NOMBRE DEL CARGO: Técnico de obra civil

OBJETIVO GENERAL DEL CARGO: Ejecución de obras civiles para los proyectos de la organización

CARGO DEL JEFE INMEDIATO: Supervisor de cuadrilla

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Entregar cuentas de gastos efectuados, como máximo 3 días después de haber llegado de viaje

2. Inventario de herramientas y material, antes de salir de la bodega y antes de abandonar el sitio de trabajo
3. Mantenimiento y cuidado de la herramienta y material. La herramienta se debe limpiar luego de cada trabajo (a diario)
4. Ejecución de cualquier tipo de obra civil que se requiera en los proyectos de montaje y mantenimiento (Ej: Cámaras, canalizaciones, vaciados)
5. Apertura de las cámaras de empalme y limpieza de las mismas antes de su cierre
6. Embalaje y transporte tanto de herramienta como de material necesario para las actividades a ejecutar
7. Devolución de herramienta y materiales a la bodega, una vez finalizada la jornada laboral
8. Responsabilidad en su proceso por el Sistema de Gestión de la Calidad
9. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial

y) Conductor

NOMBRE DEL CARGO: Conductor

OBJETIVO GENERAL DEL CARGO: Conducir y operar los diferentes vehículos cuidadosamente cumpliendo el reglamento de tránsito y las normas internas de la Organización.

CARGO DEL JEFE INMEDIATO: Jefe de transportes

PROCESO: Logística

DESCRIPCIÓN DE FUNCIONES

1. Entregar cuentas de gastos efectuados, como máximo 24 horas después de haber llegado de viaje.
2. Portar documentos de identidad Cedula de ciudadanía, carnet, aportes parafiscales, Seguro obligatorio, Tarjeta de Propiedad, revisión Técnico mecánico.

3. Revisiones Pre operacionales diarias del vehículo para que este siempre opere en condiciones óptimas y reportar las novedades por escrito al encargado
4. Inventario diario del kilometraje durante los desplazamientos.
5. Llevar por escrito, los cambios de aceite, llantas u otro elemento que sea vital de controles periódicos.
6. Llevar el control de mantenimiento preventivo para el vehículo e informar por lo menos 8 días antes al jefe inmediato (por escrito).
7. Informar de cualquier daño o avería del vehículo, de manera inmediata al superior y al director del proyecto.
8. Informar de malos tratos o situaciones que afecten al vehículo, causados por los usuarios del vehículo.
9. Informar con dos semanas de anterioridad del vencimiento de los documentos necesarios para la movilización del vehículo.
10. Solicitar autorización escrita y firmada en caso de que algún superior pretenda pasar por alto cualquiera de las funciones encomendadas al cargo.
11. Solicitar a los usuarios el cuidado y colaboración con aseo y organización interna del vehículo.
12. Asear el vehículo (limpieza general) cada 8 días como mínimo.
13. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
14. Responsabilidad en su proceso por la salud ocupacional y seguridad industrial.

z) Ayudantes

NOMBRE DEL CARGO: Ayudante

OBJETIVO GENERAL DEL CARGO: Asistir a los procesos de mantenimiento y montaje de redes de fibra óptica y eléctricos

CARGO DEL JEFE INMEDIATO: Supervisor de Cuadrilla

PROCESO: Gestión de Proyectos

DESCRIPCIÓN DE FUNCIONES

1. Inventario de equipos, herramientas y material, antes de salir de la bodega y antes de abandonar el sitio de trabajo.
2. Mantenimiento y cuidado de la herramienta y material. La herramienta se debe limpiar luego de cada trabajo (a diario)
3. Comprobar las cantidades de material necesarias para cada Obra
4. Embalaje y Transporte tanto de Herramienta como de Material necesarios para las actividades a ejecutar
5. Realización de obras civiles, de acuerdo a las indicaciones del técnico en obras civiles
6. Apertura de las cámaras de empalme y limpieza de las mismas antes de su cierre
7. Limpieza del sitio de trabajo y organización del equipo y herramienta, luego de finalizar cada trabajo
8. Devolución de herramienta y materiales a la bodega, una vez finalizada la jornada laboral
9. Responsabilidad en su proceso por el sistema de gestión de la calidad (SGC).
10. Responsabilidad en su proceso por la salud Ocupacional y seguridad industrial.

INFRAESTRUCTURA TECNOLÓGICA

La organización cuenta con una infraestructura tecnológica que soporta las actividades del área administrativa que contempla:

- ✓ Un servidor de voz
- ✓ Un servidor de datos
- ✓ Veinticinco equipos de cómputo de escritorio y portátiles
- ✓ Tres Impresoras
- ✓ Veinte teléfonos con sistema IP
- ✓ Un router
- ✓ Dos modems de internet
- ✓ Correo electrónico corporativo
- ✓ Página web corporativa
- ✓ Aplicaciones: SIESA, Geminus

CLIENTES

Los principales clientes que tiene la organización son:

- ✓ Claro
- ✓ Comcel
- ✓ Ecopetrol
- ✓ HVM Ingenieros
- ✓ ISA Internexa
- ✓ IC Asesorías y proyectos
- ✓ Azteca Telecomunicaciones Colombia
- ✓ Megabus
- ✓ Siemens

- ✓ Eléctricas de Medellín
- ✓ Energía de Pereira
- ✓ Global Crossing
- ✓ Edeq
- ✓ Metro de Medellín
- ✓ Cobra Grupo

5.3.2 FACTORES EXTERNOS

Aunque se cuenta con una cantidad significativa de clientes, se observa que se tiene una dependencia del cliente Claro debido a que este factura un 80% de los ingresos de la compañía.

Se tiene establecidas relaciones comerciales con proveedores seleccionados que ofrecen precios competitivos.

La organización actualmente está incursionando con nueva tecnología de punta para el tendido de líneas de alta tensión y de Fibra Óptica generando en la compañía un alto nivel de competitividad en el país y reafirma la capacidad para enfrentar y resolver los retos contractuales de la actualidad, no solo en el país; sino en el continente.

La compañía se ve enfrentada a fuertes competidores que se están ubicando en la región.

En los últimos años se ha incursionado en nuevos mercados donde no se tenía presencia tanto a nivel nacional (Ibagué, Bogotá) como internacional (Cancún).

Actualmente la organización maneja una cantidad considerable de información física y virtual, la cual no cuenta con ningún tipo de control para transferir, comunicar y salvaguardarla de acuerdo al nivel de criticidad de la misma.

Se evidencia un incremento de clientes potenciales debido a que las telecomunicaciones se hacen cada vez más importantes para todos los sectores.

Demográficamente, hay regiones del país de difícil acceso ocasionando restricciones para ofrecer los servicios en todas las regiones del país.

6. REQUERIMIENTOS EXIGIDOS POR LA NORMA ISO 27001

6.1 MARCO CONCEPTUAL DE LOS REQUISITOS EXIGIDOS ISO 27001

Para cumplir los requisitos de la norma ISO/IEC 27001:2006, la organización debe planificar, establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI, utilizando para ello un proceso basado en el modelo PHVA.

La norma está establecida así:

Tabla de Contenido

0 Introducción

0.1 General

0.2 Enfoque del Proceso

0.3 Compatibilidad con otros sistemas de gestión

1. Alcance

1.1 General

1.2 Aplicación

2. Referencias normativas

3. Términos y definiciones

4. Sistema de gestión de seguridad de la información

4.1 Requerimientos generales

4.2 Establecer y manejar el SGSI

4.2.1 Establecer el SGSI

4.2.2 Implementar y operar el SGSI

4.2.3 Monitorear y revisar el SGSI

- 4.2.4 Mantener y mejorar el SGSI
- 4.3 Requerimientos de documentación
 - 4.3.1 General
 - 4.3.2 Control de documentos
 - 4.3.3 Control de registros

- 5. Responsabilidad de la gerencia
 - 5.1 Compromiso de la gerencia
 - 5.2 Gestión de recursos
 - 5.2.1 Provisión de recursos
 - 5.2.2 Capacitación, conocimiento y capacidad

- 6. Auditorías internas SGSI

- 7. Revisión Gerencial del SGSI
 - 7.1 General
 - 7.2 Insumo de la revisión
 - 7.3 Resultado de la revisión

- 8. Mejoramiento del SGSI
 - 8.1 Mejoramiento continuo
 - 8.2 Acción correctiva
 - 8.3 Acción preventiva

Tabla 6. Anexo “A” ISO 27001 Objetivos de control y controles

N°	Dominio – Control		#Ctrls
A5	Política de seguridad de la información		2
	Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.		
A.5.1.1	Política de seguridad de la información	Se dispone de una política de SI aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes.	
A.5.1.2		La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua.	
A6	Organización de la seguridad de la información		11
	Gestionar la organización de la seguridad de información.		
A.6.1.1	Organización interna	La Alta Dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la SI en la Institución.	
A.6.1.2		En las actividades de SI participan representantes de todas las UU.OO. Tienen roles y funciones.	
A.6.1.3		Los roles y responsabilidades en SI están bien definidos.	
A.6.1.4		Está establecido el proceso de autorización para nuevos activos de información (AI).	

Tabla 6. (Continuación)

.6.1.5		Están definidos acuerdos de confidencialidad y se revisa con regularidad.	
A.6.1.6		Se mantiene los contactos apropiados con las autoridades pertinentes.	
A.6.1.7		Se mantiene los contactos apropiados con entidades especializadas en SI.	
A.6.1.8		El enfoque de la organización para gestionar la SI se revisa de manera independiente y periódica.	
A.6.2.1	Entidades externas	Se gestiona (identifica e implementa) los riesgos de acceso a la información de entidades externas.	
A.6.2.2		Se trata todos los requerimientos de SI antes de dar acceso a los clientes.	
A.6.2.3		Se establece acuerdos con terceros, que involucran acceder, procesar, comunicar o gestionar la información de la entidad, que abarcan los requerimientos de SI relevantes.	
A7	Gestión de activos de información (AI)		5
	Lograr y mantener la protección apropiada de los activos de información		
A.7.1.1	Responsabilidad por los activos	Se mantiene un inventario de AI.	
A.7.1.2		Todo AI tiene asignado un responsable (propietario).	
A.7.1.3		Se dispone de una normativa de uso de los AI	

Tabla 6. (Continuación)

A.7.2.1	Clasificación de la información	La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad	
A.7.2.2		Se dispone del procedimiento de rotulado y manejo de la información.	
A8	Seguridad de los recursos humanos		9
	Asegurar que todo el personal involucrado entienda sus responsabilidades, sean apropiados para sus roles y así reducir el riesgo de robo, fraude o mal uso de los activos de información.		
A.8.1.1	Antes del empleo	Se tiene documentado (de acuerdo a la política) los roles y responsabilidades de SI, de todo el personal.	
A.8.1.2		Se verifica antecedentes de todo candidato a empleado o contratista.	
A.8.1.3		Se firman contratos donde se incluye las responsabilidades de SI.	
A.8.2.1	Durante el empleo	Se procura que todos los empleados apliquen la SI según la política.	
A.8.2.2		Se sensibiliza, capacita y educa en SI pertinente a su función de trabajo.	
A.8.2.3		Se tiene establecido uno proceso disciplinario ante el incumplimiento de SI.	
A.8.3.1	Terminación o cambio del empleo	Están definidas las responsabilidades para el término o cambio de empleo.	
A.8.3.2		Se procura la entrega de activos al término de contrato.	

Tabla 6. (Continuación)

A.8.3.3		Se retira los derechos de acceso al término del contrato.	
A9	Seguridad física y medioambiental		13
	Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones y activos de información.		
A.9.1.1	Áreas seguras	Se utiliza mecanismos de protección perimétrica (muros, vigilantes, etc.) a las áreas que contienen información e instalaciones que procesan información.	
A.9.1.2		Se utiliza mecanismos de control de acceso en entradas críticas.	
A.9.1.3		Se utiliza mecanismos de seguridad en oficinas, habitaciones e instalaciones.	
A.9.1.4		Se utiliza mecanismos de protección ante amenazas externas y ambientales.	
A.9.1.5		Se aplica medidas de seguridad física y directrices para trabajar en áreas seguras.	
A.9.1.6		Se aplica medidas de seguridad en áreas de acceso público (entrega/descarga).	
A.9.2.1	Seguridad del equipo	Los equipos están ubicados en salas con protección física ante un posible acceso no autorizado.	
A.9.2.2		Los equipos están protegidos frente a fallas de servicios públicos.	
A.9.2.3		El cableado eléctrico y de comunicaciones está protegido frente a interceptación o daños.	

Tabla 6. (Continuación)

A.9.2.4		Los equipos son mantenidos en forma periódica.	
A.9.2.5		Se aplica seguridad a los equipos fuera del local	
A.9.2.6		Antes de dar de baja un equipo se elimina la información	
A.9.2.7		Todo equipo requiere autorización para ser retirado de la Institución	
A10	Gestión de operaciones y comunicaciones		32
	Asegurar la operación correcta y segura de los activos de información.		
A.10.1.1	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados y disponibles a los usuarios.	
A.10.1.2		Gestión del control de cambios en los recursos de procesamiento de información.	
A.10.1.3		Segregación de responsabilidades para reducir el mal uso de los activos.	
A.10.1.4		Separación de los recursos de desarrollo, prueba y producción.	
A.10.2.1	Gestión de la entrega de servicios de terceros	Procurar que los terceros implementen, operen y mantengan los controles de seguridad.	
A.10.2.2		Monitoreo y auditoría regular de los servicios e informes de terceros.	

Tabla 6. (Continuación)

A.10.2.3		Gestionar los cambios en servicios de terceros, considerando criticidad de sistema de negocio así como procesos involucrados y la evaluación de riesgos.	
A.10.3.1	Planeación y aceptación del sistema	Monitorear, afinar y realizar proyecciones de uso de recursos para asegurar buen desempeño.	
A.10.3.2		Establecer los criterios de aceptación de sistemas y realizar las pruebas antes de la aceptación.	
A.10.4.1	Protección contra software malicioso y código móvil	Implementar controles de prevención, detección y recuperación ante software malicioso, así como controles adecuados para la toma de conciencia.	
A.10.4.2		Asegurar que el código móvil autorizado opere de acuerdo a las políticas de seguridad.	
A.10.5.	Copias de respaldo (back-up)	Se realiza copias de respaldo de información y software, y se prueba regularmente.	
A.10.6.1		Manejar y controlar adecuadamente las redes para proteger la información e infraestructura.	
A.10.6.2	Gestión de seguridad de redes	Las características de seguridad, los niveles del servicio, y los requisitos de gestión de todos los servicios en red están identificados e incluidos en cualquier acuerdo de servicio de red, ya sea que estos servicios sean proporcionados en la empresa o subcontratos.	

Tabla 6. (Continuación)

A.10.7.1	Gestión de medios (activos de almacenamiento)	Se dispone de procedimientos para la gestión de medios removibles.	
A.10.7.2		Se dispone de procedimientos formales para la eliminación de medios.	
A.10.7.3		Se dispone de procedimientos para el manejo de información de manera confidencial.	
A.10.7.4		La documentación de los sistemas es protegida del acceso no autorizado.	
A.10.8.1	Intercambio de información (transferencia)	Se dispone de normativa para proteger la información durante su intercambio en cualquier medio de comunicación.	
A.10.8.2		Se firma acuerdos para el intercambio de información y software con entidades externas	
A.10.8.3		Se protege los medios en tránsito contra acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de la institución	
A.10.8.4		Se protege adecuadamente la información involucrada en los mensajes electrónicos	
A.10.8.5		Se dispone de normativa para proteger la información asociada con la interconexión de los sistemas de información de la institución.	

Tabla 6. (Continuación)

A.10.9.1	Servicios de comercio electrónico	Se protege la información de comercio electrónico que se trasmite en redes públicas, contra actividades fraudulentas, litigios contractuales y divulgación o modificación.	
A.10.9.2		Se protege la información de las transacciones en línea: De transmisión incompleta, pérdida de rutas, alteración, divulgación y duplicidad.	
A.10.9.3		Se protege la integridad de la información disponible públicamente.	
A.10.10.1	Monitoreo de actividades no autorizadas	Se registra pistas de auditoria, excepciones y eventos de seguridad.	
A.10.10.2		Se dispone de procedimientos de monitoreo del uso de recursos y se revisa regularmente.	
A.10.10.3		Se protege la información y los medios de registro frente a acceso manipulado o no autorizado.	
A.10.10.4		Se registra las actividades del administrador y operador del sistema.	
A.10.10.5		Se registran las fallas, se analizan y se toma la acción apropiada.	
A.10.10.6		Los relojes de los sistemas de procesamiento de información se mantienen sincronizados	
A11	Control de acceso (lógico)		25
	Controlar el acceso lógico a los activos de información		

Tabla 6. (Continuación)

A.11.1.1	Requerimientos	Se dispone de una política de control de acceso con base en requerimientos del negocio y de seguridad para el acceso.	
A.11.2.1	Gestión de acceso de usuarios	Se dispone de procedimiento de registro y baja de concesión de acceso a los sistemas y servicios de información.	
A.11.2.2		Se dispone de procedimiento para la gestión (restricción, control y asignación) de privilegios.	
A.11.2.3		Se dispone de procedimiento para la gestión de contraseñas.	
A.11.2.4		Se audita los derechos de acceso de manera regular.	
A.11.3.1	Responsabilidades de usuarios	Se promueve las buenas prácticas de seguridad para la selección y uso de contraseñas seguras.	
A.11.3.2		Se promueve que los usuarios deben asegurar la protección de los equipos desatendidos.	
A.11.3.3		Se promueve la práctica de escritorio limpio para documentos y dispositivos de almacenamiento removibles, y una política de pantalla limpia.	
A.11.4.1	Control de acceso a la red	Los usuarios solo tienen acceso a los servicios que están autorizados.	

Tabla 6. (Continuación)

A.11.4.2		Se utiliza mecanismos apropiados de autenticación para acceso de usuarios externos.	
A.11.4.3		La identificación del equipo forma parte de la autenticación.	
A.11.4.4		Se controla el acceso para el diagnóstico y configuración de puertos.	
A.11.4.5		Se segrega en la red, los usuarios y sistemas de información.	
A.11.4.6		Se restringe la capacidad de conexión de usuarios a redes compartidas.	
A.11.4.7		La red se configura de modo que no se infrinja los controles de acceso.	
A.11.5.1		Se controla el acceso al SO en las estaciones o terminales (procedimiento de conexión segura).	
A.11.5.2		Todo usuario dispone de una cuenta de acceso única.	
A.11.5.3	Control de acceso al sistema operativo	El sistema de gestión de claves asegura su calidad.	
A.11.5.4		Se restringe el uso de utilidades (software) no autorizadas, que podrían eludir las medidas de control del sistema.	
A.11.5.5		Las sesiones inactivas se cierran luego de un tiempo de inactividad.	
A.11.5.6		Se restringe el horario de acceso a las aplicaciones de alto riesgo.	

Tabla 6. (Continuación)

A.11.6.1	Control de acceso a las aplicaciones e información	Se restringe el acceso a los usuarios y al personal de TI.	
A.11.6.2		Los sistemas sensibles están en un ambiente aislado.	
A.11.7.1	Computación móvil y teletrabajo	Se dispone de política de protección de equipos móviles.	
A.11.7.2		Se dispone de política y procedimiento para teletrabajo.	
A12	Adquisición, desarrollo y mantenimiento de sistemas de información		16
	Procurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Requerimientos de seguridad de los sistemas	Se especifican los requerimientos para nuevos sistemas o mejoras, incluyendo los controles de seguridad.	
A.12.2.1	Procesamiento correcto en las aplicaciones	Se validan los datos de entrada a las aplicaciones para asegurar que esta sea correcta y apropiada.	
A.12.2.2		Se incorpora mecanismos de validación en las aplicaciones para detectar corrupción de la información.	
A.12.2.3		Se identifican los requisitos para asegurar la autenticidad e integridad de los mensajes en	
A.12.2.4		Se valida la data de salida de las aplicaciones.	

Tabla 6. (Continuación)

A.12.3.1	Controles criptográficos	Se dispone de una política de uso de controles criptográficos para proteger la información.	
A.12.3.2		Se realiza gestión de claves para dar soporte al uso de las técnicas criptográficas.	
A.12.4.1	Seguridad de los archivos del sistema	Se dispone de procedimientos para la instalación del software de los sistemas.	
A.12.4.2		Se selecciona, protege y controla los datos de prueba del sistema.	
A.12.4.3		Se controla el acceso al código fuente del sistema.	
A.12.5.1	Seguridad en los procesos de desarrollo y soporte	Los cambios se controlan mediante el uso de procedimientos de control de cambios.	
A.12.5.2		Las aplicaciones se revisan después de haber hecho cambios en el sistema operativo, para observar el impacto generado.	
A.12.5.3		Se limita a los cambios necesarios (no se fomenta las modificaciones a los paquetes).	
A.12.5.4		Se procura evitar las fugas o filtraciones de información.	
A.12.5.5		Se supervisa y monitorea el desarrollo tercerizado de software.	
A.12.6.1	Gestión de vulnerabilidades técnicas	Se procura minimizar la explotación de vulnerabilidades de los sistemas.	
A13	Gestión de incidentes de seguridad de información		5

Tabla 6. (Continuación)

	Asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que, permita una acción correctiva oportuna.		
A.13.1.1	Reporte de incidentes y debilidades	Los incidentes de SI se reportan por los canales apropiados tan rápido como sea posible.	
A.13.1.2		Se promueve que todo el personal reporte las debilidades de SI, que observe o sospeche.	
A.13.2.1	Gestión de incidentes y mejoras	Se dispone de procedimiento para respuesta rápida, eficaz y ordenada ante incidentes de SI.	
A.13.2.2		Se dispone de mecanismos para aprender a resolver incidentes, que permitan cuantificar y realizar el seguimiento de los tipos, volúmenes y costos de los incidentes de SI.	
A.13.2.3		Se recolecta y mantiene evidencias (para fines de auditoría).	
A14	Gestión de continuidad de operaciones		5
	Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos, de los efectos de fallas significativas o desastres, y asegurar su reanudación oportuna.		
A.14.1.1	Gestión de la continuidad operativa	Se dispone de un proceso de gestión de continuidad de operaciones.	
A.14.1.2		Se realiza gestión de riesgos.	
A.14.1.3		Se dispone de un Plan de Continuidad de Operaciones (PCO).	

Tabla 6. (Continuación)

A.14.1.4		Se maneja un único marco referencial de PCO.	
A.14.1.5		El PCO se prueba y actualiza en forma regular.	
A15	Cumplimiento regulatorio		10
	Evitar el incumplimiento de cualquier ley, estatuto, obligación, reglamentado o contractuales, y de cualquier requisito de seguridad.		
		Total de controles	133

Fuente: Norma ISO /IEC 27001:2005

7. METODOLOGÍA PARA DOCUMENTAR LOS PROCESOS CON EL CICLO PHVA

Se utilizará el siguiente método para elaborar la documentación de los procesos:

Codificación de los documentos internos

El primer segmento consta de dos letras, separadas por un guión del segmento siguiente, que indican el tipo de documento que se está produciendo.

Tabla 7. Tipo de documento

TIPO DE DOCUMENTO
Procedimiento (PR)
Instructivo (IN)
Registro de calidad (RC)
Formato (FO)

Fuente: Elaboración propia

El segundo segmento corresponde a tres caracteres, separados con un guion de los segmentos anterior y posterior, con las letras que identifican el proceso que emite el documento, como se muestra a continuación.

Tabla 8. Nombre del proceso.

CÓDIGO	NOMBRE DEL PROCESO
DIR	Dirección Estratégica
SIS	Seguridad de la Información
HUM	Gestión del Talento Humano
PRO	Gestión de Proyectos
CAL	Gestión de la Calidad

Fuente: Elaboración propia

El tercer segmento corresponde a dos dígitos, que empezando en 01 continúa ordenando la documentación, consecutivamente, hasta 99.

Ejemplo del código: PR-CAL-01, que se define como: Procedimiento de Gestión de la calidad, numero 01.

Contenido del Documento Interno

-El contenido de los documentos RC y FO, debe contar con un encabezado que lleve el nombre y código y el cuerpo del documento es libre, se establece de acuerdo a la necesidad.

-El contenido de los documentos PR e IN será:

1. **OBJETO:**

Es lo que se pretende lograr al elaborar y aplicar el documento

2. **ALCANCE:**

Describe los límites para el proceso o área que aplica.

3. **DEFICIONES Y/O CONVENCIONES**

Es el significado o contexto que se le da a los términos o abreviaturas más utilizadas en el proceso.

4. DESCRIPCIÓN DEL DOCUMENTO

Es el cuerpo del documento, son los pasos y el grado de detalle de la instrucción.

El contenido de los documentos llamados registros es libre y se realizan de acuerdo a las necesidades de los documentos y la organización.

Documentar las actividades bajo el ciclo PHVA

Identificar todas las actividades que se desarrollan los procesos con el fin de documentarlas teniendo en cuenta los ciclos Planear, Hacer, Verificar y Actuar.

Redactar la información de manera secuencial y continua. Sin embargo, se pueden redactar algunos documentos en prosa, redactar la documentación en forma clara y legible y adaptada al lenguaje propio de la organización.

7.1 PROCESOS Y REGISTROS PARA CADA REQUISITO DE LA ISO 27001

Las necesidades que tiene la organización de acuerdo al diagnóstico realizado, es documentar las disposiciones del Anexo A de la norma ISO 27001 que es donde se definen los controles de seguridad de la información para la organización.

Teniendo en cuenta los procesos que se ejecutan en la organización, no es necesario que todos los procesos participen en la elaboración de los documentos; sin embargo deben participar activamente en el cumplimiento de los controles de seguridad de la información.

La Gerencia General define que los procesos que administrarán la documentación del Sistema de Seguridad de la información son:

1. Dirección Estratégica
2. Gestión de la Seguridad de la Información y de los Servicios TI
3. Gestión del Talento Humano
4. Gestión de la Calidad

A continuación se elabora matriz de correlación con los controles exigidos por la norma ISO y los documentos que de acuerdo a las necesidades de la organización se establecerán para cada control del 1 al 15 dando cumplimiento a cada uno de los controles así:

Tabla 9. Matriz de Correlación Controles ISO & Procedimiento o Documento de Soporte.

MATRIZ DE CORRELACIÓN CONTROLES ISO & PROCEDIMIENTO O DOCUMENTO DE SOPORTE			
CONTROL vs DOMINIO	OBJETIVO DEL CONTROL	DESCRIPCIÓN DEL CONTROL	<u>PROCEDIMIENTO O DOCUMENTO SOPORTE</u>
5.1	Política de seguridad de la información	La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.	Política de Seguridad de la información
5.2	Revisión de la política de seguridad de la información	La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz	

Tabla 9 (Continuación)

6.1.1	Compromiso de la dirección con la seguridad de la información	La dirección debe apoyar activamente la seguridad de información dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.	Acuerdo de confidencialidad
6.1.2	Coordinación de la seguridad de la información.	Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes	
6.1.3	Asignación de responsabilidades para la SI.	Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información.	

Tabla 9 (Continuación)

6.1.4	Proceso de autorización para los servicios de procesamiento de información.	Se debe definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información.	Matriz de comunicación contacto con autoridades Matriz de comunicación con grupos de interés especial
6.1.5	Acuerdos sobre confidencialidad.	Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.	
6.1.6	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes	
6.1.7	Contacto con grupos de interés especiales	Se deben mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales	

Tabla 9 (Continuación)

6.1.8	Revisión independiente de la seguridad de la información.	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad	Lista de chequeo para el control de los servicios contratados externamente. Balance del servicio
A.6.2.1	Identificación de los riesgos relacionados con las partes externas.	Se deben identificar los riesgos para la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.	
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes	Todos los requisitos de seguridad identificados se deben considerar antes de dar acceso a los clientes a los activos o la información de la organización	

Tabla 9 (Continuación)

A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes	Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los requisitos pertinentes de seguridad	
A.7.1.1	Inventario de activos	Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.	Procedimiento Gestión de Activos de información

Tabla 9 (Continuación)

A.7.1.2	Propiedad de los activos	Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad" de una parte designada de la organización	Registro inventario de activos
A.7.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información	
A.7.2.1	Directrices de clasificación	La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.	

Tabla 9 (Continuación)

A.7.2.2	Etiquetado y manejo de información	Se deben desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización	
A.8.1.1	Roles y responsabilidades	Se deben definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización	Procedimiento Vinculación, inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación.
A.8.1.2	Selección	Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.	

Tabla 9 (Continuación)

A.8.1.3	Términos condiciones laborales.	y Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.	Registro de Acuerdo de confidencialidad de la información y código de buena conducta
A.8.2.1	Responsabilidades de la dirección	La dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.	
A.8.2.2	Educación, formación y concientización sobre la seguridad de la información	Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	

Tabla 9 (Continuación)

A.8.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad	Procedimiento Vinculación, inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación.
A.8.3.1	Responsabilidades en la terminación	Se deben definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral	
A.8.3.2	Devolución de activos	Todos los empleados, contratistas o usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.	
A.8.3.3	Retiro de los derechos de acceso	Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio	

Tabla 9. (Continuación)

A.9.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información	Procedimiento de Seguridad física y del entorno
A.9.1.2	Controles de acceso físico.	Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	
A.9.1.3	Seguridad de oficinas, recintos e instalaciones.	Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	
A.9.1.4	Protección contra amenazas externas y ambientales	Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones	

Tabla 9. (Continuación)

A.9.1.5	Trabajo en áreas seguras.	Se deben diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	Procedimiento de Seguridad física y del entorno
A.9.1.6	Áreas de carga, despacho y acceso público	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado	
A.9.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado	
A.9.2.2	Servicios de suministro	Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro	

Tabla 9. (Continuación)

A.9.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegidos contra interceptaciones o daños.	Procedimiento de Seguridad física y del entorno
A.9.2.4	Mantenimiento de los equipos.	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	
A.9.2.5	Seguridad de los equipos fuera de las instalaciones.	Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	
A.9.2.6	Seguridad en la reutilización eliminación de los equipos.	Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación	
A.9.2.7	Retiro de activos	Ningún equipo, información ni software se deben retirar sin autorización previa	

Tabla 9. (Continuación)

A.10.1.1	Documentación de los procedimientos de operación	Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten	Procedimiento Gestión de las comunicaciones y operaciones
A.10.1.2	Gestión del cambio.	Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.	
A.10.1.3	Distribución de funciones	Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización	
A.10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación	Instalaciones de desarrollo, ensayo y operación. Estas fases deben estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.	
A.10.2.1	Prestación del servicio	Se deben garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por las terceras partes	

Tabla 9. (Continuación)

A.10.2.2	Monitoreo y revisión de los servicios por terceras partes	Los servicios, reportes y registros suministrados por terceras partes se deben controlar y revisar con regularidad y las auditorias se deben llevar a cabo a intervalos regulares	Procedimiento Gestión de Cambios de los servicios TI
A.10.2.3	Gestión de los cambios en los servicios por terceras partes	Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de seguridad de la información, en los procedimientos y los controles se deben gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.	

Tabla 9. (Continuación)

A.10.3.1	Gestión de la capacidad.	Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema	Procedimiento Gestión de la Capacidad de los servicios TI y de los sistemas de información
A.10.3.2	Aceptación del sistema	Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.	
A.10.4.1	Controles contra códigos maliciosos.	Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.	

Tabla 9. (Continuación)

A.10.4.2	Controles contra códigos móviles	Cuando se autoriza la utilización de códigos móviles, la configuración debe asegurar que dichos códigos operan de acuerdo con la política de seguridad claramente definida, y se debe evitar la ejecución de los códigos móviles no autorizados	Procedimiento Gestión de las comunicaciones y operaciones
A.10.5.1	Respaldo de la información	Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada	
A.10.6.1	Controles de las redes	Las redes se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.	

Tabla 9. (Continuación)

A.10.6.2	Seguridad de los servicios de la red.	En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente	Procedimiento Gestión de las comunicaciones y operaciones
A.10.7.1	Gestión de los medios removibles	Se deben establecer procedimientos para la gestión de los medios removibles	
A.10.7.2	Eliminación de los medios.	Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo, utilizando los procedimientos formales.	
A.10.7.3	Procedimientos para el manejo de la información.	Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado	

Tabla 9. (Continuación)

A.10.7.4	Seguridad de la documentación del sistema.	La documentación del sistema debe estar protegida contra el acceso no autorizado.	Procedimiento Gestión de las comunicaciones y operaciones
A.10.8.1	Políticas y procedimientos para el intercambio de información	Se deben establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.	
A.10.8.2	Acuerdos para el intercambio	Se deben establecer acuerdos para el intercambio de la información y del software entre la organización y partes externas.	
A.10.8.3	Medios físicos en tránsito.	Los medios que contienen información se deben proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización	

Tabla 9. (Continuación)

A.10.8.4	Mensajería electrónica.	La información contenida en la mensajería electrónica debe tener la protección adecuada	Procedimiento Gestión de las comunicaciones y operaciones
A.10.8.5	Sistemas de información del negocio	Se deben establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio	
A.10.10.1	Registro de auditorías	Se deben elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso	
A.10.10.2	Monitoreo del uso del sistema	Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad	

Tabla 9. (Continuación)

A.10.10.3	Protección de la información del registro	Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizados	Procedimiento Gestión de las comunicaciones y operaciones
A.10.10.4	Registros del administrador y del operador	Se deben registrar las actividades tanto del operador como del administrador del sistema.	
A.10.10.5	Registro de fallas	Las fallas se deben registrar y analizar, y se deben tomar las acciones adecuadas.	
A.10.10.6	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	

Tabla 9. (Continuación)

A.11.1.1	Política de control de acceso	Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso	Procedimiento Control de acceso a la información
A.11.2.1	Registro de usuarios.	Debe existir un procedimiento formal para el registro y cancelación de usuarios, conceder y revocar el acceso a todos los sistemas y servicios de información.	
A.11.2.2	Gestión de privilegios.	Se debe restringir y controlar la asignación y uso de privilegios.	
A.11.2.3	Gestión de contraseñas para usuarios.	La asignación de contraseñas se debe controlar a través de un proceso formal de gestión	
A.11.2.4	Revisión de los derechos de acceso de los usuarios.	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	

Tabla 9. (Continuación)

A.11.3.1	Uso de contraseñas.	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.	Registro Concesión y Verificación de acceso a los SI
A.11.3.2	Equipo de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	
A.11.3.3	Política de escritorio despejado y de pantalla despejada	Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.	
A.11.4.1	Política de uso de los servicios de red.	Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados.	

Tabla 9. (Continuación)

A.11.4.2	Autenticación de usuarios para conexiones externas	Se deben emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	Registro Identificación de usuarios y asignación de privilegios
A.11.4.3	Identificación de los equipos en las redes.	La identificación automática de los equipos se debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.	
A.11.4.4	Protección de los puertos de configuración y diagnóstico remoto	El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado	
A.11.4.5	Separación en las redes.	En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	
A.11.4.5	Separación en las redes.	En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	

Tabla 9. (Continuación)

A.11.4.6	Control de conexión a las redes.	Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debe restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control del acceso y los requisitos de aplicación del negocio (véase el numeral 11.1).	Registro Inventario de Sistemas de información.
A.11.4.7	Control de enrutamiento en la red.	Se deben implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control del acceso de las aplicaciones del negocio.	
A.11.4.8	Procedimientos de ingreso seguros	El acceso a los sistemas operativos se debe controlar mediante un procedimiento de registro de inicio seguro	
A.11.5.2	Identificación y autenticación de usuarios	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.	

Tabla 9. (Continuación)

A.11.5.3	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Procedimiento Control de acceso a la información
A.11.5.4	Uso de las utilidades del sistema	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.	
A.11.5.5	Tiempo de inactividad de la sesión	Las sesiones inactivas se deben suspender después de un periodo definido de inactividad.	
A.11.5.6	Limitación del tiempo de conexión	Se deben utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo	
A.11.6.1	Restricción de acceso a la información.	Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.	

Tabla 9. (Continuación)

A.11.6.2	Aislamiento de sistemas sensibles.	Los sistemas sensibles deben tener un entorno informático dedicado (aislados).	Procedimiento Control de acceso a la información
A.11.7.1	Computación y comunicaciones móviles.	Se debe establecer una política formal y se deben adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles	
A.11.7.2	Trabajo remoto.	Se deben desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto	

Tabla 9. (Continuación)

A.12.1.1	Análisis y especificación de los requisitos de seguridad	Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deben especificar los requisitos para los controles de seguridad.	Procedimiento Adquisición y mantenimiento de sistemas de información
A.12.3.1	Política sobre el uso de controles criptográficos.	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	
A.12.3.2	Gestión de llaves.	Se debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.	
A.12.4.1	Control del software operativo.	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	

Tabla 9. (Continuación)

A.12.4.2	Protección de los datos de prueba del sistema.	Los datos de prueba deben seleccionarse cuidadosamente, así como protegerse y controlarse	Registro de Inventario de Sistemas de información
A.12.4.3	Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas	
A.12.5.1	Procedimientos de control de cambios.	Se deben controlar la implementación de cambios utilizando procedimientos formales de control de cambios.	
A.12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.	Se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deben revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.	
A.12.5.3	Restricciones en los cambios a los paquetes de software.	Se debe desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente	

Tabla 9. (Continuación)

A.12.5.4	Fuga de información	Se deben evitar las oportunidades para que se produzca fuga de información.	Registro de Reporte de vulnerabilidades
A.12.5.5	Desarrollo de software contratado externamente	La organización debe supervisar y monitorear el desarrollo de software contratado externamente.	
A.12.6.1	Control de vulnerabilidades técnicas	Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados	

Tabla 9. (Continuación)

A.13.1.1	Reporte sobre los eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible	Procedimiento Gestión Incidentes, Peticiones de servicio y Problemas de la seguridad de la Información y de los Servicios TI
A.13.1.2	Reporte sobre las debilidades de la seguridad	Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	
A.13.2.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	

Tabla 9. (Continuación)

A.13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Deben existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	Registro Matriz del nivel de criticidad de los incidentes
A.13.2.3	Recolección de evidencia	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente	

Tabla 9. (Continuación)

A.14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	Se debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización	Procedimiento Gestión de la Continuidad y Disponibilidad del negocio y de los servicios TI Instructivo análisis del impacto al negocio BIA
A.14.1.2	Continuidad del negocio y evaluación de riesgos	Se deben identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.	
A.14.1.3	Desarrollo e implementación de planes de continuidad	Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.	

Tabla 9. (Continuación)

A.14.1.4	Estructura para la planificación de la continuidad del negocio	Se debe mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento	Instructivo Análisis de riesgos para la continuidad y disponibilidad de los procesos críticos
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia	

Tabla 9. (Continuación)

A.15.1.1	Identificación de la legislación aplicable.	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización	Procedimiento Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información
A.15.1.2	Derechos de propiedad intelectual (DPI).	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	
A.15.1.3	Protección de los registros de la organización.	Los registros importantes se deben proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.	

Tabla 9. (Continuación)

A.15.1.4	Protección de los datos y privacidad de la información personal.	Se debe garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.	Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	Se debe disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.	
A.15.1.6	Reglamentación de los controles criptográficos.	Se deben utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes	

Tabla 9. (Continuación)

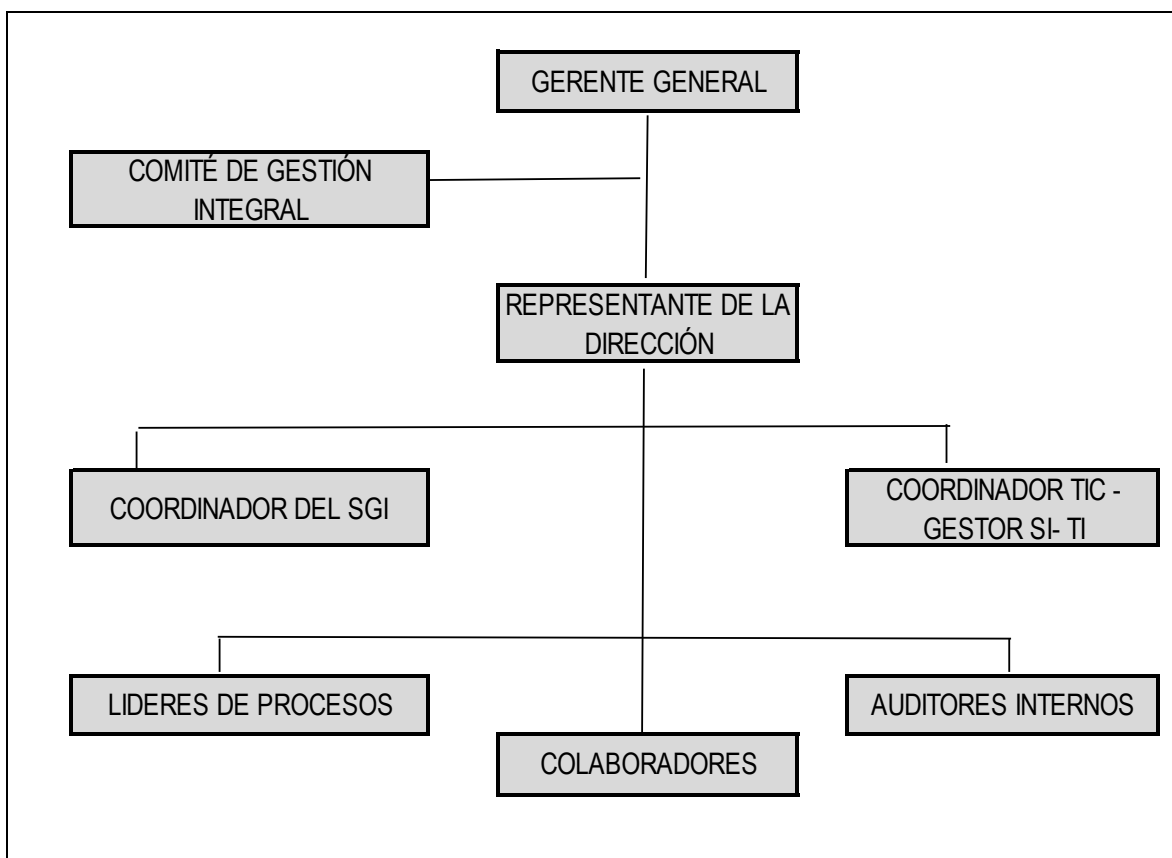
A.15.2.1	Cumplimiento con las políticas y normas de seguridad	Los directores deben garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad	Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información
A.15.2.2	Verificación del cumplimiento técnico	Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.	
A.15.3.1	Controles de auditoría de los sistemas de información.	Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro	

Fuente: Elaboración propia

7.2 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN.

Se establece el siguiente organigrama para el Sistema de Gestión de la seguridad de la información quienes serán los responsables de implementar los procedimientos establecidos y velarán por su cumplimiento dentro de la organización.

Figura 4. Roles y Responsabilidades para la Seguridad de la Información.



Fuente: Elaboración propia

7.6.1 Responsabilidades adicionales de los roles para la seguridad de la información

7.6.1.1 Gerente General

1. Creación de un comité de seguridad interdisciplinario
2. Asignar los recursos necesarios para la operación y manteniendo del SGSI.
3. Asignación de un responsable de la seguridad de la información
4. Aprobación de las políticas de seguridad de la información
5. Velar por el cumplimiento de las políticas de seguridad de la información
6. Asignación de responsabilidades asociadas al tema de la seguridad de la información

7.6.1.2 Comité de Gestión Integral

1. Revisar periódicamente el estado general de la seguridad de la información
2. Revisar y monitorear los incidentes de seguridad de la información
3. Revisar y aprobar los proyectos de seguridad de la información
4. Aprobar las modificaciones o nuevas políticas de seguridad de la información
5. Revisar el estado de cumplimiento de los controles de seguridad implementados.
6. Revisar el estado de cumplimiento de los objetivos de seguridad de la información
7. Revisar el estado de las auditorías internas y externa
8. Revisar el estado de las acciones correctivas, preventivas y de mejora

7.6.1.3 Representante de la Dirección

1. Asegurar que se realicen las actividades para identificar, documentar y satisfacer los requisitos del servicio
2. Asignar autorizaciones y responsabilidades para asegurar que se diseñan, implementan, y mejoran los procesos de la gestión de la calidad, de la gestión del servicio y de la gestión de la seguridad de la información conforme a las políticas y objetivos
3. Asegurar que los procesos de gestión del servicio están integrados en el resto de componentes del SGS.
4. Asegurar que los activos, incluyendo sus licencias, utilizados para proveer los servicios, se gestionan conforme a los requisitos legales y regulatorios, y a las obligaciones contractuales
5. Informar a la alta Dirección sobre el desempeño, oportunidad de mejora y el rendimiento del sistema de gestión integral.
6. Asegurarse de que se promueva la toma de conciencia de los requisitos del cliente en todos los niveles de la organización
7. Presentar informes, con la periodicidad establecida, para la revisión del sistema integral por la Dirección

7.6.1.4 Coordinador del SGI

Las funciones y responsabilidades establecidas para esta designación son entre otras:

1. Apoyar el desarrollo de los procedimientos de seguridad de la información y de gestión de los servicios de tecnología de la información.

2. Proponer y coordinar la realización del análisis de riesgos de seguridad de la información que abarque toda la organización.
3. Mantener contacto con grupos especiales para actualizaciones de seguridad.
4. Promover la creación y actualización de las políticas de seguridad de la información y de la gestión de servicios de tecnología de la información, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.
5. Participar en el análisis y resolución de los incidentes de seguridad de la información y la tecnología de la información
6. Coordinar la realización periódica del ciclo de auditorías internas al sistema de gestión Integral.
7. Realizar seguimiento continuo a las acciones correctivas, preventivas y de mejora del sistema de gestión integral

7.6.1.5 Coordinador TIC- Gestor SI-TI

Las funciones establecidas para esta designación son entre otras:

1. Definir políticas y procedimientos para: la gestión de accesos a todos los sistemas, gestión de activos, gestión de riesgos, gestión de continuidad y disponibilidad del negocio, gestión de capacidad, monitoreo del uso de las instalaciones de procesamiento de la información, gestión de incidentes de SI, gestión de respaldo, gestión de seguridad de la red, controles criptográficos, procesamiento correcto de las aplicaciones, Controles criptográficos, gestión de help desk para las solicitudes de servicios TI.
2. Gestionar y verificar el cumplimiento de las disposiciones establecidas, relacionadas con control de accesos, registro de usuarios, administración

de privilegios, Administración de contraseñas, utilización de servicios de red, autenticación de usuarios, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red.

3. Concientizar a los usuarios sobre los controles de seguridad de la información y las buenas prácticas.
4. Tomar las acciones correctivas que garanticen la seguridad informática requerida por la organización
5. Identificar e implementar herramientas de seguridad informática para resguardar la integridad, confidencialidad y disponibilidad de la información.
6. Velar por el cumplimiento de la ley, obligaciones reglamentarias o contractuales de cualquier requisito de seguridad.
7. Recibir y ejecutar auditorías internas y externas para verificar la efectividad y existencia de los controles de seguridad en toda la organización.

7.6.1.6 Líderes de proceso

Las funciones y responsabilidades establecidas para esta designación son entre otras:

1. Conocer y aplicar las políticas de seguridad para los activos de la organización
2. Administrar, clasificar y mantener el nivel de privacidad de la información, de conformidad con su clasificación, valor y criticidad.
3. Definir los usuarios que dentro de su área que podrán tener acceso a la información.
4. Reportar los incidentes y eventos de seguridad, siguiendo los procedimientos establecidos para este fin.

5. Garantizar la oportunidad, veracidad, exactitud, confiabilidad y disponibilidad de la información que genera y/o actualiza.
6. Responder por los recursos informáticos, hardware, software, documentación, suministros y otros elementos que le sean asignados. Del mismo modo, hacer uso racional de los productos y servicios informáticos provistos por CYFO COMUNICACIONES.
7. Responder por la seguridad de la información que lleva bajo su custodia fuera de las instalaciones de la organización
8. Seguir los procedimientos establecidos por el proceso de Gestión de la seguridad de la información y de Tecnología de la Información.
9. Reportar en la aplicación ITOP la presencia o sospecha de virus o software malicioso.
10. Plantear acciones preventivas o correctivas al sistema de gestión integral SGI

7.6.1.7 Auditores Internos

Las funciones establecidas para esta designación son entre otras:

1. Elaborar el Programa anual de auditorías internas y conseguir la aprobación de la dirección
2. Coordinar y supervisar la elaboración del plan para cada proceso a auditar
3. Coordinar y supervisar la elaboración de la lista de verificación para cada proceso a auditar
4. Coordinar y supervisar la ejecución del plan de auditoría.
5. Administrar el proceso de las auditorías internas desde la asignación de una auditoría hasta su cierre
6. Presentar resultados a la dirección sobre el resultado de las auditorías.

7.6.1.8 Colaboradores

1. Cumplir con las disposiciones de la Política de Seguridad de la Información
2. Administrar, clasificar y mantener el nivel de privacidad de la información, de conformidad con su clasificación, valor y criticidad.
3. Definir los usuarios que dentro de su área podrán tener acceso a ella y los privilegios para su tratamiento, bajo criterios de segregación de funciones.
4. Acatar la metodología y proceso de identificación, valoración, clasificación y tratamiento de los activos de información. Esto para los procesos que hagan parte del alcance del SGSI.
5. Acatar la metodología y proceso de valoración del riesgo que del SGSI. Lo anterior, para los procesos que hagan parte del alcance del SGSI.
6. Acudir y participar de los programas de formación y toma de conciencia relacionados con la seguridad de la información.
7. Implementar los procedimientos y controles para detectar y dar respuesta oportuna a los incidentes de seguridad.
8. Ejecutar las recomendaciones derivadas de los procedimientos de seguimiento y revisión del SGSI.
9. Realizar la revisión de las valoraciones de los riesgos de acuerdo a lo estipulado por la coordinación de seguridad de la información.
10. Ejecutar las recomendaciones derivadas de las auditorías internas del SGSI realizadas.
11. Plantear acciones preventivas, mejora o correctivas

8. GUÍA DOCUMENTAL

8.1 PLAN OPERATIVO PARA EL DESARROLLO DE LA GUÍA

Se establece el listado maestro de documentos donde se contemplan los procedimientos, registros, instructivos, planes de calidad, políticas y registros como plan operativo para desarrollar la guía documental. Los documentos se establecerán de acuerdo al orden del listado maestro.

Tabla 10. Listado maestro de documentos para el sistema de gestión de seguridad de la información.

LISTADO MAESTRO DE DOCUMENTOS PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
CÓDIGO	NOMBRE DEL DOCUMENTO	VERSIÓN
PROCEDIMIENTOS		
PR-DIR-03	Procedimiento de Organización de la Seguridad de la Información	1
PR-DIR-04	Procedimiento Gestión de la Continuidad y Disponibilidad del negocio y de los servicios TI	1
PR-HUM-01	Procedimiento Vinculación, inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación.	1
PR-PRO-08	Procedimiento Control de servicios contratados externamente	1
PR-SIS-02	Procedimiento Gestión de Activos de información	1
PR-SIS-03	Procedimiento de Seguridad física y del entorno	1
PR-SIS-04	Procedimiento Gestión de las comunicaciones y operaciones	1
PR-SIS-05	Procedimiento Control de acceso a la información	1
PR-SIS-06	Procedimiento Adquisición y mantenimiento de sistemas de información	1
PR-SIS-07	Procedimiento Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información	1
PR-SIS-08	Mantenimiento de activos de información	1
PR-SIS-09	Procedimiento Copias de Respaldo	1

Tabla 10. (Continuación)

PR-SIS-11	Manejo de Medios	1
PR-SIS-13	Procedimiento Gestión Incidentes, Peticiones de servicio y Problemas de la seguridad de la Información y de los Servicios TI	1
PR-SIS-15	Procedimiento Gestión de Cambios de los servicios TI	1
PR-SIS-19	Gestión de las Relaciones con el Negocio y Gestión con los proveedores	1
PR-SIS-20	Procedimiento Gestión de la Capacidad de los servicios TI y de los sistemas de información	1
INSTRUCTIVOS		
IN-DIR-02	Instructivo análisis del impacto al negocio BIA	1
IN-SIS-03	Instructivo Análisis de riesgos para la continuidad y disponibilidad de los procesos críticos	1
PLANES DE CALIDAD		
PC-MEI-03	Programa de mantenimiento de infraestructura	1
POLÍTICAS		
PO-DIR-05	Política de Seguridad de la información	1
REGISTROS		
FO-PRO-07	Registro Lista de chequeo para el control de servicios contratados externamente	1
FO-PRO-08	Registro Balance del servicio	1
FO-PRO-09	Registro de Acuerdo de confidencialidad	1
RC-DIR-01	Registro del comité de Seguridad de la información	1

Tabla 10. (Continuación)

FO-DIR-01	Registro de Presupuesto para la implementación del SGI	1
RC-HUM-16	Registro de Acuerdo de confidencialidad de la información y código de buena conducta	1
RC-HUM-25	Registro Matriz de autoridades y responsabilidades	1
RC-MEI-05	Registro mantenimiento a la infraestructura interna	1
RC-CAL-01	Registro Matriz de comunicación contacto con autoridades	1
RC-CAL-02	Registro Matriz de comunicación con grupos de interés especial	1
RC-SIS-32	Registro Matriz del nivel de criticidad de los incidentes	1
RC-SIS-41	Registro inventario de activos	1
RC-SIS-61	Registro de Reporte de vulnerabilidades encontradas.	1
RC-SIS-64	Registro Identificación de usuarios y asignación de privilegios.	1
RC-SIS-68	Registro Inventario de Sistemas de información.	1
RC-SIS-69	Registro Concesión y Verificación de acceso a los SI	1

Fuente: Elaboración propia

8.2 DOCUMENTACIÓN DE LOS PROCESOS EXIGIDOS POR LA ISO 27001

8.2.1 Procedimiento de Organización de la Seguridad de la Información

Procedimiento de Organización de la Seguridad de la Información	<u>Código: PR-DIR-03</u>
	<u>Versión:01</u>

1. OBJETO

Gestionar la seguridad de la información dentro de la organización.

2. ALCANCE

Este documento aplica para todo el sistema de gestión de seguridad de la información implementado en la organización y contiene mecanismos para mantener actualizados los documentos y procedimientos respecto a los requisitos de confidencialidad y protocolo de comunicación con autoridades y otros grupos de interés.

3. DEFINICIONES Y/O CONVENCIONES

Seguridad de la información preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad

Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Incidente de seguridad de la información: un evento o serie de eventos de

seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1 ORGANIZACIÓN INTERNA</p> <p>4.1.1 Compromiso de la dirección con la seguridad de la información</p> <p>Demostrar el compromiso de la seguridad de la información de la organización por parte de la Dirección a través de las siguientes consideraciones:</p> <p>*Asignación de recursos económicos y financieros</p> <p>*Asignación de recursos Humanos a través del nombramiento de un Gestor SI-TI</p> <p>*Identificación, medición y seguimiento de los objetivos y metas de seguridad de la información.</p> <p>* Asignación de las funciones y responsabilidades a todos los colaboradores de acuerdo a su compromiso dentro del Sistema de Gestión</p>	<p>Gerente General</p>	<p>PC-DIR-02 Proyección estratégica de la gestión integral</p> <p>FO-DIR-01 Presupuesto para la implementación del SGI</p> <p>MC-HUM-01 Manual de funciones</p> <p>PC-CAL-03 Programa de auditorías internas al SGI</p>

<p>* Verificar el cumplimiento de las disposiciones por medio de auditorías Internas.</p>		
<p>4.1.2 Coordinación de la seguridad de la información.</p> <p>Nombrar un Gestor SI-TI quién es el responsable de coordinar todos los procesos y actividades conducentes a salvaguardar la integridad, disponibilidad y confiabilidad de la información.</p> <p>Dentro de sus funciones principales son:</p> <ol style="list-style-type: none"> 1. Definir y actualizar (cuando sea necesario) políticas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de los dispositivos de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto, reportes de incidentes, la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido. 2. Analizar, definir e implementar políticas de acceso y utilización de Internet para todos los usuarios. 3. Verificar y controlar el cumplimiento de las 	<p>Gestor SI-TI</p>	<p>MC-HUM-01 Manual de funciones</p> <p>FO-CAL-04 Asistencia a eventos de capacitación y/o formación</p> <p>RC-HUM-25 Matriz de autoridades y responsabilidades</p>

<p>disposiciones establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, Administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado del sistema, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red y control de ruteo de red.</p> <p>4. Concientizar a los usuarios sobre el uso apropiado de contraseñas y de dispositivos de procesamiento de la información.</p> <p>Los representantes de la organización son:</p> <ul style="list-style-type: none"> • Gerente General: Alta dirección • Director Operativo: área operativa • Director Administrativo: área administrativa • Director Comercial: área comercial <p>La coordinación de las actividades de la seguridad de la información se desarrolla por todos los representantes en los Comité de SGI con base en la información presentada por el Gestor SI-TI.</p> <p>Los roles de los representantes de la</p>		
--	--	--

<p>organización se definen en los respectivo manuales de funciones.</p>		
<p>4.1.3 Asignación de responsabilidades para la seguridad de la información.</p> <p>Identificar las responsabilidades en cuanto a la seguridad de la información en los perfiles de cada colaborador y la de los líderes de procesos en la matriz de autoridades y responsabilidades de acuerdo a su proceso.</p>	<p>Gerente General</p>	<p>RC-HUM-25 Matriz de autoridades y responsabilidades</p>
<p>4.1.4 Proceso de autorización para los servicios de procesamiento de información.</p> <p>Tener en cuenta las siguientes consideraciones al momento de solicitar un nuevo servicio de procesamiento de la información:</p> <p>*Contar con la aprobación de la Gerencia general, cuando se requiera un nuevo servicio de procesamiento de información considerando justificación, objetivos, alcance y costos, documentar las decisiones y acciones en el acta del comité de gestión integral.</p>	<p>Gerente General Gestor SI-TI</p>	<p>RC-DIR-01 Revisiones periódicas por la dirección al Sistema de Gestión Integral</p>

<p>*Viabilizar el proyecto por parte de la Gerencia realizando una reunión con las partes involucradas donde se evalúen las consideraciones anteriores, así como fecha de cumplimiento, metodología, plan de contingencia y recuperación y otras no contempladas en la propuesta inicial.</p> <p>*Implementar el nuevo sistema de procesamiento de información una vez aprobada la propuesta, realizando verificaciones y validaciones permanentes por parte de la persona quien realiza la solicitud y por el Gestor SI-TI si se considera necesario.</p> <p>*Someter a prueba durante un tiempo considerable el nuevo sistema de procesamiento de información antes de realizar cualquier suspensión o modificación derivada de la nueva implementación.</p>		
<p>4.1.5 Acuerdos sobre confidencialidad</p> <p>Establecer acuerdos de confidencialidad con todos los colaboradores, contratistas, proveedores y terceras partes que tengan contacto con información sensible de la organización, quienes a través de la firma en el documento dejan constancia de conocer,</p>	<p>Director operativo</p> <p>Jefe de Talento Humano</p> <p>Gestor SI-TI</p>	<p>FO-PRO-09 Acuerdo de confidencialidad</p> <p>RC-HUM-16 Acuerdo de confidencialidad de la información y</p>

<p>entender y aceptar las implicaciones del acuerdo de confidencialidad de la información.</p>		<p>código de buena conducta</p>
<p>4.1.6 Contacto con las autoridades</p> <p>Implementar la matriz de comunicación con las autoridades y actualizarla anualmente.</p> <p>Identificar en la matriz los siguientes aspectos:</p> <p>Entidad, numero(s) de teléfono(s), dirección, pagina web (si la tiene), en que caso se debe contactar y quienes son los responsables de la comunicación.</p> <p>Socializar con los involucrados la matriz de comunicación y el procedimiento a seguir en caso de presentarse la necesidad de acudir a alguna autoridad.</p> <p>Reportar a la Gerencia y procesos interesados el acontecimiento de cualquier evento que haya requerido acudir a alguna autoridad, notificando la razón, hora, fecha y estado del proceso</p> <p>Establecer contacto con las autoridades de acuerdo a la matriz Comunicación con las autoridades.</p>	<p>Director Operativo</p> <p>Director Administrativo y Financiero</p> <p>Coordinador de Proyectos</p> <p>Jefe de Cuadrilla</p> <p>Jefe de Talento Humano</p>	<p>PC-CAL-08</p> <p>Matriz de comunicación contacto con autoridades</p>

<p>4.1.7 Contacto con grupos de interés especiales</p> <p>Implementar la matriz de comunicación con los grupos de interés y actualizarla anualmente.</p> <p>Mantener contacto con estos grupos especiales a través de correos electrónicos, página web, comunicación física entre otras.</p> <p>Windows</p> <p>Kasperky</p> <p>DragonJarp</p> <p>Segu.Info.News (noticias sobre seguridad de la información)</p> <p>Icontec</p> <p>Bureau veritas</p> <p>Ministerio de tecnologías de la información y las comunicaciones.</p> <p>ACIS Asociación Colombiana de Ingenieros de Sistemas</p> <p>Revisar mensualmente la información recibida de los grupos de interés y cuando aplique, tomar acciones preventivas y documentarlas en el registro RC-CAL-04.</p>	<p>Coordinador TIC</p> <p>Coordinadora del SGI</p>	<p>PC-CAL-09</p> <p>Matriz de comunicación con grupos de interés especial</p> <p>RC-CAL-04</p> <p>Acciones correctivas, preventivas y de mejora y seguimiento</p>
<p>4.1.8 Revisión independiente de la seguridad de la información.</p> <p>Evaluar en los comités de Gestión Integral el enfoque de la organización para la gestión de</p>	<p>Comité de Gestión Integral</p>	<p>RC-DIR-01</p> <p>Revisiones periódicas por la dirección al Sistema de Gestión Integral</p>

la seguridad de la información y el desempeño de su implementación junto con los cambios ocurridos en los objetivos, controles, políticas y/o procedimientos para identificar las oportunidades de mejora.		
--	--	--

8.2.2 Procedimiento Gestión de la Continuidad y Disponibilidad del negocio y de los servicios TI

Procedimiento Gestión de la Continuidad y Disponibilidad del negocio y de los servicios TI	<u>Código: PR-DIR-04</u>
	<u>Versión:01</u>

1. OBJETO

Asegurar la continuidad del negocio y de los servicios TI frente a eventos de desastre que produzcan alguna interrupción de los servicios TI o fallas importantes en los sistemas de información, que afecten la operación normal del negocio y asegurar su recuperación oportuna.

Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad de los sistemas y operación en el menor tiempo posible

2. ALCANCE

Este procedimiento aplica para la continuidad y disponibilidad de los servicios misionales y los servicios TI que presta la organización para sus clientes internos y externos.

3. DEFINICIONES Y/O CONVENCIONES

Plan de continuidad y disponibilidad del negocio (PCD): Son todas las actividades y procedimientos aprobados que hacen posible a una organización responder a un evento en tal forma que las funciones críticas del negocio continúen sin interrupción o cambio significativo

Continuidad del servicio: Capacidad de gestionar riesgos y eventos que puedan

tener un grave impacto en los servicios con el fin de prestar de forma continua los servicios en los niveles acordados.

Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Interrupción: Acontecimiento ya sea previsto o imprevisto que causa una interrupción negativa no planificada respecto a la entrega de productos y/o servicios.

Procesos críticos: Actividades claves e imprescindibles para el negocio de la organización

Desastre: Cualquier evento que crea inhabilidad en una parte de la organización para proveer sus funciones críticas del negocio por algún periodo de tiempo

Fase de Recuperación: Es la estrategia que se sigue para restablecer las actividades críticas de la organización que atente contra la continuidad del negocio.

Análisis de Impacto del Negocio (BIA): Es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<u>Política de Continuidad y Disponibilidad del negocio</u>	Gerente General	PO-DIR-03 Política de Continuidad y Disponibilidad del negocio

<p>Evitar cualquier interrupción en los procesos del negocio que afecten la operación.</p> <p>Es responsabilidad de la Alta Dirección aprobar y mantener el plan de continuidad del negocio que cubra las actividades esenciales y críticas.</p> <p>Analizar, evaluar y tratar los riesgos para limitar las consecuencias de los diferentes incidentes y asegurar la recuperación inmediata de las operaciones esenciales.</p>		
<p><u>Generalidades</u></p> <p><input type="checkbox"/> El plan de continuidad de negocio está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.</p> <p><input type="checkbox"/> Todo el personal de la organización ésta entrenado y capacitado en los procedimientos definidos y conocen claramente los roles y responsabilidades que le competen en el marco de la continuidad del negocio, mediante labores periódicas de formación, divulgación y prueba del Plan de Contingencia del Negocio.</p> <p><input type="checkbox"/> En caso de presentarse un incidente significativo se aplicará los mecanismos de comunicación apropiados, tanto internos como externos, de acuerdo con las matrices de comunicación con las autoridades y con grupos de interés especial</p>	<p>Gerente General</p>	<p>FO-CAL-04 Asistencia a eventos de capacitación y/o formación</p>

<ul style="list-style-type: none"> □ El BIA debe actualizarse cada (1) año, o cada vez que un líder de proceso lo requiera. □ Los procesos críticos deben ser recuperados dentro de los márgenes de tiempo requeridos en el plan de Continuidad del Negocio. 		
<p>4.1 FASE 1 ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS</p> <p>Detectar la urgencia de recuperación del proceso y/o servicio y los riesgos a los que están expuestos y sobre esta base desarrollar: las estrategias de recuperación, el plan de continuidad/disponibilidad del negocio y de los servicios TI, de acuerdo a los siguientes análisis:</p>		
<p>4.1.1 Análisis de Impacto del negocio para la recuperación de los procesos/ servicios críticos (BIA)</p> <p>Determinar las actividades críticas y estimar el tiempo que la organización puede tolerar en caso de un incidente o desastre que afecte la disponibilidad y continuidad del negocio, apoyados en el IN-DIR-02 Análisis del impacto al negocio.</p>	Líder de proceso	IN-DIR-02 análisis del impacto al negocio BIA
<p>4.1.2 Análisis del riesgo</p> <p>Identificar las posibles amenazas a los activos</p>	Líder de proceso	IN-SIS-03 Análisis de riesgos para la

<p>de información y las vulnerabilidades que podrían ser aprovechadas por ser amenazadas con el fin de medir el nivel del riesgo y reducir el impacto que puede provocar un evento de desastre o una interrupción significativa en los procesos/ servicios críticos.</p> <p>La siguiente es la metodología de análisis de riesgos, el cual cubre los aspectos relacionados con:</p> <p>La identificación de los procesos críticas y sus activos de información</p> <p>Tasación del activo (confidencialidad, integridad, disponibilidad)</p> <p>Identificación de riesgos de continuidad (amenazas y vulnerabilidades)</p> <p>Probabilidad de ocurrencia del riesgo</p> <p>Nivel de riesgo</p> <p>Consecuencias</p> <p>Opciones de tratamiento</p> <p>Tratamiento</p> <p>Ver IN-SIS-03 Análisis de riesgos para la continuidad y disponibilidad de los procesos/servicios críticos</p>		<p>continuidad y disponibilidad de los procesos críticos</p> <p>RC-SIS-34</p> <p>Gestión de los riesgos de la seguridad de la información y de los servicios</p>
<p>4.2 Comunicación con clientes, proveedores y/o autoridades para atender eventos que puedan afectar la continuidad de los</p>		

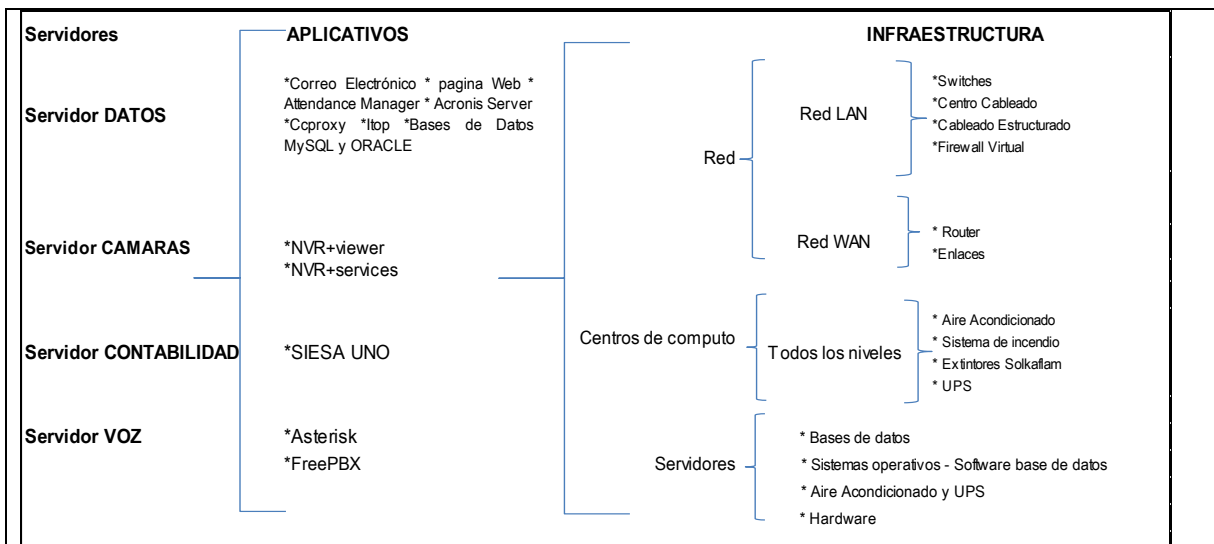
servicios de la organización						
Establecer comunicación con clientes, proveedores y/o autoridades de acuerdo a las siguientes matrices:						
CLIENTES Y PROVEEDORES						
RESPONSABE DE LA COMUNICACIÓN	CLIENTE O PROVEEDOR A CONTACTAR	NOMBRE DEL PROVEEDOR/ CLIENTE	NOMBRE DEL CONTACTO	TELEFON O FIJO	TELEFON O CELULAR	DIRECCIÓN
Mauricio Andrés Agudelo Juan Sebastián Cruz	Clientes en general		Clientes- Biblioteca de proyectos			
Rodrigo Arenas Orozco	Proveedor de herrajes	Fejumig SAS	Fernando Vargas		31371086 84	Cra 3 No 45-35 Pereira
		Hierros Antomar	Carlos Quintero	3392000		Calle 25 No. 10-59 Dosquebradas
Juan David Aguirre	Proveedor de fibra óptica	Energitel	Carlos Mario Villa	6) 3154498		Cra 8 N°14-70 Multi centro La Macarena BGA 6 Dosquebradas
		Microlink	Santiago Jaramillo Rodríguez	(1) 3147240		Cll 59 N°9-44 piso 2 Bogotá
	Proveedor de elementos de ferretería	Punto Eléctrico ferretero	Luis Alfonso Peña	3341312		Calle 16 No 9-33 Centro Pereira
		RG Distribuciones	Alejandro Castaño	(6) 3301216		Cll 8 # 9-46 Urb El Acero La Popa
Para la comunicación con las autoridades						

ENTIDADES	TELEFONO EMERGENCIA	TELEFONO FIJO	TELEFONO CELULAR	DIRECCIÓN	RESPONSABLE DE LA COMUNICACIÓN
Policía Nacional	112	3327622	018000 - 910600 018000 - 910112	Cra 4Bis Nro. 24-39	Director Operativo Coordinador de Proyectos Telmex
Cuadrante policía La Graciela Dosquebradas		3327622	3117772625	Barrio la Graciela	Director Operativo Coordinador de Proyectos Telmex
Bomberos	119	3439119 3284050	3227945	Diagonal 66 Vía la Romelia el Pollo	Jefe de Talento Humano Coord. Administrativa y Financiera
Defensa Civil		3213964- 3214694		Cr 19 Nro. 17 - 102 Urb. Basconia	Jefe de Talento Humano Coord. Administrativa y Financiera
Fiscalía General de la nación.		3267673 ext. 123 3267649 3267648		Cl. 38 Nro. 6- 50	Director Operativo Coordinador de Proyectos Telmex
Gaula Ejercito	147	3261070	3132970719	Carrera 11 No 42-46 Barrio Maraya Pereira	Director Operativo Coord. Administrativa y Financiera
Gaula policía nacional	165	3266798 Ext. 165 - 018000911129		Av. De Las Américas Comando de Policía	Director Operativo Coord. Administrativa y Financiera
Centro regulador de urgencias emergencias y desastres	125	096-3204278 096-3204295		Gobernación de Risaralda piso 2	Jefe de Talento Humano Coord. Administrativa y Financiera
4.3 FASE 2 SELECCIÓN DE ESTRATEGIAS Mantener o reanudar las actividades de la organización y sus procesos ante una				Gerente general	PC-DIR-05 Plan de Continuidad y Disponibilidad del negocio y de los servicios TI

<p>interrupción inesperada utilizando las siguientes estrategias de recuperación:</p> <p>Ausencia de personal</p> <p>Sitio alternativo</p> <p>Fallas tecnológicas</p>		<p>PC-DIR-06 Plan de Contingencia para los servicios TI</p>
<p>4.3.1 Estrategia por Ausencia de personal</p> <p>Se presenta cuando el colaborador que ejecuta los procesos críticos no puede asistir a trabajar para desarrollar las actividades propias de su cargo.</p> <p>Se establece la siguiente cadena de comunicación:</p> <p>El colaborador ausente se comunica con el Jefe inmediato.</p> <p>El Jefe inmediato comunica el evento al Jefe del Área y activa la contingencia por “Ausencia de Personal”.</p> <p>El Jefe Inmediato distribuye las actividades claves o asigna funciones al colaborador Back-up. De ser necesario, solicita al Coordinador TIC la reasignación de perfiles.</p> <p>El Jefe inmediato confirma al líder del PCD la continuidad exitosa de los procesos.</p> <p>El proceso de Talento Humano mantiene la información de los colaboradores actualizada que permite comunicarse con ellos en el evento que</p>	<p>Director Operativo</p>	<p>FO-HUM-24 Listado maestro del personal</p>

<p>se encuentren fuera de las instalaciones.</p>		
<p>4.3.2 Estrategia Sitio Alterno</p> <p>La alternativa de traslado del personal se presenta en el evento que los colaboradores no puedan acceder a las instalaciones de la organización y de esta manera se afronta un evento de contingencia permitiendo la continuidad de las operaciones de los procesos críticos desde un sitio alternativo de operación.</p> <p>A continuación enunciamos el procedimiento para activar la Estrategia de “Sitio Alterno”:</p> <p>El líder del comité de crisis activa el PCD y comunica el evento el incidente al comité de recuperación y logística, solicitando el desplazamiento al “Lugar alternativo de trabajo”, este lugar será en la ciudad de Medellín en la Dirección: Carrera 51B No.12 Sur-46 Guayabal, donde se cuenta con:</p> <ul style="list-style-type: none"> -Disponibilidad de vías de acceso principales y secundarias para tránsito fluido -Dispone de sistemas de transporte público adecuado y suficiente. -Dispone de servicios de electricidad, de agua, de comunicación. 	<p>Comité de crisis</p> <p>Comité de recuperación</p> <p>Comité de Logística</p>	

<p>- El sitio alterno está equipado con réplicas de los equipos informáticos y telecomunicaciones, así como enlaces de conexión y espacio para atención al público y operar negocios. Ver numeral 4.3</p> <p>Los comités definidos para atender la continuidad, ejecutarán sus responsabilidades de acuerdo al numeral 4.4.1 “Responsabilidades de los equipos necesarios para el desarrollo del PCD”</p>		
<p>4.3.3 Estrategia Tecnológica</p> <p>La contingencia se presenta cuando el hardware y/o software presenta fallas, o por interrupción prolongada de telecomunicaciones.</p> <p>El proceso de Seguridad de la información tiene estructurado el siguiente Plan de Continuidad para los aplicativos e infraestructura del negocio:</p>		



De todas las alternativas existentes hay que elegir la más adecuada en cada caso. Dependerá de las necesidades de la organización, en cuanto a tiempos de recuperación, costos económicos, recursos, etc.

Además deberá considerarse otros factores como:

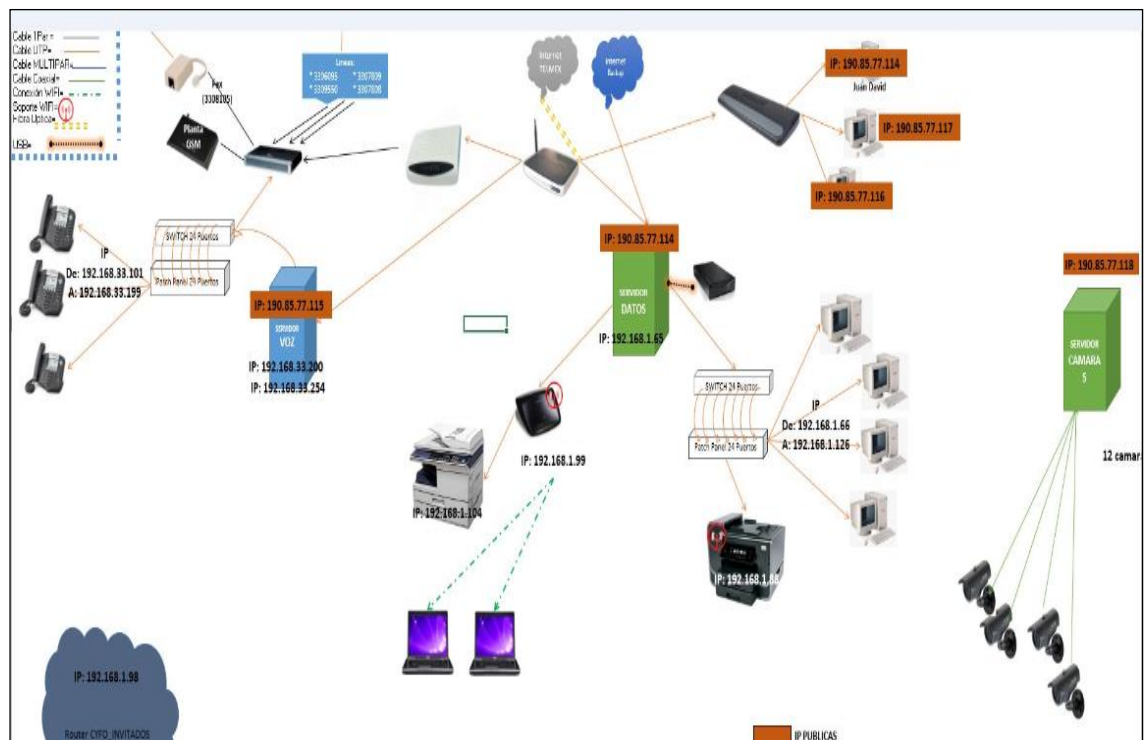
- Ubicación y superficie requerida
 - ✓ Espacio suficiente
 - ✓ Zonas acondicionadas para acoger a personal
- Recursos técnicos necesarios:
 - ✓ Hardware
 - ✓ Software
 - ✓ Comunicaciones
 - ✓ Datos de respaldo
- Recursos humanos requeridos
 - ✓ Recursos materiales y de infraestructura
 - ✓ Servicios auxiliares necesarios
 - ✓ Tiempos de activación
 - ✓ o Costo

4.4 Redundancia de la infraestructura de procesamiento de la información

Utilizar el esquema Activo-Activo para duplicar la redundancia, así funcionan simultáneamente los componentes que integran la infraestructura TI.

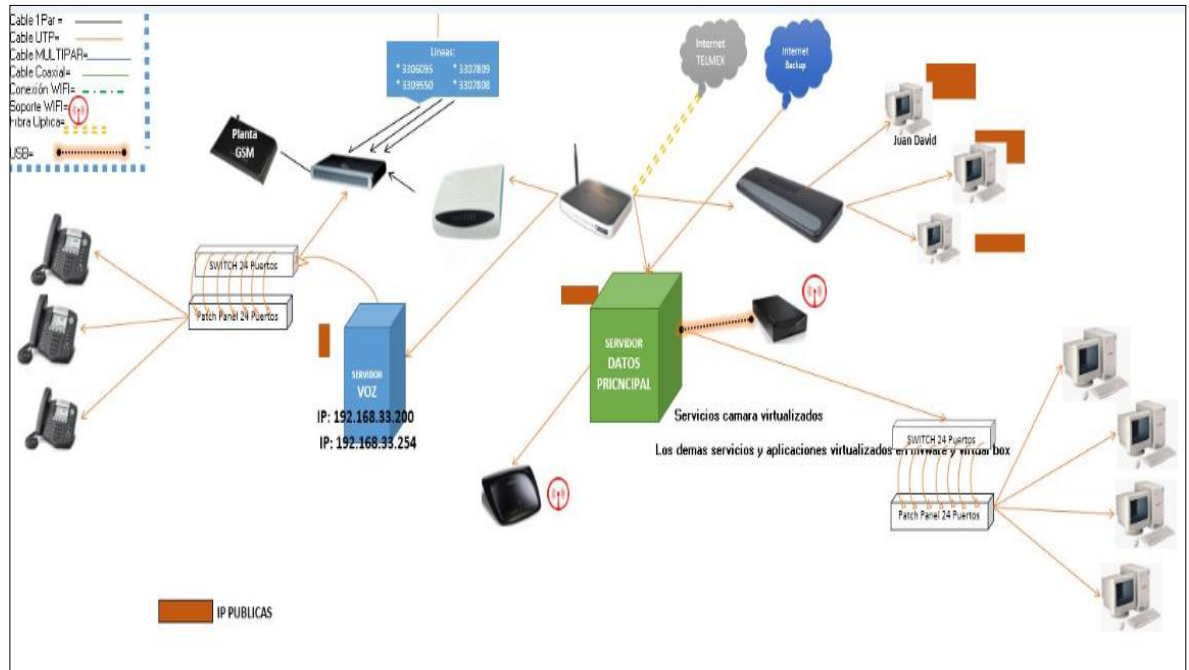
A continuación se identifica la infraestructura TI del sitio principal y del sitio de recuperación

Gráfico 2: Sitio principal



Fuente: Elaboración propia

Gráfico 3: Sitio de recuperación



Fuente: Elaboración propia

4.5 FASE 3 DESARROLLO DEL PLAN

Para desarrollar el Plan de Continuidad se define:

- Los equipos necesarios para el desarrollo del Plan y sus responsabilidades.
- El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan.
- Los procedimientos de actuación ante incidentes.
- La estrategia de vuelta a la normalidad

4.5.1 Responsabilidades de los equipos necesarios para el desarrollo del PCD

<p>Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan.</p> <p>Aunque la composición y número de equipos puede variar según el tipo de estrategia de recuperación, a continuación se muestran los equipos que formar parte del Plan:</p> <p>-Comité de Crisis: Encargado de dirigir las acciones durante la contingencia y recuperación.</p> <p>-Equipo de Recuperación: Su función es restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.).</p> <p>-Equipo Logístico: Responsable de toda la logística necesaria en el esfuerzo de recuperación</p> <p>-Equipo de las Unidades de Negocio: Encargados de la realización de pruebas que verifiquen la recuperación de los sistemas y/o procesos críticos.</p> <p>-Equipo de Relaciones Públicas: Encargado de las comunicaciones con proveedores, colaboradores, socios y clientes.</p>		
---	--	--

COMITÉ DE CRISIS	
ROL / NOMBRE	RESPONSABILIDADES
<p>Líder: Luis Felipe Ramírez</p> <p>Cargo: Gerente General</p>	<p>El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación.</p>

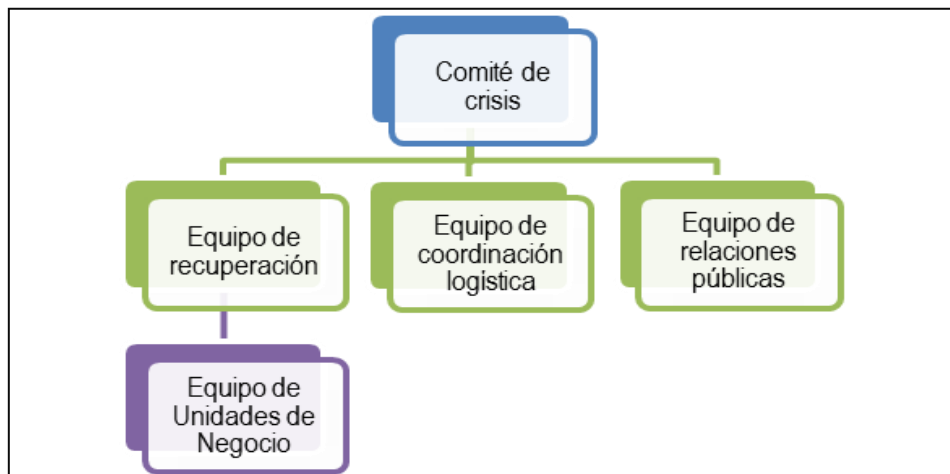
<p>Teléfono:3206986130</p> <p>Integrante: Mauricio Andrés Agudelo</p> <p>Cargo: Director Operativo</p> <p>Teléfono: 3137451717</p> <p>Integrante: Norma Liliana Arias</p> <p>Cargo: Coord. Adm y Financiera</p> <p>Teléfono:</p>	<p>Este Comité debe tomar las decisiones “clave” durante los incidentes, además de hacer de enlace con la dirección de la organización, manteniéndoles informados de la situación regularmente.</p> <p>Las principales tareas y responsabilidades de este comité son:</p> <ul style="list-style-type: none"> • Análisis de la situación. • Decisión de activar o no el Plan de Continuidad. • Iniciar el proceso de notificación a los empleados a través de los diferentes responsables. • Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación
COMITÉ DE RECUPERACIÓN	
ROL / NOMBRE	RESPONSABILIDADES
<p>-Líder de la recuperación operativa: Mauricio Andrés Agudelo</p> <p>Teléfono: 3137451717</p> <p>-Contacto Secundario de Recuperación operativa: William Álvarez Toro</p> <p>Teléfono: 3137400491</p> <p>-Líder de la Recuperación tecnológica: Juan David Aguirre</p> <p>Teléfono: 3172429102</p>	<p>El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación.</p> <p>Esto incluye: infraestructura física, servidores, PC's, comunicaciones de voz y datos, backup y cualquier otro elemento necesario para la restauración de un servicio.</p>

<p>-Contacto Secundario de Recuperación tecnológica: Leiner Andrés López Teléfono: 3128046057</p> <p>-Líder de la recuperación física: Norma Liliana Arias Teléfono: 3105079999</p> <p>-Contacto secundario de recuperación física: Valentina Gómez Teléfono:3183919886</p>	
COMITÉ DE LÓGISTICA	
ROL / NOMBRE	RESPONSABILIDADES
<p>-Líder del comité de logística: John Faber Salazar Teléfono:3136233729</p> <p>-Contacto Secundario de comité de logística: William Álvarez Toro Teléfono: 3137400491</p>	<p>Este equipo es responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como:</p> <ul style="list-style-type: none"> ✓ Transporte de material y personas (si es necesario) al lugar de recuperación ✓ Suministros de oficina. ✓ Comida. ✓ Reservas de hotel, si son necesarias. ✓ Contacto con los proveedores. <p>Este equipo debe trabajar conjuntamente con los demás, para asegurar que todas las necesidades logísticas sean cubiertas.</p>

COMITÉ DE RELACIONES PÚBLICAS Y ATENCIÓN A CLIENTES	
ROL / NOMBRE	RESPONSABILIDADES
<p>Líder de las relaciones publicas: Norma Liliana Arias</p> <p>Teléfono:3105079999</p> <p>-Contacto secundario para las relaciones públicas: Anthony Arévalo</p> <p>Teléfono:3137400430</p>	<p>Canalizar la información que se realiza al exterior en un solo punto para que los datos sean referidos desde una sola fuente. Sus funciones principales son:</p> <ul style="list-style-type: none"> • Elaboración de comunicados • Comunicación con las partes implicadas <p>Uno de los valores más importantes de una organización son sus clientes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación.</p>
COMITÉ UNIDADES DEL NEGOCIO	
ROL / NOMBRE	RESPONSABILIDADES
<p>-Líder del comité de unidades del negocio (informática): Juan David Aguirre</p> <p>Teléfono: 3172429102</p> <p>-Contacto Secundario del comité de unidades del negocio (informática): Leiner Andrés López</p> <p>Teléfono: 3128046057</p> <p>-Líder del comité de unidades del negocio (operacional): Mauricio Andrés Agudelo</p> <p>Teléfono: 3137451717</p>	<p>Estos equipos estarán formados por las personas que trabajan con las aplicaciones críticas, y serán los encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar.</p> <p>Cada equipo deberá configurar las diferentes pruebas que deberán realizar para los sistemas.</p>

<p>-Contacto Secundario del comité de unidades del negocio: William Álvarez Toro</p> <p>Teléfono: 3137400491</p>	
--	--

Figura 5: Equipos para ejecutar el plan de continuidad y disponibilidad.

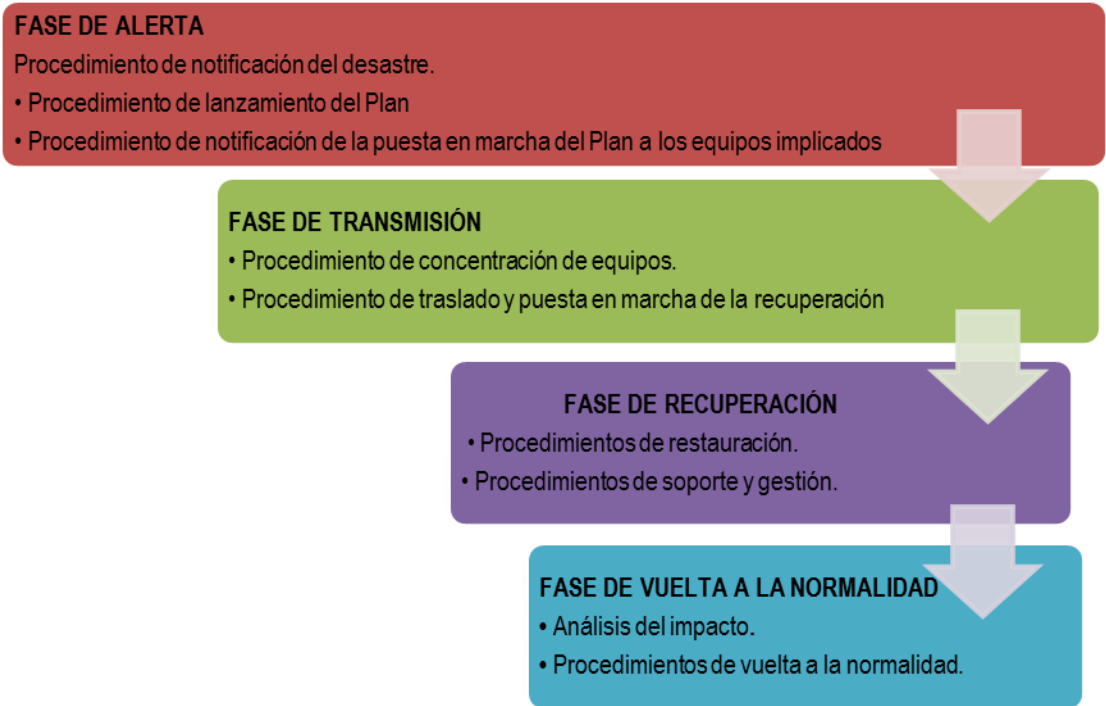


Fuente: Elaboración propia.

4.5.2 El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan.

A continuación se desarrollan los procedimientos a seguir, y su actuación para cada una de las fases de la activación del Plan de Continuidad.

Figura 6: Fases de activación del plan de continuidad



Fuente: Elaboración propia

<p>4.5.3 Fase de Alerta</p> <p>Al momento de identificar cualquier evento que implique la pérdida parcial o total de uno o varios servicios críticos se actuará de la siguiente manera:</p> <p><u>Notificación</u></p> <p>Cualquier colaborador de la organización que sea consciente de un incidente grave que pueda afectar el normal funcionamiento de la empresa, debe comunicarlo a su Jefe inmediato proporcionando el mayor detalle posible en la</p>	<p>Colaboradores</p> <p>Comité de crisis</p>	
--	--	--

descripción de los hechos.

El Jefe Inmediato comunica al Coordinador TIC los incidentes informáticos o al Director Operativo los incidentes operacionales, con el fin de evaluar la situación e informar al Responsable del Comité de Crisis.

Evento	Acción
Incendio Inundación Tempestad Robo Disturbios Virus Pérdida de información	Aviso inmediato con el máximo detalle posible al Jefe Inmediato.

Evaluación

Una vez que un miembro del Comité de Crisis es contactado e informado del incidente, se procederá a evaluar la situación inicial de los daños con la recopilación de la mayor información posible.

El Comité informará a los responsables de los distintos equipos de lo ocurrido y de la situación en ese momento para que permanezcan en situación de espera, hasta que se tome la decisión de disparar el Plan o iniciar otro tipo de

estrategia							
<table border="1"> <thead> <tr> <th data-bbox="295 336 544 415">Evento</th> <th data-bbox="544 336 995 415">Acción</th> </tr> </thead> <tbody> <tr> <td data-bbox="295 415 544 1092"> Conocimiento por algún miembro del Comité de incidente ocurrido. </td> <td data-bbox="544 415 995 1092"> <p>El equipo del Comité se reunirá en un lugar acordado previamente y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad.</p> <p>Será necesario informar de la situación a los siguientes responsables:</p> <ul style="list-style-type: none"> • Responsable de Seguridad. • Comité de Dirección de la Empresa. • Relaciones Públicas. • Equipo de Recuperación. • Responsable de los Equipos. </td> </tr> </tbody> </table>		Evento	Acción	Conocimiento por algún miembro del Comité de incidente ocurrido.	<p>El equipo del Comité se reunirá en un lugar acordado previamente y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad.</p> <p>Será necesario informar de la situación a los siguientes responsables:</p> <ul style="list-style-type: none"> • Responsable de Seguridad. • Comité de Dirección de la Empresa. • Relaciones Públicas. • Equipo de Recuperación. • Responsable de los Equipos. 		
Evento	Acción						
Conocimiento por algún miembro del Comité de incidente ocurrido.	<p>El equipo del Comité se reunirá en un lugar acordado previamente y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad.</p> <p>Será necesario informar de la situación a los siguientes responsables:</p> <ul style="list-style-type: none"> • Responsable de Seguridad. • Comité de Dirección de la Empresa. • Relaciones Públicas. • Equipo de Recuperación. • Responsable de los Equipos. 						
<p><u>Ejecución del Plan</u></p> <p>Una vez que el Comité de Crisis ha decidido poner en marcha el Plan de Recuperación, se deben convocar a los Responsables y componentes de cada equipo la situación de inicio de las actividades del Plan para comenzar los procedimientos de actuación de cada uno de ellos.</p>							
4.5.4 Fase de Transición							

<p>La Fase de Transición es la fase previa a la de recuperación de los sistemas. Es importante que en esta fase exista una coordinación entre los diferentes equipos y equipos de logística, ya que son éstos los encargados de que todo esté disponible para comenzar la recuperación en el menor tiempo posible.</p> <p>Podemos dividir la fase de transición en dos partes principalmente:</p> <ul style="list-style-type: none"> • Procedimientos de concentración y traslado de personas y equipos. • Procedimientos de puesta en marcha del centro de recuperación. <p>Ambos procedimientos son la base del proceso de recuperación de los sistemas. Si esta parte falla, no será posible comenzar la recuperación, y por tanto el Plan de Continuidad fallará.</p> <p>A continuación pasamos a describir de manera detallada cada uno de los procedimientos y equipos que deben interactuar en esta fase de transición.</p> <p style="text-align: center;"><u>Procedimientos de concentración y traslado de material y personas</u></p> <p>Dependiendo de la solución final que se decida como estrategia de respaldo, este procedimiento puede variar.</p>	<p>Comité de logística</p> <p>Comité de recuperación</p>	
---	--	--

<p>Una vez avisados los equipos y puesto en marcha el Plan, deberán acudir al centro de reunión. En el caso de que la emergencia se declare en horas de trabajo, se tomará como punto de encuentro la glorieta del Parque Industrial.</p> <p>Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como centro de respaldo, o cualquier otro designado por el Comité de Dirección de Crisis.</p> <p>Además del traslado de personas al centro de recuperación (si es necesario) hay que realizar una importante labor de coordinación para el traslado de todo el material necesario para poner en marcha el centro de recuperación (cintas de backup, material de oficina, documentación, ...)</p> <p style="text-align: center;"><u>Procedimientos de puesta en marcha del centro de recuperación</u></p> <p>Una vez concentrados los distintos equipos que van a intervenir en la recuperación, y con todos los elementos necesarios disponibles para comenzar la recuperación, hay que poner en marcha este centro, estableciendo la infraestructura necesaria, tanto de software como de comunicaciones, de acuerdo al plan PC-DIR-05.</p>		
---	--	--

4.5.5 Fase de Recuperación

Una vez que hemos establecido las bases para comenzar la recuperación, se procederá a la carga de datos y a la restauración de los servicios críticos. Este proceso y el anterior suele precisar los mayores esfuerzos e intervenciones para cumplir con los plazos fijados.

Podemos dividir esta fase en dos:

- Procedimientos de Restauración
- Procedimientos de Gestión y Soporte

Procedimientos de Restauración

Estos procedimientos se refieren a las acciones que se llevan a cabo para restaurar los sistemas críticos.

Procedimientos de soporte y gestión

Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se reanude el negocio con las máximas garantías de éxito. Los integrantes del equipo de unidades de negocio serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

<p>4.5.6 Fase de vuelta a la Normalidad. Fin de la emergencia</p> <p>Una vez con los procesos críticos en marcha y solventada la contingencia, debemos plantearnos las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento. Para ello vamos a dividir esta fase en diferentes procedimientos:</p> <ul style="list-style-type: none"> • Análisis del impacto. • Procedimientos de vuelta a la normalidad <p style="text-align: center;"><u>Análisis del impacto</u></p> <p>El análisis de impacto pretende realizar una valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad.</p> <p style="text-align: center;"><u>Procedimientos de vuelta a la normalidad</u></p> <p>Una vez determinado el impacto deben establecerse los mecanismos que en la medida de lo posible lleven a recuperar la normalidad total de funcionamiento. Estas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.</p>	<p>Comité de recuperación</p>	
<p>4.5.7 Generación de informes y evaluación</p> <p>Una vez solventado el incidente y vuelto a la normalidad, cada equipo deberá realizar un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de</p>		

<p>Continuidad, los tiempos empleados, dificultades con las que se encontraron, etc.</p> <p>Toda esta información servirá para valorar si el Plan ha funcionado según lo planeado, así como conocer los posibles fallos, y en su caso, tenerlos en cuenta para la adecuación del mismo.</p>		
<p>4.6 FASE 4 PRUEBAS Y MANTENIMIENTO</p> <p>Probar la efectividad de las estrategias diseñadas y permitir el continuo mejoramiento del PCN de la organización. Esta etapa le da a la empresa la oportunidad de identificar y prevenir problemas y fallas del plan de continuidad de manera que puedan ser atendidas, preparando el negocio para la emergencia real.</p> <p>Los objetivos del plan de pruebas son:</p> <ul style="list-style-type: none"> • Practicar los procedimientos ante un incidente o desastre. • Identificar áreas que necesitan mejora. • Permitir al PCN permanecer activo, actualizado, entendible y usable. • Demostrar la habilidad de recuperación. • Concienciación y formación para los empleados a través de la realización de pruebas. 		

<p>Alcance de las pruebas</p> <p>Las pruebas deben ejecutarse durante un tiempo en el que las afectaciones a la operación normal sean mínimas y deben comprender los elementos críticos y simular condiciones de proceso, aunque se realicen fuera del horario laboral de la organización.</p> <p>Las pruebas deben incluir las siguientes tareas:</p> <ul style="list-style-type: none"> • Verificar la totalidad y precisión del Plan. • Evaluar el desempeño del personal involucrado. • Evaluar la coordinación entre los miembros del grupo de contingencia, proveedores y otros terceros. • Identificar la capacidad de recuperar registros e información vital. • Medir el desempeño de los sistemas operativos y computacionales. <p>Durante esta etapa se debe establecer un programa de pruebas con escenarios simulados, planeados en el tiempo, teniendo en cuenta los requerimientos de cada prueba y con una revisión exhaustiva de los resultados de las mismas, para generar mejoras a los planes.</p>		
--	--	--

<p>4.6.1 Tipos de pruebas:</p> <p><u>Simulaciones /escritorio</u></p> <p>Técnica utilizada: -Se ejecuta con previo aviso. -Creación de un nuevo escenario</p> <p>- Operación: Se realiza el ejercicio de papel de un escenario de desastre que se realiza en la sala de juntas</p> <p><u>Restauración</u></p> <p>- Técnica utilizada: Creación de un escenario -Seguimiento en vivo de todas las estrategias de recuperación. -Se ejecuta con previo aviso -Apoyo de los proveedores de recuperación</p> <p>- Operación: Prueba integrada con todos los elementos que hacen parte del plan de contingencia</p>																				
<p>4.6.2 Plan de Pruebas</p> <p>Realizar las pruebas de continuidad de acuerdo a las fechas establecidas en el cronograma</p> <table border="1" data-bbox="293 1478 997 1822"> <thead> <tr> <th colspan="6">CRONOGRAMA DE PRUEBAS AL PLAN DE CONTINUIDAD Y DISPONIBILIDAD 2014</th> </tr> <tr> <th>TIPO DE PRUEBA</th> <th>FRECUENCIA</th> <th>ENE-MAR</th> <th>ABR-JUN</th> <th>JUL-SEP</th> <th>OCT-DIC</th> </tr> </thead> <tbody> <tr> <td>Simulacro /Escritorio</td> <td>Trimestral</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> </tr> </tbody> </table>	CRONOGRAMA DE PRUEBAS AL PLAN DE CONTINUIDAD Y DISPONIBILIDAD 2014						TIPO DE PRUEBA	FRECUENCIA	ENE-MAR	ABR-JUN	JUL-SEP	OCT-DIC	Simulacro /Escritorio	Trimestral	X	X	X	X		<p>RC-DIR-10 Pruebas al Plan de</p>
CRONOGRAMA DE PRUEBAS AL PLAN DE CONTINUIDAD Y DISPONIBILIDAD 2014																				
TIPO DE PRUEBA	FRECUENCIA	ENE-MAR	ABR-JUN	JUL-SEP	OCT-DIC															
Simulacro /Escritorio	Trimestral	X	X	X	X															

Restauración	Semestral	X	X		<p>continuidad/disponibilidad</p> <p>RC-DIR-12 Encuesta para las pruebas del plan de continuidad/disponibilidad</p> <p>PR-SGI-05 Acciones correctivas, preventivas y/o de mejora.</p> <p>RC-DIR-14 Eficacia de las pruebas de restauración</p>
<p>Diligenciar el registro RC-DIR-10 de las pruebas al plan de Continuidad y Disponibilidad, estableciendo el objetivo de la prueba, los observadores, los participantes, la descripción del acontecimiento desfavorable y de sus consecuencias para la organización, los antecedentes y el alcance de la prueba.</p> <p>Este documento se debe desarrollar previo a la ejecución de la prueba por el Líder de PCN responsable o los delegados.</p> <p><u>Ejecución de las Pruebas</u></p> <p>Durante la ejecución de las pruebas deben registrar las actividades desarrolladas por los participantes, asignar una calificación al desempeño en la ejecución de la actividad y el tiempo empleado para el mismo; estos deben ser semejantes a las planeadas en el “Plan de recuperación de los servicios y procesos de la organización para garantizar la continuidad” PC-DIR-05. Adicionalmente, si se presentan incidentes dentro de la prueba estas se deben registrar en el espacio de las observaciones.</p> <p><u>Retorno a la Normalidad</u></p>					

<p>En este reporte se relacionan las actividades que se ejecutan para retornar a la operación normal, caso devolución a los puestos de trabajo, captura de las operaciones que no se procesaron en un aplicativo, entre otras.</p> <p>Aplicar una vez finalice la ejecución de la prueba el registro RC-DIR-12 “Encuestas de las pruebas del plan de continuidad y disponibilidad” en donde se busca determinar el grado de satisfacción con la prueba. La conforman aspectos como: duración de la prueba, cómo fueron las instrucciones que recibieron para ejecutar la prueba, la comunicación de la misma, y se identifican las oportunidades de Mejora.</p> <p><u>Eficacia de la prueba</u></p> <p>El líder del PNC debe evaluar la eficacia de la prueba recopilando y analizando los datos suministrados en las encuestas de las pruebas; registrar en el RC- DIR-14 “Eficacia de las pruebas de restauración”, los tiempos, procedimientos y funcionalidad de las fases de ejecución y retorno a la normalidad y definir las conclusiones y resultados obtenidos de la prueba con el fin de identificar oportunidades para tomar acciones correctivas, preventivas y/o de mejora.</p> <p>Volver a probar el plan después de:</p> <ul style="list-style-type: none"> -Implementar cambios significativos en el entorno 		
---	--	--

<p>del negocio.</p> <p>-Cuando se ejecute el plan de continuidad y disponibilidad.</p>		
<p>4.6.3 Mantenimiento al plan de Continuidad y Disponibilidad</p> <p>Asegurar que todas las áreas permanezcan preparadas para el manejo de incidentes relacionados a la continuidad del negocio a pesar de los cambios a las personas, los procesos y la tecnología.</p> <p>Los principales disparadores del mantenimientos para el PCD son:</p> <ul style="list-style-type: none"> •Revisiones periódicas (anual). •Adecuaciones identificadas por el control de cambios. •Adecuaciones identificadas como resultado de pruebas o ejercicios. <p>Mantener por parte del Coordinadora del SGI la lista de contactos con autoridades actualizada y publicada en las zonas físicas seguras ubicadas así:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Edificación principal, nivel 2, área administrativa <input type="checkbox"/> Edificación principal, nivel 1, área operativa 	<p>Coordinador TIC</p> <p>Coordinador SGI</p>	<p>PC-CAL-08</p> <p>Matriz de comunicación contacto con autoridades</p> <p>PC-CAL-09</p> <p>Matriz de comunicación con grupos de interés especial</p>

<ul style="list-style-type: none"> <input type="checkbox"/> Edificación principal, subnivel, área de almacén y <input type="checkbox"/> área de recepción <p>Mantener por parte del Coordinador TIC una copia actualizada de la base de datos de la gestión de la configuración (CMDB) con una periodicidad semanal, en un servicio de almacenamiento de información temporal (nube).</p>		
<p>5. Entrenamiento</p> <p>Lograr la participación y compromiso del personal involucrado en el PCD y de todos los colaboradores de la organización.</p> <p>Concientizar y entrenar al personal en los procedimientos a seguir en caso de un incidente o desastre.</p> <p>Entre los puntos a considerar en el temario de entrenamiento inicial están:</p> <ul style="list-style-type: none"> •Estrategias del plan •Estructura y contenido de los planes. •Responsabilidades de los equipos que ejecutarán el plan de continuidad y disponibilidad. 	<p>Coordinador TIC</p> <p>Coordinador SGI</p>	<p>FO-CAL-04</p> <p>Asistencia a eventos de capacitación y/o formación</p>
<p>6. Control de cambios al PCD</p> <p>Evaluar por parte del proceso de gestión de cambios, el impacto que las solicitudes de cambio en los servicios TI sobre el plan de continuidad y disponibilidad.</p>	<p>Coordinador TIC</p>	<p>PR-SIS-15</p> <p>Gestión de Cambios</p>

8.2.3 Procedimiento Vinculación, inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación

Procedimiento Vinculación, inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación	<u>Código: PR-HUM-01</u>
	<u>Versión:01</u>

1. OBJETO

Describir como se debe llevar a cabo de manera eficaz el proceso de selección y vinculación de personal con las características, aptitudes y actitudes requeridas a fin de proveer el talento humano idóneo y necesario para el desarrollo de las actividades individuales y colectivas de la Organización, así mismo define los procesos de inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación del personal.

2. ALCANCE

El presente procedimiento aplica a todo el personal que ingrese o que forme parte de CYFO Comunicaciones y Fibra Óptica CIA. S.A. y describe los pasos generales que se requieren para las actividades de selección, vinculación, inducción, reinducción, entrenamiento, evaluación de desempeño, y desvinculación del personal

3. DEFINICIONES Y/O CONVENCIONES

Selección: Consiste en una serie de pasos específicos que se emplean para decidir qué solicitantes deben ser contratados.

Vinculación: Es el proceso mediante el cual se relaciona una persona con otra o se crea una dependencia entre alguna de las dos.

Inducción: Proceso dirigido a iniciar al nuevo colaborador en su integración a la cultura organizacional de la empresa, además de brindar información general, amplia y suficiente que permita la ubicación del empleado y de su rol dentro de la organización para fortalecer su sentido de pertenencia y la seguridad para realizar su trabajo de manera autónoma.

Reinducción: Hace parte de un proceso progresivo de formación y aprendizaje de los colaboradores y personal administrativo que actualmente hacen parte de la compañía, ya que es indispensable para su desarrollo humano en la entidad y para que ésta pueda cumplir adecuadamente su misión. Están dirigidos a actualizar a los colaboradores en relación con las políticas, normas y procedimientos de cada nueva administración y a reorientar su integración a la cultura organizacional

Entrenamiento: Enseñanza organizada que está dirigida al aumento de la capacidad de rendimiento físico, Psíquico, Intelectual o técnico de un individuo.

Fuentes de reclutamiento: Son las diferentes fuentes potenciales para la consecución de posibles aspirantes para cubrir una vacante y se clasifican de la siguiente manera:

Promociones Internas: Es la búsqueda al interior de la organización para detectar si existe personal que cumple con el perfil del cargo y las competencias que se pretende proveer en un cargo específico.

Referidos: Son los posibles candidatos recomendados por los colaboradores activos de la compañía para ocupar una vacante.

Candidatos espontáneos: Son las personas que envían directamente su hoja de vida a la Organización.

Convocatorias abiertas: Es la publicación de la necesidad de cubrir una vacantes en anuncios de prensa, agencias de empleo, SENA (Servicio Nacional de Aprendizaje), asociaciones de Profesionales, universidades, agencias de empleos temporales o empresas con servicios especializados

Desvinculación: Proceso mediante el cual se realiza el reporte de la novedad de retiro de todas las

Terminación del contrato: Es el proceso mediante el cual se finaliza el vínculo laboral.

Prueba Idoneidad: Tienen como objetivo evaluar el grado de conocimientos y habilidades adquiridos mediante el estudio, la práctica o el ejercicio de sus actividades considerando pertinente la realización de pruebas escritas o prácticas para su comprobación.

Contrato de trabajo por obra: Aquellos contratos realizados para una obra determinada o servicio específico y de duración determinada.

Contrato a término indefinido: Aquellos contratos que se celebran sin determinar su fecha de término.

Sistema de Seguridad Social: Derechos otorgados al trabajador por medio de La Ley 100 de 1993 la cual se compone de los siguientes subsistemas: Pensiones, Salud, Riesgos Profesionales y Servicios Sociales complementario

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
4.1 Solicitar o requerir personal	Jefe inmediato	FO-HUM-01

<p>Notificar al Jefe de Talento humano la necesidad de cubrir una vacante diligenciando el FO-HUM-01 en el numeral 1, firmado por el Jefe inmediato que solicita cubrir la vacante y con las autorizaciones requeridas</p> <p>Firmas de autorización:</p> <p>a) Si el origen de la vacante es por reemplazo de personal o por contratación temporal, se requiere la firma de la dirección a la cual hace parte el nuevo cargo.</p> <p>b) Si el origen de la vacante es puesto de nueva creación o reposición con mayor sueldo, se deberá contar con las firmas anteriores y del Gerente General</p>	<p>Direcciones</p> <p>Gerente General</p> <p>Jefe de Talento Humano</p>	<p>Requisición de personal</p>
<p>4.2 Convocatorias al cargo</p> <p>Efectuar la convocatoria de aspirantes al cargo utilizando las fuentes de reclutamiento establecidas por la compañía como promociones internas, referidos, candidatos espontáneos y convocatorias abiertas.</p>	<p>Jefe de Talento Humano</p>	
<p>4.3. Selección de personal</p> <p>4.3.1 Selección de hojas de vida de personal nuevo</p>	<p>Jefe de Talento Humano</p>	<p>RC-HUM-01</p> <p>Cargo de aspirantes</p>

<p>Clasificar e identificar diligenciando el registro de aspirantes al cargo para tabular las hojas de vida de los aspirantes que cumplen con los requerimientos del cargo a cubrir y citar a los opcionados a entrevista con el jefe inmediato.</p> <p>No se tendrán en cuenta las hojas de vida de candidatos que tengan vínculos familiares con colaboradores activos.</p> <p>Verificar los antecedentes por las siguientes páginas web: https://antecedentes.policia.gov.co:7005/WebJudicial/index.xht http://www.procuraduria.gov.co/portal/antecedentes.html y dejar como constancia el documento generado de la consulta.</p> <p>Realizar la entrevista por parte del jefe inmediato con el fin de comprobar la idoneidad del aspirante.</p> <p>Aplicar, una vez terminada la entrevista, el test de personalidad de los 16 factores.</p> <p>Tabular las respuestas del test por medio de la página web: http://www.psicologia-online.com/test/test_personalidad_16_factores/pro_16pf.php; con estos resultados se</p>		<p>FO-HUM-07</p> <p>Entrevista del personal nuevo</p> <p>Documento de origen externo</p> <p>Test de personalidad del 16 factores</p> <p>Antecedentes disciplinarios de la policía y procuraduría</p> <p>MC-HUM-02</p> <p>Manual de competencias</p> <p>FO-HUM-03</p> <p>Requisitos de ingreso</p>
---	--	---

<p>alimenta el nivel de competencia del aspirante en cuanto a las habilidades.</p> <p>Entregar al área de Talento Humano el nombre del candidato seleccionado con el de realizar las respectivas validaciones de la información suministrada en la hoja de vida y otros requeridos por la organización, así:</p> <ul style="list-style-type: none">• Certificados académicos. Se realiza de forma directa comparando lo registrado en la hoja de vida contra los soportes físicos adjuntos a la misma.• Referencias laborales y personales, a través de llamada telefónica y las cartas de referencia. <p>En el caso de existir alguna inexactitud en la información laboral suministrada por el aspirante, éste será descartado y se le dará prioridad al candidato siguiente dentro de los más opcionados.</p> <p>El plazo para realizar todo el proceso de contratación del personal se tomará dos días después de que el colaborador entregue la documentación requerida.</p>		
--	--	--

<p>4.3.2 Promoción, ascensos y traslados del personal activo</p> <p>Buscar al interior de la organización para detectar si existe personal que cumple con el perfil del cargo y las competencias que se pretende proveer.</p> <p>Notificar las responsabilidades y deberes de seguridad de la información, cuando se presenten cambios o relevos en los diferentes cargos.</p>	<p>Jefe Inmediato</p>	<p>FO-HUM-19 Notificación promoción interna</p> <p>FO-HUM-01 Requisición de personal</p> <p>RC- HUM-03 Inducción y Reinducción al personal</p>
<p>4.3.3 Gestión de la documentación para la vinculación</p> <p>Comunicar al aspirante seleccionado el resultado del proceso de selección y solicitar la documentación que se requiere para su vinculación.</p> <p>El postulante debe realizar por su cuenta, la gestión total de la documentación requerida y sin la cual no se iniciará el procedimiento de vinculación.</p>	<p>Jefe de Talento Humano</p>	<p>FO-HUM-03 Requisitos de ingreso</p>
<p>4.3.4 Examen médico de ingreso</p> <p>Remitir al aspirante seleccionado a una clínica</p>		

<p>asignada por la Organización para que le sea efectuado un examen médico laboral de ingreso, y así evaluar las condiciones de salud acordes al cargo a desempeñar.</p> <p>Revisar el concepto médico y determinar la viabilidad de la vinculación; en caso de presentarse alguna recomendación se debe analizar la situación con el jefe inmediato para proceder a la vinculación.</p> <p>Realizar seguimiento al cumplimiento de las recomendaciones médicas durante el período de prueba del contrato para determinar la continuidad en el cargo.</p>	<p>Jefe de Talento Humano</p>	<p>FO-HUM-05 Autorización exámenes médicos</p> <p>Documento de origen externo: Concepto de aptitud laboral</p>
<p>4.4. Vinculación</p> <p>La compañía tomará la decisión de contratar o no al aspirante teniendo las recomendaciones entregadas por el médico especialista en Salud Ocupacional; una vez aprobado el ingreso se procede a diligenciar el formato de Vinculación de personal.</p> <p>Elaborar autorización para apertura de cuenta de ahorros para el pago de nómina.</p> <p>Realizar afiliaciones al Sistema General de</p>	<p>Jefe de Talento Humano</p>	<p>FO-HUM-02 Vinculación de personal</p> <p>FO-HUM-06 Autorización de apertura de cuenta</p> <p>RC-HUM-26 Foliación</p> <p>RC-HUM-02</p>

<p>Seguridad Social y Caja de Compensación</p> <p>Realizar afiliaciones a las pólizas de seguros adicionales.</p> <p>Archivar toda la documentación en la hoja de vida del trabajador y diligenciar el formato de foliación.</p> <p>Diligenciar al día siguiente del ingreso del colaborador, el listado maestro de los colaboradores.</p>		<p>Listado Maestro</p>
<p>4.4.1 Acuerdos sobre la seguridad de la información</p> <p>Como parte de los términos y condiciones iniciales del cargo, sin importar las funciones a desempeñar, se deberá firmar:</p> <p>Un contrato de trabajo laboral donde se definen las condiciones y obligaciones del empleado y el empleador.</p> <p>Socializar y firmar con el colaborador el acuerdo de confidencialidad donde se definen las reglas de seguridad para la divulgación, modificación, almacenamiento, distribución y/o eliminación segura de la información.</p>	<p>Jefe de Talento Humano</p>	<p>RC-HUM-17 Contrato laboral término indefinido</p> <p>RC-HUM-18 Contrato laboral término fijo</p> <p>RC-HUM-19 Contrato de trabajo por obra</p> <p>Contrato de Aprendizaje</p> <p>RC-HUM-16 Acuerdo sobre el uso de la información y</p>

		código de buena conducta
<p>4.5. Inducción de ingreso</p> <p>Realizar inducción y /o reinducción al nuevo colaborador por las áreas involucradas.</p>	Jefe de Talento Humano	RC- HUM-03 Inducción y Reinducción al personal
<p>4.6 Evaluación del desempeño de los colaboradores</p> <p>Nuevas vinculaciones:</p> <ul style="list-style-type: none"> • Realizar la evaluación de la efectividad de las funciones por parte del jefe inmediato antes de cumplir su período de prueba. • Entregar informe con el concepto de la continuidad laboral al Jefe de Talento Humano. <p>Colaboradores con ≤ 1 año de antigüedad</p> <p>Ejecutar una evaluación de desempeño anual en el primer mes del año a todos los colaboradores, considerando las siguientes actividades:</p> <ul style="list-style-type: none"> • Organizar las pruebas que constituyan la 	Jefe de Talento Humano	RC-HUM-04 Evaluación de desempeño anual RC-HUM-27 Matriz de desempeño

<p>evidencia del desempeño laboral, considerando los compromisos adquiridos durante el período a evaluar</p> <ul style="list-style-type: none"> • Aplicar la evaluación de desempeño anual en compañía del colaborador con el fin de retroalimentarlo y acordar compromisos de mejora • Establecer las acciones preventivas o correctivas según el resultado de la evaluación de desempeño. <p>Verificar el cumplimiento de los compromisos comparando los logros y contribuciones en el desarrollo de sus tareas del período actual respecto al período evaluado.</p> <p>Después de aplicada la evaluación de desempeño se debe diligenciar la matriz de desempeño con los compromisos adquiridos por las partes para su posterior ejecución y seguimiento.</p>		
<p>4.7 Incentivos</p> <p>Ejecutar el plan de incentivos de acuerdo a los resultados de la evaluación de desempeño.</p>	<p>Jefe de Talento Humano Gerente General</p>	<p>PC-HUM-01 Plan de incentivos</p>

<p>4.8 Desvinculación del colaborador</p> <p>La terminación del vínculo laboral sea por mutuo acuerdo o de manera unilateral debe realizarse mediante comunicado escrito por parte de quien toma la decisión.</p> <p>Cuando se trata de terminación voluntaria, la organización debe notificar dicha aceptación de manera escrita e iniciar los trámites correspondientes.</p> <p>Una vez el colaborador esté desvinculado a la organización, notificar inmediatamente por correo electrónico a las entidades de Seguro y Funerarias para su exclusión</p> <p>Notificar al colaborador las responsabilidades y deberes relacionados con la seguridad de la información que siguen vigentes después de terminado el contrato laboral. (acuerdo de confidencialidad de la información)</p>	<p>Jefe de Talento Humano</p>	<p>FO-HUM-11 Notificación de finalización contrato</p> <p>FO-HUM-12 Aceptación de la renuncia</p>
<p>4.8.1 Autorizar exámenes médicos de desvinculación</p> <p>Entregar por el Jefe de Talento Humano al colaborador la autorización para realizarse los exámenes médicos de egreso en la entidad</p>	<p>Jefe de talento Humano</p>	<p>FO-HUM-05 Autorización examen médico ocupacional</p>

<p>asignada por la compañía y dejar constancia de la entrega de esta autorización</p> <p>Después de realizada la valoración médica de egreso, el colaborador que se retira debe llevar el concepto medico a la compañía.</p>		<p>Documento de origen externo:</p> <p>Concepto de aptitud laboral</p>
<p>4.8.2 Paz y salvo</p> <p>Con el propósito de garantizar la devolución de los activos de la compañía, restringir los derechos de acceso y movilidad, y certificar el paz y salvo con los procesos, se debe diligenciar el formato de “Constancia de paz y salvo y encuesta de retiro”; el cual lo debe tramitar el área de Gestión del Talento Humano en compañía del colaborador en retiro.</p> <p>Tramitar el paz y salvo a la mayor brevedad posible (24 horas), de acuerdo a los siguientes lineamientos:</p> <p>1. Una vez notificado en Talento humano el retiro del colaborador, el jefe de Talento Humano deberá enviar un correo a todas los procesos implicadas en la liquidación como:</p> <ul style="list-style-type: none"> ✓ Jefe inmediato firmar el paz y salvo cuando no se tienen pendientes y/o entregables con las funciones que desempeñaba el colaborador. 	<p>Líderes de Procesos</p>	<p>RC-HUM-05</p> <p>Constancia de Paz y Salvo y encuesta de retiro</p>

<ul style="list-style-type: none"> ✓ Jefe de compras y almacén, firmar el paz y salvo cuando el colaborador entrega todos los activos que estaban bajo su responsabilidad y custodia. ✓ Jefe de Transporte, firmar el paz y salvo cuando el colaborador no tiene pendientes con legalizaciones y/o entrega de vehículos. ✓ Coordinador TIC, firmar el paz y salvo cuando el colaborador hace entrega de los activos que estaban bajo su responsabilidad y custodia. El Coordinador debe cancelar correos, accesos lógicos y físicos, contraseñas de seguridad, entre otros relacionados con la seguridad de la información. ✓ Coordinador SGI, firmar el paz y salvo cuando el colaborador está a paz y salvo con procesos relacionados con el SGI. ✓ Contador, firma el paz y salvo cuando se verifica el estado de los anticipos, legalizaciones y otros pendientes en contabilidad. ✓ Coordinador Administrativo y financiero, firmar el paz y salvo cuando se verifica el estado de los préstamos, libranzas, saldo de celular entre otros del colaborador. ✓ Director Operativo y Jefe de personal, firmar el paz y salvo, cuando verifica el estado de los pendientes con el área, el 		
--	--	--

<p>Director y/o Jefe de personal, deben notificar las horas extras pendientes por pago.</p> <p>Cuando el colaborador tiene algún pendiente con cualquiera de las áreas, el responsable de está, deberá enviar un correo electrónico a todos los implicados informando la retención del paz y salvo e informar al colaborador el motivo de la retención para que esté tramite el pendiente.</p> <p>Una vez se tenga el paz y salvo completamente diligenciado, el área contable tiene 8 días calendario para la liquidación del colaborador.</p>		
<p>4.8.3 Liquidación y pago de prestaciones sociales</p> <p>Suministrar por parte del proceso de Gestión del Talento Humano al área de contabilidad, el expediente del colaborador con:</p> <p>La hoja de vida</p> <p>Notificación de finalización del contrato</p> <p>Aceptación de la renuncia (cuando aplique)</p> <p>Autorización para descuentos (si aplica)</p>	<p>Jefe de Talento Humano</p>	<p>RC-HUM-05 Constancia de Paz y Salvo y encuesta de retiro</p> <p>RC-HUM-06 Hoja de vida</p> <p>FO-ADM-15 Autorización de descuentos</p>
<p>4.8.4 Entregar certificados laborales</p> <p>Generar y entregar los certificados cuando sean requeridos por el colaborador:</p>	<p>Jefe de Talento Humano</p>	<p>FO-HUM-13 Retiro de cesantías</p> <p>FO-HUM-14</p>

<ul style="list-style-type: none">• Certificado laboral• Oficio para retiro de cesantías (si aplica)• Certificación del último pago de seguridad social		Certificado laboral
---	--	---------------------

8.2.4 Procedimiento Control de Servicios Contratados Externamente

Procedimiento Control de Servicios Contratados Externamente	<u>Código: PR-PRO-08</u>
	<u>Versión:01</u>

1. OBJETO

Asegurar que todos los servicios contratados externamente pasen por un filtro que garantice el cumplimiento de parámetros específicos los cuales pueden influir en la calidad del servicio contratado, en los servicios de tecnología de la información y la seguridad de la información.

2. ALCANCE

Este documento tiene como alcance proveer la metodología y puntos de control que la empresa dispone para realizar el control a los servicios contratados externamente.

Los servicios que la empresa suele contratar externamente son:

- Levantamientos topográficos.
- Estudios de suelos.
- Modelación de estructuras.
- Pruebas de resistencia del concreto.
- Servicio de transporte terrestre de carga.
- Perforaciones horizontales dirigidas.
- Hincado de postes.
- Asesorías y/o consultoría
- Guarda y custodia de archivos activos e inactivos
- Servicio de hosting.
- Rastreo satelital de vehículos

- Otros que puedan resultar a causa de la operación

3. DEFINICIONES Y/O CONVENCIONES

Persona Natural: Persona Natural es una persona humana que ejerce derechos y cumple obligaciones a título personal. Al constituir una empresa como Persona Natural, la persona asume a título personal todos los derechos y obligaciones de la empresa.

Persona Jurídica: Persona Jurídica es una empresa que ejerce derechos y cumple obligaciones a nombre de ésta. Al constituir una empresa como Persona Jurídica, es la empresa (y no el dueño) quien asume todos los derechos y las obligaciones de la empresa

Estándar: Se refiere a las disposiciones que en forma general sirven como modelo, norma, patrón o referencia de algo

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1. Cumplimiento de requisitos previos a la prestación del servicio por un tercero</p> <p>Antes de dar paso a la prestación de un servicio por parte de personas naturales o jurídicas externas a la empresa, es necesario</p>	<p>Directores de área / Coordinadores / Personal administrativo / Personal operativo</p>	<p>FO-PRO-07 Lista de chequeo para el control de servicios contratados externamente</p>

<p>que éstas cumplan con ciertos requisitos previos a fin de evitar tropiezos o contratiempos durante la prestación del servicio. Por tal razón, como actividad previa, es necesario diligenciar y validar el formato FO-PRO-07. El incumplimiento de los requisitos consignados en el formato anterior podrá ocasionar que la organización decida no continuar con el proceso de prestación del servicio.</p>		
<p>4.2. Identificación de procesos o partes de procesos operados por terceros.</p> <p>Los procesos o partes de procesos operados por terceros se pueden clasificar de acuerdo a los procesos misionales de la empresa así:</p> <p>Construcción y Montaje:</p> <ul style="list-style-type: none"> - Tendido de cable. - Obras civiles. - Transporte de materiales. - Pruebas de resistencia de materiales. - Hincado de postes <p>Diseño:</p> <ul style="list-style-type: none"> - Calculo de estructuras. - Levantamientos topográficos. - Calculo de tensiones y flechas. 	<p>Directores de área / Coordinadores / Personal administrativo Coordinador TIC</p>	

<ul style="list-style-type: none"> - Estudio de suelos. <p>Mantenimiento:</p> <ul style="list-style-type: none"> - Instalación de cruces de líneas. - Vigilancia de red. <p>Comercialización:</p> <ul style="list-style-type: none"> - Intermediación aduanera. <p>Sistemas:</p> <ul style="list-style-type: none"> - Servicio de Hosting - Diseño y desarrollo de páginas web - Diseño y soluciones de aplicaciones informáticas 		
<p>4.3 Identificación de riesgos con partes externas.</p> <p>Cuando exista la necesidad de otorgar acceso a terceras partes a información el Gestor SI-TI y el Propietario de la Información de que se trate, llevará a cabo y documentará una evaluación de riesgos para identificar los controles específicos, teniendo en cuenta, entre otros aspectos:</p> <ul style="list-style-type: none"> • El tipo de acceso requerido (físico/lógico y a qué recurso). • Los motivos para los cuales se solicita el acceso. 	<p>Directores de área / Directores / Personal administrativo/ Coordinador TIC</p>	<p>FO-PRO-12</p> <p>Lista de chequeo de requisitos para autorizar el acceso a la información por terceras partes</p>

<ul style="list-style-type: none"> • La clasificación de la información. • Los controles empleados por la tercera parte. • La incidencia de este acceso en la seguridad de la información. <p>Diligenciar la lista de chequeo para autorizar el acceso a la información FO-PRO-12 con la identificación de los riesgos.</p> <p>En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.</p>		
<p>4.4. Autorizaciones para el uso de la información</p> <p>Una vez caracterizada la información con los parámetros anteriores, el emisor puede autorizar (parcial o totalmente), condicionar o denegar el acceso a la información y establecer la ruta de transmisión.</p> <p>Documentando todo lo anterior en el registro FO-PRO-12.</p>	<p>Directores de área / Coordinadores / Personal administrativo</p>	<p>FO-PRO-12 Lista de chequeo de requisitos para autorizar el acceso a la información por terceras partes</p> <p>FO-PRO-09 Acuerdo de</p>

<p>Generar un Acuerdo de Confidencialidad con las partes externas tomando como referencia el modelo FO-PRO-09, en caso de que producto de la caracterización, se requiera establecer un acuerdo específico de seguridad de la información.</p> <p>Comunicar las políticas de seguridad de la información:</p> <p>PO-SIS-11 Control de acceso a la información</p> <p>PO-SIS-03 Protección de los datos personales</p>		<p>confidencialidad</p> <p>PO-SIS-11 Control de acceso a la información</p> <p>PO-SIS-03 Protección de los datos personales</p>
<p>4.4.1 Balance del servicio</p> <p>Luego de la prestación del servicio es necesario validar que éste haya cumplido con las expectativas inicialmente pactadas. Por eso debe diligenciarse un cuadro comparativo donde se consignen los objetivos iniciales Vs. los resultados obtenidos y el porcentaje de cumplimiento de cada uno de los parámetros evaluados. Finalmente se concluye si la prestación del servicio fue satisfactoria o no.</p>	<p>Directores de área / Directores / Personal administrativo/ Coordinador TIC</p>	<p>FO-PRO-08 Balance del servicio</p>

<p>4.5 Gestionar acuerdos de servicio</p> <p>Establecer acuerdos con terceras partes cuando estos van a proveer servicios de tecnología de la información para garantizar la disponibilidad de los niveles de servicio establecidos para que estos sean implementados, mantenidos y operados.</p> <p>Ver PR-PR-SIS-19"Gestión de las Relaciones con el Negocio y Gestión con los proveedores"</p>	<p>Coordinador TIC</p>	<p>RC-SIS-53 Contrato de soporte UC</p> <p>PR-SIS-19 Gestión de las Relaciones con el Negocio y Gestión con los proveedores"</p>
<p>4.5.1 Monitoreo y Revisión de los acuerdos</p> <p>Realizar semestralmente o una vez durante la vigencia del acuerdo, una auditoría con el fin de verificar el cumplimiento de los requisitos establecidos en el contrato de soporte.</p> <p>Establecer, de acuerdo a los resultados de la verificación las acciones necesarias para corregir los hallazgos no conformes detectados.</p>	<p>Coordinador TIC</p>	<p>RC-CAL- 01 Plan para realizar la auditoria Interna</p> <p>RC-CAL-02 Lista de verificación</p> <p>RC-CAL-04 Acciones correctivas, preventivas y de mejora y seguimiento</p>

<p>4.6 Gestión de cambios con terceras partes</p> <p>Cuando durante la vigencia de un acuerdo de soporte con terceras partes, se detecte la necesidad de efectuar cambios o mejoras en los procesos y/o controles que rigen la prestación del servicio se debe tramitar una solicitud de servicio por medio del link: http://192.168.1.65/cmdb/web/pages/UI.php donde indique:</p> <ul style="list-style-type: none"> - El objeto y alcance del cambio. - Los resultados esperados del cambio - Los posibles riesgos del cambio <p>Ver PR-SIS-15 Gestión de Cambios de los servicios TI.</p>	<p>Director de área</p> <p>Coordinadores de proyectos</p>	<p>RC-SIS-53 Contrato de soporte UC</p> <p>PR-SIS-15 Gestión de Cambios de los servicios TI</p>
--	---	---

8.2.5 Procedimiento Gestión de activos de información (AI)

<u>Procedimiento Gestión de activos de información (AI)</u>	Código: PR-SIS-02
	Versión:01

1. OBJETO

Proveer las medidas de seguridad necesarias para proporcionar una protección adecuada a los activos de la Organización, así como controlar, generar responsabilidades, normas de uso y clasificación sobre los activos de información.

2. ALCANCE

Aplica para el tratamiento de todos los activos de información identificados en el documento RC-SIS-41 Inventario de los activos de información.

3. DEFINICIONES Y/O CONVENCIONES

Información: Se considera información a todo dato relacionado con las actividades y servicios de una organización, que tenga valor para ésta según estime su propietario, atendiendo a las escalas de valoración utilizadas, los requisitos legales, su sensibilidad y criticidad para la organización, cualquiera sea su forma y medio de comunicación y/o conservación (información de los sistemas, documentos impresos).

Información clasificada: es un tipo de información sensible que está restringida o regulada para clases particulares de personas. Se requiere una habilitación formal de seguridad para manejar y acceder a documentos clasificados.

Activo de información: Es todo aquello que la organización considere importante

o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos, contraseñas y/o números de cuentas.

Activo: cualquier cosa que tiene valor para la organización

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1 RESPONSABILIDAD POR LOS ACTIVOS</p> <p>4.1.1 Inventario de activos</p> <p>Identificar todos los activos seguridad de la información de acuerdo a la siguiente clasificación:</p> <p>*Hardware: equipamiento de computación, accesorios y periféricos, impresoras, servidores, scanner, vehículos, OTDR, PMD, medidores de potencia</p> <p>*Software: software de aplicaciones, software de sistemas, licencias</p> <p>*Comunicaciones: telefonos, fax</p> <p>*Talento Humano: recurso humano</p> <p>*Infraestructura: edificios y ubicaciones físicas.</p> <p>*Información en medio fisico: bases de datos, archivos de datos, documentación, contratos, acuerdos, correspondencia,</p>	<p>Gestor SI-TI</p>	<p>RC-SIS-41 Inventario de los activos de información</p>

<p>pliegos del cliente</p> <p>El Gestor de la seguridad de la información es el responsable de mantener actualizado el inventario de activos de seguridad de la información con los movimientos, adquisiciones y bajas de los mismos.</p>		
<p>4.1.2 Propiedad de los activos</p> <p>Asignar un responsable de los activos de información por medio del registro acta de entrega, quien deberá asumir las siguientes funciones:</p> <p>a) informar sobre cualquier cambio que afecte el inventario de activos</p> <p>b) Cumplir los controles de seguridad establecidos para los activos</p> <p>Nota: Los propietarios de los activos de información pueden delegar la administración de sus funciones a personal idóneo a su cargo, pero seguirá conservando la responsabilidad sobre los activos.</p> <p>Registrar la devolución del activo en el registro Acta de entrega/devolución de activos de información.</p>	<p>Propietarios de los activos de información</p>	<p>RC-SIS-05</p> <p>Acta de entrega/devolución de activos de información</p>
<p>4.1.3 Uso aceptable de los activos</p>		

<p>Nota: Todo uso de activos de información debe ser para propósitos del Servicio.</p> <p>El Servicio no permite el uso personal de los activos de información.</p> <p>Todos los colaboradores, contratistas y usuarios de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados al procesamiento de la misma, incluyendo:</p> <ul style="list-style-type: none"> a) correo electrónico, b) estaciones de trabajo, c) dispositivos móviles, d) herramientas y equipos de trabajo <p>Reglas para los usuarios de activos de información:</p> <ul style="list-style-type: none"> -No deben divulgar información del Servicio ni de sus usuarios externos, que haya sido clasificada como “Confidencial” o de “Uso Interno”, salvo que hayan sido expresamente autorizados por el Propietario de la Información, quien deberá hacerse responsable de esta divulgación. -Está prohibido que los usuarios sustraigan información de las instalaciones de la organización sin previa autorización. -Deben solicitar autorización por escrito 	<p>Propietarios de los activos de información</p>	
--	---	--

<p>al Propietario de la Información, cuando necesiten proporcionar información “Confidencial” o de “Uso Interno” a terceros.</p> <p>La entrega de esta información se realizará suscribiendo acuerdos de confidencialidad con el tercero y aplicando los controles específicos que se definan.</p> <p>-Deben cumplir con todos los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deberán mantenerse alineadas con las leyes vigentes.</p> <p>-Deben proteger sus elementos de control de acceso, como contraseñas, dispositivos y otros, ya que son individuales, intransferibles y de responsabilidad única de cada propietario.</p> <p>-Deben reportar inmediatamente a su Jefe inmediato cualquier incidente que ponga en riesgo la seguridad de la información.</p>		
--	--	--

<p>4.2 CLASIFICAR LA INFORMACIÓN</p> <p>4.2.1 Directrices para clasificar la información</p> <p>Clasificar la información según su valor, los requisitos legales, su sensibilidad y criticidad para la organización.</p> <p>El propietario de la información en función de su importancia y nivel de impacto, confidencialidad, disponibilidad e integridad clasificará la información en:</p> <p>Nivel 1</p> <p>Clasificación: Pública</p> <p>Descripción: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea colaborador de la organización o no. Publico</p> <p>Nivel 2</p> <p>Clasificación: Uso Interno</p> <p>Descripción: Información que sin poder ser publicada, puede ser conocida y utilizada por todos los colaboradores y algunas partes externas autorizadas y cuya divulgación o uso no autorizado podría ocasionar pérdidas leves o asumibles por la organización.</p> <p>Información relacionada con procedimientos internos de operación.</p>	<p>Propietarios de información</p>	<p>RC-SIS-41</p> <p>Inventario de los activos de información</p>
---	------------------------------------	--

<p>Nivel 3</p> <p>Clasificación: Confidencial</p> <p>Descripción: Información que solo puede ser conocida y utilizada por un grupo de colaboradores que lo necesitan para cumplir sus funciones y algunas entidades externas autorizadas que hayan firmado el acuerdo de confidencialidad, su divulgación no autorizada podría ocasionar pérdidas significativas para la organización. Se trata de información sensible, como lo es la información del cliente, bases de datos, mecanismos de configuración y procedimientos de seguridad de la información.</p> <p>Nivel 4</p> <p>Clasificación: Estrictamente Confidencial</p> <p>Descripción: Información que sólo puede ser conocida y utilizada por el Gerente General, Directores Operativo, Comercial y Administrativo y Gestor de la Seguridad de la información, quienes están directamente implicados con las decisiones estratégicas de la organización. Su divulgación o uso podría</p>		
---	--	--

<p>ocasionar graves pérdidas para la imagen de la organización, de los accionistas o de los clientes.</p> <p>Hacen parte de esta información: claves de acceso a los sistemas de la organización o de terceros, decisiones estratégicas de crecimiento, informes de organismos de control, inversiones, entre otras.</p> <p>Sólo el propietario de la información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:</p> <ul style="list-style-type: none"> • Asignarle <i>una fecha de efectividad en el momento de una nueva clasificación.</i> • <i>Informar inmediatamente la nueva clasificación a los usuarios del documento.</i> <p>Se etiquetará la información exclusivamente a los niveles 3“Confidencial” y 4“Estrictamente confidencial”</p>		
<p>4.2.2 Tratamiento para la información al momento de la recepción</p> <p>Al momento de recibir información generada por terceros, esta deberá ser tratada como información de nivel 3 “Confidencial” hasta que su propietario</p>	<p>Propietario de información</p>	

<p>realice la clasificación definitiva y de ser necesario la comunique a todos los usuarios interesados para mantener la validez de la información y garantizar su manejo adecuado.</p>		
<p><u>POLÍTICA PARA EL TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA</u></p> <p>1. <u>La información clasificada como confidencial y estrictamente confidencial deberá ser conocida o utilizada solo por usuarios autorizados.</u></p> <p>2. <u>Todos los usuarios que por motivos de trabajo accedan a la información clasificada como confidencial y estrictamente confidencial, deberán firmar el acuerdo de confidencialidad.</u></p> <p>3. <u>La información clasificada como confidencial y estrictamente confidencial deberá permanecer en todo momento restringida a su uso y acceso.</u></p> <p>4. <u>La información en medio digital clasificada como confidencial y estrictamente confidencial deberá almacenarse en equipos de procesamiento debidamente protegidos y con clave de acceso.</u></p>	<p>Propietario de información</p> <p>Colaboradores</p>	<p>PO-SIS-01</p> <p>Tratamiento de la información clasificada</p>

<p>5. <u>La información en medio física clasificada como confidencial y estrictamente confidencial deberá almacenarse bajo llave permanentemente, y durante su uso deberá ser protegida y utilizada solo por personas autorizadas.</u></p> <p>6. <u>Siempre que la información clasificada como nivel 4 “Estrictamente confidencial” sea enviada a través de redes de comunicación propias o ajenas deberá viajar encriptado y la clave de descifrado deberá ser enviada por otro medio.</u></p>		
<p>4.2.3 Etiquetado y manejo de información</p> <p>Etiquetado</p> <p>Etiquetar toda la información en medio físico clasificada como confidencial y estrictamente confidencial considerando el siguiente rotulo.</p> <div style="border: 2px dashed blue; padding: 10px; text-align: center;"> <p>ESTRICTAMENTE CONFIDENCIAL</p> <p>“La información descrita en el presente documento es de uso reservado y exclusivo de Cyfo Comunicaciones. Está prohibida su reproducción sin previa autorización o su utilización en otros fines distintos para el cual fue entregada”</p> </div>	<p>Propietario de información</p>	<p>PR-SIS-06</p> <p>Adquisición y mantenimiento de sistemas de información</p>

CONFIDENCIAL

“La información descrita en el presente documento es de uso reservado y exclusivo de Cyfo Comunicaciones. Está prohibida su reproducción sin previa autorización o su utilización en otros fines distintos para el cual fue entregada”

Documentación en medio físico:

- Colocar el rotulo en la primera página del documento en un lugar visible.
- Asegurar que los documentos rotulados se encuentran en lugares protegidos y bajo llave.

Documentación en medio digital:

- Rotular el archivo con marca de agua de texto “CONFIDENCIAL” o “ESTRICTAMENTE CONFIDENCIAL” de acuerdo a su clasificación, de manera diagonal.
 - Asignar una clave de acceso para proteger su confidencialidad de acuerdo a los lineamientos del procedimiento PR-SIS-06
- “Adquisición y mantenimiento de sistemas de información” No 4.3 controles criptográficos.

4.2.4 Disposición final de la información de uso interno:

<p>-Soporte papel: Debe depositarse en papeleras dispuestas a tal efecto para posteriormente ser destruidos bajo control.</p> <p>-Soporte electrónico: Antes de ser desechados o reutilizados, deben ser procesados para su borrado lógico o hacer ilegible la información contenida.</p>	<p>Propietario de información</p>	<p>RC-SIS-41 Inventario de los activos de información</p>
---	-----------------------------------	---

8.2.6 Procedimiento Seguridad física y del entorno

<u>Procedimiento Seguridad física y del entorno</u>	<u>Código: PR-SIS-03</u>
	<u>Versión:01</u>

1. OBJETO

Que el lector conozca las directrices establecidas por la organización para procurar la seguridad física de la infraestructura y de los activos de información, así como el tratamiento que se le debe prestar a los mismos con el fin de salvaguardar la información contenida en ellos.

2. ALCANCE

El presente documento incluye las disposiciones para controlar el acceso a las áreas seguras tanto del personal interno como de los invitados, y el tratamiento que se debe aplicar a los activos de información para procurar la disponibilidad, confidencialidad e integridad de la información.

3. DEFINICIONES Y/O CONVENCIONES

Activo: cualquier cosa que tiene valor para la organización

Acceso Físico: Posibilidad de acceder físicamente a una infraestructura, a un activo o a cualquier sistema operativo.

Activo de Información: Todo aquello que tiene algún valor para la organización y que contiene o manipula información, y por lo tanto debe protegerse.

Amenaza: Probabilidad de ocurrencia de un evento que afecte cualquier activo de información

Área segura: se relaciona con accesos físicos, teniendo como objetivo impedir el acceso sin autorización, daños e interferencia a las instalaciones de la empresa y su información.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Perímetro de seguridad física: El sitio escogido para colocar los sistemas de información, equipos de cómputo y comunicaciones, deben estar protegidos por barreras y controles físicos, para evitar intrusión física, inundaciones, y otro tipo de amenazas que afecten su normal operación.

Zona de Seguridad: se relaciona con accesos físicos, teniendo como objetivo impedir el acceso sin autorización, daños e interferencia a las instalaciones de la empresa y su información.

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
4.1 ÁREAS SEGURAS 4.1.1 Perímetro de seguridad física, controles de acceso físico y Protección contra amenazas externas y ambientales.	Coordinador TIC	
a) Protección física zona segura 1:		

<p>Ubicación: Está ubicado en la edificación principal, nivel 2, área administrativa.</p> <p>Contenido: Zona segura 1, equipos de cómputo, impresoras, Escáner, Teléfonos fijos, celulares, discos duros, licencias.</p> <p>Protección: Puerta metálica de ingreso al segundo nivel, con cerrojo permanente el cual abre solo con lector biométrico, tarjeta de aproximación y/o llave.</p> <p>Esta zona cuenta para su protección, con un sensor de movimiento, que mantiene su carga mediante batería en caso de presentarse falla eléctrica.</p> <p>Esta área esta monitoreada con un sensor detector de humo, para alertar la presencia de un incendio.</p> <p>Responsable: Directora administrativa y financiera.</p>	<p>Directora administrativa y financiera.</p>	<p>PC-MEI-03 Programa de mantenimiento de infraestructura</p> <p>RC-MEI-05 Registro mantenimiento a la infraestructura interna</p>
<p>b) Protección física zona segura 2:</p> <p>Ubicación: Está ubicado en la edificación principal, nivel 2, área administrativa.</p> <p>Contenido: Servidor de datos, servidor de voz, servidor de contabilidad.</p> <p>Protección: Puerta metálica de ingreso</p>	<p>Coordinador TIC</p>	<p>PC-MEI-03 Programa de mantenimiento de infraestructura</p> <p>RC-MEI-05 Registro mantenimiento a la infraestructura</p>

<p>al segundo nivel, con cerrojo permanente el cual abre solo con lector biométrico, tarjeta de aproximación y/o llave.</p> <p>Esta zona cuenta para su protección, con un sensor de movimiento, que mantiene su carga mediante batería en caso de presentarse falla eléctrica.</p> <p>Esta área esta monitoreada con un sensor detector de humo, para alertar la presencia de un incendio.</p> <p>Responsable: Coordinador TIC.</p>		<p>interna</p>
<p>c) Protección física zona segura 3:</p> <p>Ubicación: Está ubicado en la edificación principal, nivel 1, área operativa.</p> <p>Contenido: Equipos de cómputo, impresoras, Escáner, Teléfonos fijos, celulares.</p> <p>Protección: Puerta metálica de ingreso al primer nivel.</p> <p>Esta zona cuenta para su protección, con un sensor de movimiento, que mantiene su carga mediante batería en caso de presentarse falla eléctrica.</p> <p>Esta área esta monitoreada con un sensor detector de humo, para alertar la</p>	<p>Coordinador de proyecto Telmex.</p>	<p>PC-MEI-03 Programa de mantenimiento de infraestructura</p> <p>RC-MEI-05 Registro mantenimiento a la infraestructura interna</p>

<p>presencia de un incendio</p> <p>Responsable: Coordinador de proyecto Telmex.</p>		
<p>d) Protección física zona segura 4:</p> <p>Ubicación: Está ubicado en la edificación principal, subnivel, área de almacén.</p> <p>Contenido: Equipos de cómputo, Teléfono fijo, Celulares, OTDR, Impresora.</p> <p>Protección: Puerta metálica, con cerrojo eléctrico permanente y cierre automático. Esta zona cuenta para su protección, con un sensor de movimiento, que mantiene su carga mediante batería en caso de presentarse falla eléctrica. Esta área esta monitoreada con un sensor detector de humo, para alertar la presencia de un incendio.</p> <p>Responsable: Jefe de Almacén y compras.</p>	<p>Jefe de Almacén y compras.</p>	<p>PC-MEI-03 Programa de mantenimiento de infraestructura</p> <p>RC-MEI-05 Registro mantenimiento a la infraestructura interna</p>
<p>e) Protección física zona segura 5:</p> <p>Ubicación: Edificación principal, área externa.</p> <p>Contenido: Infraestructura física,</p>		

<p>humana, de información, técnica y financiera.</p> <p>Protección: Puertas metálicas de acceso frontal para vehículos y personas, esta última está doblemente protegida por rejas metálicas.</p> <p>El techo cuenta para su protección, con un sensor de movimiento, que mantiene su carga mediante batería en caso de presentarse falla eléctrica.</p> <p>Esta área esta monitoreada con un sensor detector de humo, para alertar la presencia de un incendio</p> <p>Responsable: Director Administrativo y financiero</p>	<p>Director Administrativo y financiero</p>	<p>PC-MEI-03 Programa de mantenimiento de infraestructura</p> <p>RC-MEI-05 Registro mantenimiento a la infraestructura interna</p>
<p>4.1.2 Seguridad de oficinas, recintos e instalaciones</p> <p>Con el fin de controlar el acceso de visitantes se han definido las siguientes disposiciones:</p> <ol style="list-style-type: none"> 1. Solicitar al invitado a través del sistema de citófono su identificación y nombre del colaborador a visitar. 2. Confirmar con el colaborador visitado la pertinencia de la visita y en caso 	<p>Auxiliar Administrativa Todo el personal Jefe de Talento Humano</p>	<p>RC-SIS-08 Control de visitantes y equipos</p>

<p>afirmativo permitir el acceso del visitante al área de recepción.</p> <p>3. Solicitar en recepción un documento de identificación, diligenciar los formatos control de visitantes e ingreso y salida de equipos, y entregar el carné para invitados.</p> <p>4. Indicar en el formato control de visitantes la fecha, hora de ingreso y salida, área, propósito de la visita y persona que lo autoriza.</p> <p>5. Registrar en el RC-SIS-08 Ingreso y salida de equipos los equipos portátiles que el visitante ingresa a la organización.</p> <p>6. Solicitar al colaborador visitado que se acerque a recepción por su invitado y conducirlo hasta el lugar de reunión.</p> <p>Con el fin de controlar el acceso al personal vinculado a la organización se han definido las siguientes disposiciones</p> <p>1. Registrar el ingreso y salida a las instalaciones en el lector de huella</p>		
--	--	--

<p>ubicado en la zona de parqueo.</p> <p>2. Dotar a todos los colaboradores con el carné empresarial, el cual debe ser portado permanentemente en un lugar visible.</p> <p>3. Brindar al personal desvinculado de la organización el tratamiento establecido para los visitantes.</p>		
<p>4.1.3 Trabajo en áreas seguras</p> <p>1. Supervisar en todo caso la ejecución de trabajos por parte de terceros en la zona de seguridad.</p> <p>2. Notificar al personal involucrado sobre la ejecución de trabajos en la zona de seguridad cuando esto afecte el desarrollo de sus funciones.</p>	<p>Directora Administrativa y Financiera.</p> <p>Coordinador TIC</p>	
<p>4.1.4 Áreas de carga, despacho y acceso público</p> <p>Se utiliza una cadena con una señal “Paso restringido”, para controlar el acceso al área de despacho y carga desde el exterior de la edificación.</p>	<p>Jefe de Almacén y Compras</p>	

<p>4.2 SEGURIDAD DE LOS EQUIPOS</p> <p>4.2.1 Ubicación y protección de los equipos.</p> <p>Los activos de información tanto ópticos como de cómputo deben conservarse en lugares seguros con el fin de proteger tanto su integridad física como la información contenida en ellos, por lo anterior, se deben tener en cuenta las siguientes consideraciones:</p> <ol style="list-style-type: none"> 1. Ubicar sensores de detección de humo y cámaras de circuito cerrado de televisión en los lugares donde existan activos de información. 2. Ubicar extintores solkaflan en las áreas donde se encuentran los equipos. 3. Se utiliza las ups como mecanismo de protección contra falla del suministro de energía eléctrica. 4. Controlar el consumo de alimentos en las estaciones de trabajo donde se encuentran ubicados los activos de información o durante la manipulación de los mismos. 5. Se utiliza una planta de energía alterna, para asegurar la continuidad del procesamiento de información, en 	<p>Coordinador TIC</p> <p>Jefe de Talento Humano</p>	
---	--	--

caso de fallas de energía prolongadas.		
<p>4.2.2 Servicios de suministro</p> <ul style="list-style-type: none"> •Dotar el servidor y los equipos de cómputo de fuentes de suministro eléctrico con batería (UPS). •Disponer de una planta de energía alterna. •Verificar el voltaje de las baterías UPS cada 3 meses y documentar los resultados obtenidos en el RC-SIS- 09. 	Coordinador TIC	RC-SIS-09 Control del estado de las baterías UPS
<p>4.2.3 Seguridad del cableado</p> <p>Mantener los cables tanto de datos, voz y eléctricos, ocultos dentro de la estructura de la edificación, en caso contrario, distribuirlos por medio de canaleta.</p> <p>Incluir en el programa de mantenimiento de infraestructura la revisión del cableado.</p>	Coordinador TIC	PR-SIS-08 Mantenimiento de activos de información
<p>4.2.4 Mantenimiento de los equipos.</p> <p>Mantener actualizado el plan de mantenimiento de los activos de información de acuerdo a lo indicado en el procedimiento PR-SIS-08 "Mantenimiento de activos de</p>	Auxiliar Administrativa	PR-SIS-08 Mantenimiento de activos de información

<p>información” conservando todos los registros establecidos en él y cumpliendo con el plan anual de mantenimiento de activos de información.</p> <p>Nota: Cuando sea necesario contratar con un tercero el mantenimiento de los equipos, el Coordinador TIC genera un acuerdo de confidencialidad con el tercero.</p>	<p>Coordinador TIC</p>	<p>FO-PRO-09 Acuerdo de confidencialidad</p>
<p>4.2.5 Seguridad de los equipos fuera de las instalaciones.</p> <p>En todo caso, cuando un activo de procesamiento de información debe retirarse de la organización, se debe seguir el siguiente procedimiento</p> <p>1. Equipos de Cómputo: Mediante autorización del Coordinador TIC y jefe inmediato, diligenciando el registro de entrega de activos de información. Se excluyen los equipos portátiles asignados de manera permanente a algunos colaboradores del área directiva y gerencial.</p> <p>2. Equipos Operativos: Entregar por parte del Coordinador de proyectos el Check list de alistamiento de recursos diligenciado al Jefe de Compras y</p>	<p>Coordinador TIC Jefe de Compras y Almacén</p>	<p>RC-SIS-05 Acta de entrega / devolución de equipos de computo</p> <p>RC-SIS-08 Registro de ingreso y salida de equipos</p>

<p>Almacén para avalar la entrega del equipo.</p> <p>3. Transportar y operar los equipos operativos, de acuerdo a las directrices establecidas en el instructivo IN-COM-04.</p> <p>4. Verificar la integridad y buen estado del equipo cuando se realiza la devolución del activo información.</p> <p>5. Los equipos cuentan con póliza de seguro que los protege fuera de las instalaciones</p> <p>6. Los activos retirados no se dejarán desatendidos en lugares públicos.</p> <p>7. Se evitará, en la medida de lo posible, que el activo contenga información sensible. Si es posible, la información debería de eliminarse de forma segura antes de salir fuera de las zonas seguras.</p>		
<p>4.2.5.1 Seguimiento a los activos que están fuera de las instalaciones</p>	<p>Coordinador TIC</p>	<p>FO-CAL-03 Análisis de datos</p>

<p>Los cinco primeros días hábiles de cada mes el Coordinador TIC debe realizar una llamada telefónica o enviar un correo electrónico a las personas responsables de los activos de información que se encuentran fuera de las instalaciones aplicando la siguiente encuesta.</p> <p>Analizar los resultados obtenidos y tomar las acciones necesarias para asegurar el buen funcionamiento de los activos de procesamiento de información.</p> <p>Retroalimentar al personal involucrado, las acciones tomadas.</p> <p>Considerar en los resultados de la encuesta, para la nueva valoración de los riesgos (vulnerabilidades o amenazas) por el comité de gestión integral.</p>		
---	--	--

Fecha:			
Nombre del responsable del activo:			
Cargo:			
Favor completar las siguientes preguntas	SI	NO	
1. ¿En activo se encuentra ubicado en un lugar seguro y bajo supervisión permanente del responsable?			
2. ¿Se está realizando el back up semanal a la información que maneja el activo de información?			
2. ¿Para acceder al sistema operativo del activo de			

información, debe registrar la clave asignada?		
4. ¿El activo, ha presentado alguna falla (si responde SI, favor informar la falla presentada)		
Cuál?		
5. Se ha presentado algún incidente donde posiblemente se ha perdido información del trabajo realizado? (si responde SI, favor informar el incidente presentado)		
Cuál?		
En caso de no recibir respuesta a este correo durante los próximos tres días hábiles siguientes a la fecha de envío se entenderán como favorables todas las respuestas solicitadas		
<p>4.2.6 Seguridad en la reutilización eliminación de los equipos.</p> <ol style="list-style-type: none"> 1. Llevar ante el comité de bajas la solicitud de supresión de los equipos. 2. Eliminar toda la información y datos sensibles contenidos en ellos y extraer todo software licenciado. 3. Proceder de acuerdo a las indicaciones del comité de bajas. 	<p>Jefe de almacén y compras</p> <p>Director Operativo</p>	<p>RC-COM-16</p> <p>Acta de bajas</p>
<p>4.2.7 Retiro de activos</p> <ol style="list-style-type: none"> 1. El retiro de los equipos de las 		

<p>instalaciones debe hacerse con autorización del responsable del equipo.</p> <p>2. El retiro de los equipos debe quedar registrado en el software que controla el inventario.</p> <p>3. Implementar un procedimiento para los activos que manejan información donde se especifique un tiempo máximo para los equipos retirados, la manera de verificar el cumplimiento de la devolución y el control para los equipos que permanecen fuera de las instalaciones.</p>	<p>Jefe de Almacén y Compras</p> <p>Coordinador TIC</p>	<p>RC-SIS-05</p> <p>Acta de entrega / devolución de equipos de computo</p> <p>RC-SIS-08</p> <p>Registro de ingreso y salida de equipos.</p>
--	---	---

8.2.7 Procedimiento Gestión de comunicaciones y operaciones

<u>Procedimiento Gestión de comunicaciones y operaciones</u>	<u>Código: PR-SIS-04</u>
	<u>Versión:01</u>

1. OBJETO

Mantener la operación correcta y segura de los medios de procesamiento de la información estableciendo responsabilidades y procedimientos para la gestión y operación de los mismos.

2. ALCANCE

El presente documento incluye las disposiciones para gestionar las comunicaciones y operaciones tanto del personal interno como de los invitados, y el tratamiento que se debe aplicar a los activos de información para procurar la disponibilidad, confidencialidad e integridad de la información.

3. DEFINICIONES Y/O CONVENCIONES

Trazabilidad: Es el conjunto de aquellos procedimientos preestablecidos y autosuficientes que permiten conocer el histórico, la ubicación y la trayectoria de un producto o lote de productos a lo largo de la cadena de suministros en un momento dado.

Código Móvil: Es un código de software que se transfiere de un computador a otro y luego se ejecuta automáticamente y lleva a cabo una función específica con poca o ninguna interacción del usuario. El código móvil se asocia con una variedad de servicios ubicados en la capa intermedia (middleware).

Red: Una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Integridad: Se refiere a la corrección y complementación de los datos en una base de datos. Cuando los contenidos se modifican con sentencias INSERT, DELETE o UPDATE, la integridad de los datos almacenados puede perderse de muchas maneras diferentes. Pueden añadirse datos no válidos a la base de datos, tales como un pedido que especifica un producto no existente.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista. De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Disponibilidad: Es una medida que nos indica cuanto tiempo está ese equipo o sistema operativo respecto de la duración total durante la que se hubiese deseado que funcionase. Típicamente se expresa en porcentaje. No debe de ser confundida con la rapidez de respuesta.

Encriptación: Es el proceso para volver ilegible información considerada importante. La información una vez encriptado sólo puede leerse aplicándole una clave.

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1. Procedimientos y responsabilidades operacionales</p> <p>4.1.1. Documentación de los procedimientos de operación</p> <p>Mantener actualizados los procedimientos de operación identificados para recuperar los servicios de tecnología de la información y las aplicaciones críticas de la organización.</p>	<p>Coordinador TIC</p> <p>Propietarios de activos.</p>	<p>PR-SIS-09 Copias de Respaldo.</p> <p>PR-SIS-08 Mantenimiento de Equipos.</p> <p>PR-SIS-11 Manejo de Medios.</p>
<p>4.1.2 Gestión del cambio</p> <p>Gestionar los cambios en los sistemas operativos y sistemas de información por medio de una solicitud de servicio al link http://192.168.1.65/cmdb/web/pages/UI.php, con el fin de que se evalúe el cambio para reducir el impacto en la prestación de los servicios.</p>	<p>Coordinador TIC</p>	<p>PR-SIS-15 Gestión de Cambios de los servicios TI</p>

<p>Ver PR-SIS-15 Gestión de Cambios de los servicios TI</p>		
<p>4.1.3 Distribución de funciones</p> <p>Reducir las posibilidades de modificación no autorizada o uso no intencional de los activos de información de acuerdo a las siguientes directrices:</p> <p>*Crear perfiles de usuario que sean consecuentes con las descripciones del cargo que desempeñan, y que contengan los mínimos accesos a los sistemas de información para llevar a cabo sus funciones.</p> <p>• El Gestor SI-TI valida estos perfiles al menos 2 veces al año</p>	<p>Coordinador TIC</p>	
<p>4.1.4 Separación de las instalaciones de desarrollo, ensayo y operación</p> <p>Utilizar el OF2-0430 PC de sistemas como ambiente de pruebas y el servidor SVR-C6J1 corresponde al ambiente de producción, aplica para las</p>	<p>Coordinador TIC</p>	

<p>actualizaciones de las aplicaciones críticas (geminus) y para los sistemas operativos de la organización.</p> <p>Utilizar distintos perfiles de usuarios para sistemas productivos y de prueba.</p>		
<p>4.2 Gestión de la prestación de servicios por terceras partes</p> <p>Gestionar la relación con terceras partes mediante la aplicación de las disposiciones del PR-PRO-08 Control de Servicios Contratados Externamente.</p>	<p>Coordinador TIC</p>	<p>PR-PRO-08 Control de servicios contratados externamente.</p>
<p>4.3 Planificación y aceptación del sistema</p> <p>Gestionar la capacidad de los sistemas de información y de los CI de los servicios de tecnología de la información mediante el procedimiento PR-SIS-20 Gestión de capacidad.</p>	<p>Coordinador TIC</p>	<p>PR-SIS-20 Gestión de la Capacidad de los servicios TI y de los sistemas de información</p>
<p>4.3.1 Aceptación del sistema</p> <p>Establecer un ambiente de pruebas para la actualización de parches y actualizaciones de seguridad antes de ser puestas en producción.</p>	<p>Coordinador TIC</p>	

<p>Los siguientes ítems deben ser considerados previo a una aceptación formal:</p> <ul style="list-style-type: none"> •Requerimientos de capacidad y desempeño. •Procedimiento de recuperación ante errores y planes de contingencia. •Preparación y rutinas de pruebas. •Acuerdo de los controles de seguridad a implementar. •Procedimientos de operación manual. •Acuerdos de continuidad del negocio. •Evidencia de que la instalación del nuevo sistema, no afectará a los actuales en producción, en particular en tiempos de utilización excesiva. •Evidencia de que la instalación del nuevo sistema, no afectará al nivel de seguridad actual en producción. •Entrenamiento en la operación de los nuevos sistemas. •Facilidad del uso, cómo afectan al desempeño de los usuarios y como prevén errores humanos. 		
<p>4.4 Protección contra códigos malicioso y móviles</p>		

<p>4.4.1 Controles contra códigos maliciosos.</p> <p>Para prevenir que códigos maliciosos afecten el sistema operativo, se crean cuenta con acceso limitado (usuario estándar) con esto, se evita que algunos códigos se ejecuten ya que se requeriría una contraseña de administrador para hacerlo.</p> <p>-Para la detección, todos los equipos cuentan con un antivirus actualizado.</p> <p>-Para la recuperación se cuenta con el backup de la información y se mantiene la función de restaurar el sistema activa en todo los equipos, con el fin de volver a un estado anterior a la afección de la máquina en caso de algún ataque.</p> <p>Adicional a esto se realiza una revisión detallada de código malicioso en los mantenimientos programados en el plan de calidad PC-SIS-02.</p> <p>Para concientizar a los usuarios directamente afectados por los códigos maliciosos, se programan socializaciones semestrales, refrescando técnicas y/o tips de cómo</p>	<p>Coordinador TIC</p>	<p>PC-SIS-02 Mantenimiento de los equipos tecnológicos y accesorios</p> <p>PO-SIS-06 Descargas de internet</p> <p>FO-CAL-04 Asistencia a eventos de capacitación y/o formación</p>
---	------------------------	--

<p>prevenir código maliciosos en sus equipos.</p> <p>Para proteger la compañía de códigos maliciosos provenientes de internet, se dispone la siguiente política:</p> <p style="text-align: center;"><i>POLÍTICA DE DESCARGAS DE INTERNET</i></p> <ul style="list-style-type: none">✓ Dar correcto uso a los recursos de internet por parte de todos los colaboradores, para evitar la contaminación de los activos de información a causa de virus, malware, spyware, entre otros.✓ Evitar la descarga de música, videos, software, y Archivos ejecutables, salvo previa autorización y revisión de código malicioso de dicho elemento por parte del Gestor SI-TI.✓ Mantener vigente la base de datos de códigos maliciosos del software antivirus mediante la actualización automática del software. Realizar una revisión bimestral en cada equipo, encaminada a detectar software malicioso, con el fin de		
--	--	--

<p>controlar dicho riesgo.</p> <p>✓ Instalar a todos los equipos que adquiera la compañía software antivirus actualizado para poder ser entregado al usuario final.</p>		
<p>4.4.2 Controles contra códigos móviles</p> <p>Se permite el uso únicamente de los siguientes códigos móviles:</p> <p>JavaScript</p> <p>Java applets</p> <p>Controles ActiveX</p> <p>Animaciones flash</p> <p><i>POLÍTICA DE USO DE CÓDIGO MÓVIL</i></p> <p>✓ Dar correcto uso a los códigos móviles autorizados por parte de todos los colaboradores, para regular las transferencias de dichos elementos.</p> <p>✓ Dar correcto uso y transporte a los códigos móviles entre equipos de la compañía.</p> <p>-Activar medidas técnicas por medio de</p>	<p>Coordinador TIC</p>	<p>PO-SIS-07 Uso del código móvil</p>

<p>seguimiento de las vulnerabilidades publicadas en listas abiertas de distribución o a partir de los boletines de los fabricantes, analizando el impacto de la vulnerabilidad.</p>		
<p>4.5 Respaldo de la información Gestionar el respaldo de la información por medio de la realización de backup periódicos de acuerdo a los lineamientos del procedimiento de respaldo.</p>	<p>Coordinador TIC</p>	<p>PR-SIS-09 Respaldo</p>
<p>4.6 Gestión de la seguridad de las redes 4.6.1 Controles de las redes</p> <p>En todo contrato de redes se identifican las características de seguridad, niveles de servicio y requerimientos de todos los servicios de red independiente de que sea interna y externa.</p> <p>Cuando se trate de conexiones externas se aplica el contrato establecido con dicho proveedor, dada la dificultad de condiciones para</p>	<p>Coordinador TIC</p>	

<p>establecer con ellos acuerdos de servicios particulares.</p> <p>Monitorear regularmente la capacidad del proveedor de servicios de red para manejar los servicios contratados de una manera segura.</p> <p>Los servicios de red incluyen la provisión de conexiones, servicios de red privados y soluciones de seguridad de red manejadas como firewalls y sistema de detección de intrusos.</p> <p>Se implementan controles de autenticación y conexión de la red.</p>		
<p>4.6.2 Seguridad de los servicios de la red.</p> <p>La compañía proporciona a los grupos de interés relacionados con la organización, servicios informáticos para su utilización en actividades relacionadas con las labores de la compañía, por tal motivo se hace necesario seguir la siguiente política de uso:</p>	<p>Coordinador TIC</p> <p>Jefe de Talento Humano</p> <p>Gerente General</p>	<p>RC-SIS-29 Autorización de Conexión a la red.</p> <p>PR-HUM-05 Disciplinario.</p> <p>RC-SIS-53 Contrato de soporte UC</p>

<p>Condiciones de uso</p> <p>Usar la red para acceder, ofrecer o tomar información siempre que esté de alguna forma relacionada con el entorno laboral, y que este uso se realice de forma responsable a fin de evitar perjuicios a (o de) terceros.</p> <p>En cualquier caso, cumplir los siguientes requisitos.</p> <p>Utilizar correctamente los recursos suministrados por la compañía, respetando las políticas, procedimientos e instructivos de uso interno.</p> <p>No permitir el acceso a la infraestructura de red y a los recursos suministrados a personas u organizaciones ajenas a la compañía sin autorización expresa del Gestor SI-TI de la información o del Gerente General.</p> <p>Contar en su equipo de cómputo como mínimo con un software antivirus actualizado.</p> <p>No se considera aceptable y no puede ser usada la red bajo ningún</p>		
--	--	--

<p>concepto para:</p> <p>-Cualquier acto que viole las leyes vigentes.</p> <p>-Fines privados comerciales, salvo autorización expresa.</p> <p>La suscripción de personas o entidades ajenas a la organización a listas de distribución de correo automático o de interés general sin autorización expresa y por escrito del Gestor SI-TI que en todo caso deberá conservarse para acreditar la autorización.</p> <p>La creación, utilización y difusión de cualquier tipo de material que ponga en peligro la seguridad de la red, que esté destinado a sabotear el uso de la red o que cause molestias o daños a otros usuarios (virus, escaneos indiscriminados, difusión de correo publicitario, cadenas de correo, accesos indebidos, congestión de enlaces).</p> <p>La conexión a la red de cualquier elemento físico o lógico que modifique la topología de la misma sin la debida</p>		
---	--	--

<p>autorización.</p> <p>La utilización de direcciones de red sin que hayan sido previamente asignadas por el Administrador de la red.</p> <p>No está permitida, en ningún caso, la manipulación de los componentes de la red (Router, switch, servidores, firewall, modem).</p> <p>Responsabilidades</p> <p>Es responsabilidad de cada usuario adoptar las medidas necesarias indicadas en este documento. Cuando se demuestre un uso incorrecto por personal de la organización, aplicar el proceso disciplinario establecido en el PR-HUM-05.</p> <p>En caso de ser personal externo a la compañía se suspende la prestación del servicio de conexión a CYFO, especialmente cuando la violación de las normas indicadas en este documento esté causando una degradación de los servicios de la red y/o implique a la compañía en algún tipo de responsabilidad, así como</p>		
---	--	--

<p>cuando suponga una modificación de la topología de la red o una conexión no autorizada. El administrador de la red es quien toma la decisión y es quien restablece la conexión en el momento en que se compruebe que el motivo de la suspensión se ha eliminado.</p> <p>Los servicios de red están protegidos por sistema antivirus el cual contiene a su vez firewall y sistema de detección de intrusos.</p>		
<p>4.7 Manejo de los medios (activos de almacenamiento)</p> <p>4.7.1 Procedimiento para la gestión de medios removibles.</p> <p>El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, SD, discos duros externos, IPod, celulares, cintas, Tablet) sobre la infraestructura para el procesamiento de la información de la compañía, es autorizado solo para aquellos colaboradores cuyo perfil del cargo y funciones lo requiera, tales como:</p> <p>Gerencia General Director Operativo</p>	<p>Coordinador TIC</p> <p>Directores</p> <p>Gerente General</p> <p>Coordinador de proyectos</p>	<p>RC-SIS-12 Bloqueo de puertos en equipos.</p> <p>RC-SIS-13 Destrucción de medios con información sensible.</p> <p>RC-SIS-33 Control de los medios removibles.</p>

<p>Director Comercial Directora Admón. Y financiera Coordinador TIC.</p> <p>Se autoriza también a los coordinadores de proyectos de campo el uso de medios removibles, ya que por razón de su trabajo requieren de estos medios para el trabajo en campo.</p> <p>Los cargos que nos están autorizados para manejar los medios removibles, pueden acceder a éstos, a través de una solicitud a los directores de área, donde detalle la información a copiar y la duración de la actividad. Los directores de área aprobarán vía correo electrónico dicha solicitud.</p> <p>El Coordinador TIC se encargará de la configuración de los puertos para el bloqueo de puertos USB-SD, unidad de CD-DVD- Blue ray; y su posterior retiro, se deja el registro control de medios removibles.</p> <p>Aplicar los siguientes controles para el manejo de los medios removibles: *Borrar la información del medio</p>		
--	--	--

<p>removible cuando no lo necesiten más.</p> <p>*La destrucción de un medio removible se gestiona de acuerdo a las disposiciones del numeral 4.7.2</p> <p>*La información almacenada en estos medios que necesiten estar disponibles más tiempo, deberán ser almacenados fuera de las instalaciones para evitar su pérdida o deterioro del medio.</p> <p>* Habilitar el uso de los medios removibles solamente si hay una razón de negocio para hacerlo.</p>		
<p>4.7.2 Eliminación de los medios.</p> <p>Llevar al comité de bajas todos los medios identificados en el anterior numeral y dejar un registro RC-COM-16 de su disposición final.</p> <p>Se tendrá en cuenta para dicho proceso, lo estipulado en el instructivo de bajas de inventario IN-COM-06</p> <p>Las acciones a realizar sobre medios que contengan información sensible pueden ser:</p> <ul style="list-style-type: none"> • Eliminar por incineración o trituración. 	<p>Coordinador TIC</p> <p>Comité de bajas</p>	<p>IN-COM-06 Comité de Bajas de Inventario</p> <p>RC-COM-16 Actas de bajas</p> <p>RC-SIS-13 Destrucción de medios con información sensible.</p>

<ul style="list-style-type: none"> • Formateo a bajo nivel para evitar el uso por parte de otra aplicación. 		
<p>4.7.3 Procedimiento para el manejo de la información.</p> <p>-Aplicar las disposiciones del procedimiento PR-SIS-02 para manejar, almacenar y clasificar la información de acuerdo a su criticidad así: publica, interna, confidencial, extremadamente confidencial.</p> <p>- Se restringe el acceso a la información solo a personal autorizado.</p> <p>-Almacenar la información en un entorno seguro de acuerdo a la disposición de almacenamiento dispuesto por el propietario de este.</p>	<p>Líderes de proceso</p> <p>Coordinador TIC</p>	<p>PR-SIS-02</p> <p>Gestión de activos de información (AI)</p>
<p>4.7.4 Seguridad de la documentación del sistema.</p> <p>Proteger la documentación del sistema de acceso no autorizado aplicando los siguientes controles:</p> <p>*Mantener la documentación del</p>	<p>Coordinador TIC</p> <p>Coordinadora del SGI</p>	<p>RC-SIS-15</p> <p>Matriz de identificación de documentos confidenciales y estrictamente confidenciales</p>

<p>sistema de forma segura</p> <p>* Tener la autorización del propietario de la información para acceder a la documentación del sistema.</p> <p>*La documentación del sistema clasificada como confidencial y estrictamente confidencial es protegida (encriptado) antes de ser enviada vía red pública.</p>		
<p>4.8 Intercambio de la información</p> <p><i>POLÍTICA DE INTERCAMBIO DE INFORMACIÓN:</i></p> <ul style="list-style-type: none"> ✓ Fomentar la transparencia en el intercambio de información puesta a disposición de partes externas. ✓ Excluir de publicación toda la información clasificada como confidencial y/o estrictamente confidencial. ✓ Compartir conocimiento directo y especialmente activo a través del contacto personal con los involucrados. ✓ El acceso y el uso de conocimiento basados en la en el respeto de los respectivos derechos de propiedad 	<p>Colaboradores</p> <p>Director</p> <p>Operativo</p>	<p>PR-PRO-08</p> <p>Control de servicios contratados externamente</p> <p>PO-SIS-07</p> <p>Intercambio de información</p>

<p>intelectual.</p> <ul style="list-style-type: none"> ✓ La información se puede transmitir solo cuando se esté seguro de su destinatario. ✓ En caso de información confidencial, deben aplicarse los controles criptográficos correspondientes. ✓ Evitar el uso de conexiones inalámbricas públicas, para el envío de información importante. ✓ Mantener actualizado el sistema de antivirus. ✓ Eliminar y/o proteger bajo llave la información importante que ya no se encuentre en uso. ✓ Evitar intercambio de información importante por llamadas telefónicas en lugares públicos. ✓ Reportar cualquier incidente relacionado al intercambio de la información. ✓ Evitar el intercambio de software, salvo que esta persona u organización cuente con la autorización para realizarlo. <p>Ver Procedimiento para el control de servicios contratados externamente, el intercambio de información con terceras</p>		
--	--	--

partes PR-PRO-08.		
<p>4.8.2 Acuerdos para el intercambio de información</p> <p>Aplicar el FO-PRO-09 acuerdo de confidencialidad cuando sea necesario intercambiar información con terceras partes</p> <p>-Usar el sistema de rotulación de la información sensible, asegurando que el significado de los rótulos es comprendido y que la información es apropiadamente protegida.</p> <p>- Aplicar la protección de datos, derechos de autor, licencias de software y consideraciones similares.</p> <p>Ver en el PR-PRO-08 “Control de servicios contratados externamente” las disposiciones sobre los acuerdos para el intercambio de la información y del software entre la organización y las partes externas.</p>	<p>Coordinador TIC</p> <p>Director Operativo</p>	<p>PR-PRO-08 Control de servicios contratados externamente</p> <p>FO-PRO-12 Lista de chequeo de requisitos para autorizar el acceso a la información por terceras partes</p> <p>FO-PRO-09 Acuerdo de confidencialidad</p>
<p>4.8.3 Medios físicos en tránsito.</p> <p>Aplicar los siguientes controles para minimizar las vulnerabilidades a acceso no autorizado, a mal uso, o a corrupción</p>	Colaborador	

<p>durante su transporte físico:</p> <ul style="list-style-type: none"> ✓ Usar transportadoras confiables ✓ Utilizar un medio de empaque confiable que proteja el contenido contra cualquier daño físico que pueda ocurrir. 		
<p>4.8.4 Mensajería electrónica.</p> <p>Se establecen las siguientes directrices para el manejo y protección de la información contenida en la mensajería electrónica.</p> <p>Utilizar contraseñas seguras para las cuentas de los cargos que por el manejo de información importante lo amerita como:</p> <ul style="list-style-type: none"> • Gerente General. • Directores (Administrativo, Operativo, Comercial). • Ejecutivos de cuenta. • Contadora. • Auxiliar contable. • Jefe de talento humano. • Coordinador TIC. • Junta de accionistas. <p>Las contraseñas serán conformadas</p>	<p>Coordinador TIC</p>	<p>RC-SIS-27 Control de claves de encriptación.</p>

<p>por 7 caracteres entre (Mayúsculas, minúsculas, números, Caracteres especiales).</p> <p>Verificar por parte de los usuarios del correo electrónico la correcta dirección del destinatario antes realizar el envío.</p> <p>Utilizar contraseñas para: *El ingreso al software de correo electrónico (Outlook, Thunderbird, Windows mail.).</p> <p>La información clasificada como confidencial y/o estrictamente confidencial se encripta aplicando lo establecido en el PR-SIS-06 Adquisición y mantenimiento de sistemas de información #4.3 controles criptográficos.</p>		
<p>4.8.5 Sistemas de información del negocio</p> <p>Aplicar los siguientes controles:</p> <ul style="list-style-type: none"> • Restringir el acceso a la información sensible • Establecer los usuarios que pueden acceder al sistema 	<p>Coordinador TIC</p>	<p>RC-SIS-01 Backup</p>

<ul style="list-style-type: none"> • Respaldo de la información para protección de la información asociada. 		
<p>4.9 Servicios de comercio electrónico</p> <p>4.9.1 – 4.9.2 Se excluye debido a que la organización no realiza comercialización electrónica, ni actividades afines por tal motivo no se cuenta con una plataforma para dicho fin.</p> <p>4.9.3 Información disponible al público</p> <p>Se realizan pruebas de vulnerabilidades al sitio web semestralmente, dado que la pagina está contratada con un tercero, adicional, se aplica los controles correspondiente a clasificación de la información y control de servicios contratados externamente.</p>		
<p>4.10 Monitoreo (de actividades no autorizadas)</p> <p>4.10.1 Registro de auditorías de los usuarios</p>	<p>Coordinador TIC</p>	<p>Visor de eventos de Windows</p>

<p>Mantener los registros de auditoria de las actividades de los usuarios para facilitar investigaciones futuras y para el monitoreo del control de acceso.</p> <p>Se excluye de esta disposición las veces en que sea necesario formatear un equipo, reemplazarlo por otro, o que la aplicación que realice el monitoreo se vea afectada y deba ser desinstalada.</p>		
<p>4.10.2 Monitoreo del uso del sistema</p> <p>Se establece el siguiente sistema de monitoreo para controlar que los usuarios solamente ejecuten actividades autorizadas explícitamente:</p> <ul style="list-style-type: none"> ✓ Intentos fallidos de ingresos tanto a la red como a sistemas de información y sistemas operativos. ✓ Encendido y detención del sistema. ✓ Cambio o intento de cambio en la configuración <p>Esta información es generada a través de visor de eventos de Windows, y dicha información será monitoreada</p>	<p>Coordinador TIC</p>	<p>Visor de eventos de Windows</p>

<p>semestralmente o cuando se tenga algún indicio de violación de controles.</p>		
<p>4.10.3 Protección de la información del registro</p> <p>Proteger los registros del sistema para evitar su modificación o eliminación así:</p> <ul style="list-style-type: none"> * Las aplicaciones generaran un registro de actividades que permiten de manera sencilla realizar seguimiento de operaciones y eventos. * Los registros de eventos aportan información sobre los sistemas, redes, aplicaciones y usuarios, el acceso a estos registros queda limitado a las personas autorizadas para su análisis. * Los registros son protegidos para evitar la modificación o eliminación no autorizada * Los registros de eventos serán utilizados como pistas de auditoría en la función de revisión y control. <p>La información es protegida por medio de backup y se encriptan los discos duros de los equipos portátiles.</p>	<p>Coordinador TIC</p>	<p>RC-SIS-01 Backup.</p> <p>PR-SIS-02 Gestión de activos de información.</p>

<p>4.10.4 Registros del administrador y del operador del sistema</p> <p>Administrar y monitorear semestralmente los registros de los logs del:</p> <ul style="list-style-type: none"> ✓ Servidor ✓ Red ✓ Equipos de computo ✓ Cámaras de seguridad ✓ Impresoras ✓ Antivirus <p>Dejar el registro de la evidencia del monitoreo.</p> <p>Los parámetros de monitoreo son:</p> <ul style="list-style-type: none"> ✓ El tiempo en el que ocurrió el evento (éxito o fracaso); ✓ Información acerca del evento (modificación de archivos) ✓ Información acerca de Fallas (errores que se presentaron y acciones correctivas que se tomaron). <p>La cuenta, el administrador u operador y los procesos involucrados.</p>	<p>Coordinador TIC</p>	<p>Visor de eventos de Windows</p>
<p>4.10.5 Registro de fallas</p> <p>Registrar y analizar las fallas reportadas por los usuarios por problemas de procesamiento de información o</p>	<p>Coordinador TIC</p>	<p>PR-SGI-05</p> <p>Acciones correctivas preventivas y de mejora.</p>

<p>sistemas de comunicación y tomar acciones correctivas para evitar la repetición del problema.</p> <p>Seguir el procedimiento de Gestión Incidentes, Peticiones de servicio y Problemas de la seguridad de la Información y de los Servicios TI PR-SIS-13 y el procedimiento de acciones correctivas, preventivas y de mejora PR-SGI-05.</p>		<p>PR-SIS-13</p> <p>Gestión Incidentes, Peticiones de servicio y Problemas de la seguridad de la Información y de los Servicios TI</p>
<p>4.10.6 Sincronización de relojes</p> <p>Sincronizar los relojes de los sistemas críticos identificados como: Teléfonos, Servidores, Equipos de cómputo, Lectores biométricos, los cuales tienen como patrón de medida, la hora legal Colombiana de internet: http://horalegal.sic.gov.co/</p> <p>Y su cambio en servidores es reportado en RC-SIS-21 control de cambios de los sistemas operativos y de información.</p>	<p>Coordinador TIC</p>	<p>RC-SIS-21</p> <p>Control de cambios de los sistemas operativos y de información</p>

8.2.8 Procedimiento Control de acceso a la información

<u>Procedimiento Control de acceso a la información</u>	<u>Código: PR-SIS-05</u>
	<u>Versión:01</u>

1. OBJETO

Impedir el acceso no autorizado a los sistemas de información, sistemas operativos, aplicaciones, bases de datos, y a la información.

Implementar técnicas de autenticación y autorización para el acceso seguro de los usuarios.

Controlar la seguridad en la conexión a redes.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

2. ALCANCE

Este procedimiento aplica a todos los procesos de la organización y a los usuarios (Colaboradores, Clientes, Contratistas, Proveedores) que tengan acceso de alguna manera a la red, sistemas operativos, comunicaciones móviles.

3. DEFINICIONES Y/O CONVENCIONES

Acceso: Es un flujo de información entre un sujeto y un objeto.

Sujeto: Es una entidad activa que solicita acceso a un objeto o a los datos de un objeto.

Objeto: Es una entidad pasiva que contiene Información.

Red: Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Usuario: Es un conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso. Es decir, un usuario puede ser tanto una persona como una máquina, un programa, etc.

Sistema operativo (SO): Es el software básico de una computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario.

Aplicación: Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

Sistema de información (SI): Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Esto lo diferencia principalmente de otros tipos de programas como los sistemas operativos (que hacen funcionar al ordenador), las utilidades (que realizan tareas de mantenimiento o de uso general), y los lenguajes de programación (con el cual se crean los programas informáticos).

Puertos de configuración: Son los puertos físicos comúnmente llamados de consola o de administración, o en ocasiones los llaman puertos auxiliares, y son aquellos puertos o interfaces que vienen en elementos de red (switches, routers, PBX) y que permiten configurar el aparato por primera vez.

Es aquel por el que se ingresa con un Hyperterminal mediante puerto COM1 (generalmente).

Sistema de aplicación: Es un conjunto integrado de programas de computación diseñados para determinada función que tiene actividades específicas de entrada, procesamiento y salida.

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1 POLITICA DE CONTROL DE ACCESO A LA INFORMACIÓN</p> <ul style="list-style-type: none"> • Permitir el acceso a la información necesaria para el desarrollo de sus actividades a los colaboradores, clientes, proveedores y contratistas autorizados. • Controlar el retiro de privilegios a los usuarios que ya no prestan servicios a la organización. • Facilitar privilegios de acceso a la información a terceras partes solamente durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas. • Dar acceso a la información teniendo en cuenta la clasificación de la misma al interior de la organización (Publica, Uso 	<p>Gerencia General Coordinador TIC</p>	<p>FO-CAL-04 Asistencia a eventos de capacitación y/o formación PO-SIS-11 Política de control de acceso a la información.</p>

<p>Interno, Confidencial, Extremadamente confidencial).</p> <ul style="list-style-type: none"> • Acatar la legislación pertinente y obligaciones contractuales, relacionadas con la protección del acceso a los datos. 		
<p>4.2 GESTIÓN DEL ACCESO DE USUARIOS</p> <p>4.2.1 Registro de usuarios</p> <p>*Utilizar IDs de usuarios únicos para permitir a los usuarios vincularse y ser responsables de sus acciones.</p> <p>* Verificar que el nivel de acceso otorgado sea apropiado para el propósito organizacional y que sea consistente con la política de seguridad de la organización.</p> <p>Procedimiento para el registro y cancelación de usuarios:</p> <p>➤ Registro:</p> <ul style="list-style-type: none"> - Diligenciar el registro de concesión y verificación de acceso a los SI. - Dar a conocer y firmar el acuerdo de uso e ingreso a los SI, cuando aplique. <p>➤ Cancelación:</p> <ul style="list-style-type: none"> - Eliminar y/o modificar el usuario con el 	<p>Coordinador TIC.</p>	<p>RC-SIS-68 Inventario de Sistemas de información.</p> <p>RC- SIS-69 Concesión y Verificación de acceso a los SI.</p>

<p>fin de restringir el acceso a los SI asignados, cuando dicha persona salga de la compañía o cambie de cargo y por ende de funciones.</p> <ul style="list-style-type: none"> - Antes de la firma del paz y salvo se debe realizar una verificación de los derechos otorgados en el registro RC-SIS-69. <p>Hacer uso del procedimiento disciplinario si los colaboradores intentan un ingreso no autorizado.</p>		
<p>4.2.2 Administración de privilegios</p> <p>Los siguientes sistemas de usuario múltiple que requieren protección contra el acceso no autorizado, se administran de acuerdo a la matriz RC-SIS-64.</p> <ul style="list-style-type: none"> ✓ Sistemas de información: <ul style="list-style-type: none"> • Geminus • Sistema UNO ✓ Sistemas operativos. ✓ Correo Electrónico. ✓ Bases de datos. • CMDB <p>Para otorgar privilegios a los sistemas es necesario ser un requerimiento mínimo para su rol funcional y contar con la autorización del Director de área.</p>	<p>Coordinador TIC</p>	<p>RC-SIS-64 Identificación de usuarios y asignación de privilegios.</p>

<p>Los privilegios se asignan a un ID de usuario diferente de aquellos utilizados para el uso normal de la organización.</p>		
<p>4.2.3 Gestión de contraseñas para usuarios</p> <p>Cambiar las contraseñas de los usuarios cada dos meses estas son entregadas personalmente, para poder verificar la identidad de un usuario, sin embargo para casos en que la persona se encuentre fuera de las instalaciones, se entregara telefónicamente directamente al usuario de la contraseña, previa autenticación y por reconocimiento de voz.</p> <p>Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica escrita. Tampoco deben ser comunicadas en conversaciones telefónicas a menos que el usuario se encuentre fuera de las instalaciones, proceder antes a la identificación del interlocutor.</p> <p>Para confirmar la entrega de contraseña</p>	<p>Coordinador TIC</p>	<p>RC-HUM-16 Acuerdo de confidencialidad y código de buena conducta</p> <p>RC-SIS-71 Entrega de contraseñas</p>

<p>se diligencia el registro RC-SIS-71 “Entrega de contraseñas”.</p> <p>Con el fin de velar por la confidencialidad de las contraseñas, todos los colaboradores al vincularse con la compañía firman un acuerdo de confidencialidad para preservar la información. Ver RC-HUM-16. Esta declaración incluye términos y condiciones laborales.</p> <p>Las claves secretas son almacenadas en un sistema de información de una forma segura.</p> <p>Las claves secretas predeterminadas por el vendedor son cambiadas después de la instalación del sistema o software.</p>		
<p>4.2.4 Revisión de los derechos de acceso de los usuarios</p> <p>-Revisar los derechos de acceso de los usuarios semestralmente a fin de garantizar que no se obtengan privilegios no autorizados y mantener un control eficaz del acceso a los datos y a los</p>	<p>Gestor de seguridad de la información.</p>	<p>RC-SIS-64 Identificación de usuarios y asignación de privilegios.</p>

<p>servicios de información.</p> <p>-Los derechos de acceso del usuario son revisados y re-asignados cuando se traslada es promovido dentro de la misma organización.</p> <p>- Revisar la asignación de privilegios a intervalos de 3 meses.</p> <p>-Registrar los cambios en las cuentas privilegiadas para una revisión periódica.</p>		
<p>4.3 RESPONSABILIDADES DE LOS USUARIOS</p> <p>4.3.1 Uso de Contraseñas</p> <p>Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas aplicando la siguiente política:</p> <ul style="list-style-type: none"> ✓ Mantener las contraseñas en secreto. ✓ Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas. ✓ Seleccionar contraseñas con longitud fija. ✓ Las contraseñas no deben estar basadas en datos que otros puedan 	<p>Coordinador TIC</p> <p>Usuarios</p>	<p>FO-CAL-04</p> <p>Asistencia a eventos de capacitación y/o formación</p> <p>PO-SIS-12</p> <p>Política de uso de contraseñas.</p>

<p>obtener fácilmente mediante información relacionada con el usuario (nombres, números de teléfono, fecha de nacimiento)</p> <ul style="list-style-type: none"> ✓ Evitar reutilizar o reciclar contraseñas. ✓ Cambiar las contraseñas temporales en el primer inicio de sesión. ✓ Evitar incluir contraseñas en los procesos automatizados de inicio de sesión. ✓ Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad. 		
<p>4.3.2 Equipo de usuario desatendido</p> <p>Aplicar bloqueo de seguridad para proteger la información de las terminales cuando el usuario se ausenta de su estación de trabajo utilizando las teclas (Windows + L).</p> <p>Aplicar el bloqueo automático a los dos minutos del equipo estar desatendido.</p>	<p>Coordinador TIC</p> <p>Usuarios</p>	
<p>4.3.3 Política de escritorio despejado y pantalla despejada.</p>		

<p>Se adopta la siguiente política para proteger documentos en medio físico, en disposición virtual y en dispositivos de almacenamiento removibles :</p> <ul style="list-style-type: none"> • Ocultar los documentos físicos y en medios removibles en gabinetes y/o cualquier otro medio seguro cuando no estén siendo utilizados, especialmente al ausentarse de la estación de trabajo o estando fuera del horario laboral. • Mantener bajo llave la información estrictamente confidencial. Controlar la recepción y envío de mensajería física, dejando registro de dichos elementos en el punto de acopio. • Restringir las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo. • Retirar inmediatamente la información sensible o confidencial, una vez impresa. • Mantener en el escritorio del equipo como máximo 6 iconos para evitar la pérdida o robo de la información. 	<p>Coordinador TIC</p> <p>Usuarios</p>	<p>FO-CAL-04 Asistencia a eventos de capacitación y/o formación</p> <p>PO-SIS-13 Política de escritorio limpio y pantalla despejada</p>
<p>4.4 CONTROL DE ACCESO A LAS REDES</p>		

<p>POLITICA DE USO DE LOS SERVICIOS DE RED</p> <ul style="list-style-type: none"> • Asignar cuentas de acceso a la red de datos organizacionales a cada colaborador que según sus funciones lo requiera. • Usar la red para acceder, ofrecer o tomar información siempre que esté de alguna forma relacionada con el entorno laboral, y que este uso se realice de forma responsable a fin de evitar perjuicios a/o de terceros • No permitir el acceso a la infraestructura de red y a los recursos suministrados por la compañía a personas u organizaciones ajenas sin autorización expresa • Restringir el acceso a la red de equipos de cómputo que no cuenten como mínimo con un software antivirus actualizado. • Restringir la conexión de medios removibles personales y/o de personal externo a la organización, en los equipos de cómputo de la compañía. • No permitir el uso de la red para cualquier acto que viole las leyes 	<p>Coordinador TIC</p> <p>Usuarios</p>	<p>FO-CAL-04</p> <p>Asistencia a eventos de capacitación y/o formación</p> <p>PO-SIS-14</p> <p>Política de acceso a las redes</p>
--	--	---

<p>vigentes.</p> <ul style="list-style-type: none"> • No permitir el uso de la red para fines privados comerciales, salvo autorización expresa. 		
<p>4.4.2 Autenticación de usuarios para conexiones externas</p> <p>Implementar medidas de encriptación de datos para las comunicaciones remotas de usuarios, en conjunto con una autenticación robusta. (VPN,token).</p>	<p>Coordinador TIC</p>	
<p>4.4.3 Identificación de los equipos en las redes</p> <p>Los equipos de la red son identificados de la siguiente manera:</p> <ul style="list-style-type: none"> • Tres dígitos de ubicación: OF1: Oficina 1 piso OF2: Oficina 2 Piso BG1: Bodega PRY: Proyectos externos. Y pueden ser creados más códigos, con forme se valla ampliando las instalaciones de la organización. • Guion intermedio entre la ubicación y el serial. • Tres últimos dígitos del serial del equipo (torre). 	<p>Coordinador TIC</p>	

<p>Y se realiza una identificación de cada equipo por su MAC, evitando así que otro equipo duplique o simule la identificación establecida.</p>		
<p>4.4.4 Protección de los puertos de configuración y diagnóstico remoto</p> <p>La empresa controla el acceso lógico y físico a los puestos de configuración así:</p> <p>Permitir el acceso físico a la zona segura 2 (Servidor de datos, voz y contabilidad) solo a personal autorizado.</p> <p>Considerar la identificación automática del equipo como un medio para autenticar las conexiones de ubicaciones y equipos específicos.</p>	<p>Coordinador TIC</p>	
<p>4.4.5 Separación en las redes</p> <p>La organización utiliza como método de control para la separación de las redes lo siguiente:</p> <p>Se divide la red principal mediante VPN a través de un switch en voz, datos e IP</p>	<p>Coordinador TIC</p>	

<p>públicas.</p> <p>Mediante routers divide la red principal en 2 redes de usuarios: CYFO (usuarios internos) y CYFO_INVITADOS (clientes, proveedores, contratistas), con el fin de proteger el acceso no autorizado a los sistemas críticos de la información de la organización.</p>		
<p>4.4.6 Control de conexión a las redes</p> <p>Se aplican controles para las aplicaciones atendiendo a horarios, los cuales estarán estipulados en el listado de control de privilegios, esto para los sistemas de información.</p> <p>Dado que para la organización es importante tener conexión 24 horas al correo electrónico, este no aplicará para los controles de conexión.</p> <p>Para las conexiones es a internet, como conexiones inalámbricas se aplicara un control de contraseña y se llevara el registro de autorización de conexión a las redes.</p>	<p>Coordinador TIC</p>	<p>RC-SIS-29 Autorización de Conexión a la red</p>
<p>4.4.7 Control de enrutamiento en la red.</p>		

<p>La organización dispone de enrutamiento manual, y utiliza direcciones IP fijas, con el fin de lograr un control más detallado y evitar conexiones no autorizadas.</p>		
<p>4.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO</p> <p>4.5.1 Procedimientos de registro de inicio seguro</p> <p>El siguiente es el procedimiento como medio de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos:</p> <ul style="list-style-type: none"> • Autenticar usuarios autorizados asignando una clave según # 4.2.3 Gestión de contraseñas para usuarios. • El registro de un usuario en el sistema operativo muestra un pantallazo en el cual solo aparece el campo para digitar la clave, minimizando la oportunidad de acceso no autorizado. • Limitar la cantidad de intentos fallidos permitidos a 3, después de estos, se debe reportar como incidente de seguridad de la información. 	<p>Coordinador TIC</p>	<p>RC-SIS-66 Registro de intentos exitosos y fallidos de ingreso al sistema.</p>

<ul style="list-style-type: none"> • Registrar intentos exitosos y fallidos de autenticación del sistema. RC-SIS-66 Registro de intentos exitosos y fallidos de ingreso al sistema. <p>Establecer un tiempo de espera de 12 horas antes de permitir intentos adicionales del registro de inicio, o mediante la habilitación a través de una cuenta de administrador.</p>		
<p>4.5.2 Identificación y autenticación de usuarios</p> <p>Permitir el uso de ID genéricos para una persona cuando las funciones accesibles o acciones llevadas a cabo por el ID no necesitan ser rastreadas (por ejemplo, sólo acceso de lectura), o cuando existen otros controles establecidos (por ejemplo, la clave secreta para un ID genérico sólo es emitido para una persona a la vez y se registra dicha instancia).</p>	<p>Coordinador TIC</p>	
<p>4.5.3 Sistema de gestión de contraseñas</p> <p>El sistema de gestión de contraseñas aplica las siguientes directrices:</p>		<p>PC-SIS-14</p>

<ul style="list-style-type: none"> • Las contraseñas son cambiadas según el plan de calidad PC-SIS-14 “Cambio de contraseñas” en los sistemas operativos, cuentas de Skype, correo electrónico y sistemas de información. • Se diligencia el registro RC-SIS-65 Matriz de contraseñas, para evitar la reutilización de contraseñas, y al cual se le aplicara control criptográfico. 	<p>Coordinador TIC</p>	<p>Cambio de Contraseñas</p> <p>RC-SIS-73 Histórico de contraseñas</p>
<p>4.5.4 Uso de las utilidades del sistema</p> <p>-Se restringe el acceso a la configuración de los sistemas operativos tanto de los equipos como de los servidores.</p> <p>- Aplicar la segregación de las utilidades del sistema del software de la aplicación.</p> <p>- Se limita el uso de las utilidades del sistema a un número práctico mínimo de usuarios autorizados y confiables.</p>	<p>Coordinador TIC</p>	
<p>4.5.5 Tiempo de inactividad de la sesión</p> <p>- Cerrar la aplicación y las sesiones en red después de un período de inactividad de 2 minutos.</p> <p>Ver 4.3.2 Equipo de usuario desatendido.</p>	<p>Coordinador TIC usuarios</p>	

<p>4.5.6 Limitación del tiempo de conexión</p> <p>Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.</p> <p>Documentar mediante comunicación escrita, firmada únicamente por el gerente general, al personal que no tienen restricciones horarias y las razones de su autorización, también al propietario de información sensible que requiera una extensión horaria ocasional.</p>	<p>Coordinador TIC</p>	<p>RC-SIS-67</p> <p>Autorizaciones de limitación de tiempo de conexión.</p>
<p>4.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN</p> <p>4.6.1 Restricción de Acceso a la Información</p> <p>Controlar los derechos de acceso de los usuarios; lectura, escritura, eliminar y ejecutar.</p> <p>Controlar los derechos de acceso de otras</p>	<p>Coordinador TIC</p>	

<p>aplicaciones.</p> <p>Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación.</p>		
<p>4.6.2 Aislamiento de los sistemas sensibles</p> <p>Identificar y documentar explícitamente la sensibilidad o confidencialidad del sistema de aplicación por parte del propietario de la aplicación sensible.</p> <p>Cuando una aplicación confidencial va a correr en un ambiente compartido, el propietario de la aplicación confidencial identifica y acepta los sistemas de aplicación con los cuales va a compartir recursos y los riesgos correspondientes.</p>	<p>Coordinador TIC</p> <p>usuarios</p>	
<p>4.7 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO</p> <p>4.7.1. Computación y comunicaciones móviles</p> <p>Política de computación y comunicaciones móviles:</p>		

<ul style="list-style-type: none"> ✓ Velar por que no se comprometa la información de la organización cuando se utilizan computadores portátiles livianos (notebooks) o computadores portátiles pesados (laptops) ✓ Permanecer el usuario siempre cerca del dispositivo. ✓ Disco duro encriptado ✓ No poner identificaciones de la organización en el dispositivo, salvo los estrictamente necesarios ✓ No poner datos de contacto técnico en el dispositivo. ✓ Mantener cifrada la información clasificada ✓ Realizar por parte de los usuarios respectivos la copia de seguridad de la información (backup) en memorias USB ✓ Aplicar proceso de gestión de contraseñas ✓ Mantener actualizado el sistema de protección antivirus. ✓ Prevenir a los usuarios sobre la conexión de sus equipos a redes externas y/o públicas ✓ Mantener el equipo protegido físicamente contra robo mediante 	<p>Coordinador TIC Usuarios</p>	<p>FO-CAL-04 Asistencia a eventos de capacitación y/o formación</p> <p>PO-SIS-15 Política de computación y comunicaciones móviles.</p>
--	---	--

<p>guaya que lo figue en sitios como vehículos, hoteles, centros de conferencia, sitios de reunión</p>		
<p>4.7.2. Trabajo Remoto</p> <p>Política de trabajo remoto.</p> <p>No permitir actividades de trabajo remoto:</p> <ul style="list-style-type: none"> - Para evitar el robo y/o divulgación no autorizada de información - Para evitar acceso remoto no autorizado a los sistemas internos de la organización o uso inadecuado de los servicios <p>Para evitar la contaminación por virus por transferencia de archivos.</p>	<p>Coordinador TIC</p>	<p>FO-CAL-04 Asistencia a eventos de capacitación y/o formación</p> <p>PO-SIS-16 Política de trabajo remoto.</p>

8.2.9 Procedimiento Adquisición y mantenimiento de sistemas de información

<u>Procedimiento Adquisición y mantenimiento de sistemas de información</u>	<u>Código: PR-SIS-06</u>
	<u>Versión:01</u>

1. OBJETO

Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos y reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

2. ALCANCE

Este procedimiento aplica a todos los sistemas de información e información clasificada como confidencial y estrictamente confidencial.

3. DEFINICIONES Y/O CONVENCIONES

Sistema de información (SI): Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Sistema operativo (SO): Es el software básico de una computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos hardware y el usuario.

Aplicación: Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

Esto lo diferencia principalmente de otros tipos de programas como los sistemas operativos (que hacen funcionar al ordenador), las utilidades (que realizan tareas de mantenimiento o de uso general), y los lenguajes de programación (con el cual se crean los programas informáticos).

Criptografía: Técnicas de cifrado y/o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes. Por tanto el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes.

Vulnerabilidad técnica: Son el resultado de bugs o de fallos en el diseño del sistema.

Parche: Es una actualización de un programa usado para solucionar problemas o la usabilidad de una versión previa de la aplicación.

Información confidencial: Es aquella información que es accesible únicamente por personal autorizado

Bugs: Un error de software, comúnmente conocido como bug (bicho), es un error o fallo en un programa de computador o sistema de software que desencadena un resultado indeseado.

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
4.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN		

<p>4.1.1 Análisis y especificación de los requisitos de seguridad</p> <p>Los requisitos de seguridad asociados a los sistemas de procesamiento de información que sean contratados externamente ya sea para desarrollo, arriendo o compra, se controlan de acuerdo a los siguientes lineamientos:</p> <ul style="list-style-type: none"> -Contar con un manual de usuario, sobre el manejo de la aplicación. -Disponer de un control de usuarios, para separar funciones dentro de la aplicación. -Todas las compras o contratos de arriendo de sistemas nuevos de procesamiento de información se realizan después de un proceso de prueba del producto. <p>Ver PR-SIS-04 # 4.3.2 (Aceptación del sistema).</p>	<p>Jefe de Almacén y compras</p> <p>Coordinador TIC</p>	<p>RC-SIS-25</p> <p>Criterios de aceptación de los sistemas de información.</p>
<p>4.2 PROCESAMIENTO CORRECTO EN LAS APLICACIONES</p> <p>Validación de los datos de entrada, control de procesamiento interno, integridad del mensaje y la validación de los datos de salida son excluidos dado que la organización no desarrolla software ni actividades afines, por consiguiente, no se requiere la infraestructura para dicha labor</p>		

<p>4.3 CONTROLES CRIPTOGRÁFICOS</p> <p>Aplicar los niveles de seguridad para proteger documentos clasificados como confidenciales y estrictamente confidenciales de acuerdo al procedimiento PR-SIS-02 Gestión de activos de información.</p> <p><i>POLÍTICA SOBRE EL USO DE LOS CONTROLES CRIPTOGRÁFICOS</i></p> <p>No enviar información de carácter crítico en el cuerpo del mensaje del correo electrónico, es preferible adjuntar el documento por correo electrónico con las medidas de seguridad establecidas.</p> <p>Utilizar técnicas de cifrado para impedir que personas no autorizadas puedan acceder a él.</p> <p>No enviar por correo electrónico, o mediante terceros, las claves de seguridad de los documentos enviados, estas deben ser informados al receptor en forma verbal o por correspondencia certificada.</p> <p>Crear contraseñas de acuerdo a las normas de seguridad establecidas por la organización.</p> <p>Exigir a cada colaborador su responsabilidad en la utilización de técnicas</p>	<p>Coordinador TIC</p>	<p>PR-SIS-05 Procedimientos y políticas para el control de acceso a la información.</p> <p>RC-SIS-15 Matriz de identificación de documentos confidenciales y estrictamente confidenciales</p> <p>PR-SIS-02 Gestión de activos de información</p> <p>PO-SIS-04 Uso de</p>
--	------------------------	--

<p>de cifrado establecidas por la organización.</p> <p>Respetar los derechos fundamentales de las personas, a la intimidad, incluyendo el secreto a las comunicaciones y la protección de los datos personales.</p> <p>Permitir el acceso legal a claves criptográficas, de los datos cifrados, cuando sea requerido por las autoridades respectivas.</p>		<p>controles criptográficos</p>
<p>4.3.2 Gestión de claves</p> <p>En la organización todas la claves criptográficas están protegidas contra:</p> <p>Modificación: Almacenar las clave en un software diseñado para tal fin.</p> <p>Perdida y destrucción: Aplicar el procedimiento PR-SIS-04 “Gestión de comunicaciones y operaciones” en el # 4.5 “Respaldo”.</p> <p>Divulgación no autorizada: Aplicar la política de gestión de contraseñas y utilizar el acuerdo de confidencialidad a las personas a quien aplique.</p> <p>Aplicar procedimiento establecido PR-SIS-05 “Procedimientos y políticas para el control de acceso a la información” # 4.2.3 “Gestión de contraseñas” para:</p> <ul style="list-style-type: none"> • Gestión de claves • Reglas para cambio y/o actualización 	<p>Coordinador TIC</p>	<p>PR-SIS-04 Gestión de comunicaciones y operaciones</p> <p>PR-SIS-05 Control de acceso a la información</p>

<p>de claves (cuando cambiarlas y cómo hacerlo).</p> <ul style="list-style-type: none"> • Recuperación de claves perdidas o corruptas. 		
<p>4.4 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA.</p> <p>4.4.1 Control del software operativo.</p> <p>Controlar las actualizaciones de la infraestructura tecnológica mediante:</p> <ul style="list-style-type: none"> -La actualización del software operacional, aplicaciones es realizada solo por personal autorizado. -Los sistemas operacionales sólo tienen códigos ejecutables aprobados, y no códigos de desarrollo o compiladores. -El software de las aplicaciones y el sistema de operación sólo se implementa después de una prueba extensa y satisfactoria por parte del proveedor y se llevan a cabo en ambientes separados. <p>Se cuenta con el backup de la información antes de implementar los cambios.</p>	<p>Coordinador TIC</p>	
<p>4.4.2 Protección de los datos de prueba del sistema y el control de acceso al código fuente de los programas son excluidos</p>	<p>Coordinador TIC</p>	

<p>debido a que la organización adquiere las aplicaciones con proveedores de fábrica, quienes manejan la base de datos y el código fuente de las mismas por lo tanto no se tiene acceso a dicha información.</p>		
<p>4.5 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE.</p> <p>Procedimiento de control de cambios, revisión técnica de las aplicaciones después de los cambios en el sistema operativo, las restricciones en los cambios a los paquetes de software y el desarrollo de software contratado externamente; son excluidas dado que los proveedores de los sistemas de información son los dueños del código fuente.</p>	<p>Coordinador TIC</p>	
<p>4.5.1 Control de cambios</p> <p>Aplicar el procedimiento de control de cambios PR-SIS-15 para gestionar los cambios en los sistemas operativos y en las aplicaciones críticas (Geminus, Sistema UNO).</p>	<p>Coordinador TIC</p>	<p>PR-SIS-15 Gestión de Cambios de los servicios TI</p>
<p>4.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema</p>	<p>Coordinador TIC</p>	

<p>Controlar los cambios de los sistemas operativos a través del procedimiento de cambios dispuesto, y realizar pruebas de las aplicaciones críticas (Geminus, Sistema UNO), en ambientes de prueba antes de realizar dicha implementación.</p>		
<p>4.5.4 Fuga de información.</p> <ul style="list-style-type: none"> -Bloquear puertos USB, DVD, CD de los equipos de cómputo. -Restringir la navegación de páginas como YouTube, redes sociales, Hotmail, Yahoo. -Monitorear las actividades del personal y del sistema, cuando sea permitido bajo la legislación o regulación existente. -Monitorear la utilización del recurso en los sistemas de cómputo. 	<p>Coordinador TIC</p>	
<p>4.5.5 Desarrollo de software contratado externamente</p> <p>Dejar por escrito en el contrato de la aplicación, el número de licencias, propiedad del código desarrollado, derechos de propiedad intelectual de dicho código, certificado de calidad de la aplicación en caso de aplicar, y el proveedor debe realizar las pruebas en nuestro ambiente de</p>	<p>Coordinador TIC</p>	

pruebas.		
<p>4.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA.</p> <p>4.6.1 Control de las vulnerabilidades técnicas:</p> <p>Contratar un proveedor que certifique las vulnerabilidades técnicas de la red de la organización.</p> <p>Considerar las vulnerabilidades identificadas en el mapa de riesgos para evaluar el impacto y la probabilidad y tomar acciones si lo amerita.</p> <p>Contar con un inventario de los sistemas de información, el cual tiene los campos de vendedor del software, números de versión, personas responsables del software (usuarios).</p> <p>Mantener contacto (correo electrónico, telefónico) con el proveedor del sistema de información, con el fin obtener información y estar actualizados en las últimas versiones y/o parches (RC-SIS-68).</p> <p>Dependiendo la criticidad de la vulnerabilidad encontrada y/o reportada por el fabricante se actuara de la siguiente manera:</p>	<p>Coordinador TIC</p>	<p>RC-SIS-68 Inventario de Sistemas de información</p> <p>RC-SIS-61 Reporte de vulnerabilidades encontradas.</p>

<p>Leve: Puede tratarse en los siguientes 5 días, después de detectada la vulnerabilidad.</p> <p>Media: Puede tratarse en los siguientes 2 días, después de detectada la vulnerabilidad.</p> <p>Critica: Debe tratarse el día, en el cual se detecta la vulnerabilidad.</p> <p>Dado que el tamaño de la organización no facilita la posibilidad de realizar pruebas en sistemas alternos, para probar los parches y/o actualizaciones de los sistemas de información, se realizara una copia de seguridad del sistema a tratar, con el fin de poder restaurar a un estado anterior, en caso de que los cambios afecten o causen daños no deseados.</p>		
---	--	--

8.2.10 Procedimiento Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información

<u>Procedimiento Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información</u>	<u>Código: PR-SIS-07</u>
	<u>Versión:01</u>

1. OBJETO

Asegurar que los sistemas de Gestión de la Organización cumplan con las normas y políticas vigentes relacionadas con la seguridad de la información

2. ALCANCE

Aplica a todos los procesos de la organización que manejan y procesan información soportada en: papel, disco magnético, óptico o electrónico, fotografía o muestra patrón o una combinación de éstos.

3. DEFINICIONES Y/O CONVENCIONES

Derechos de propiedad intelectual (DPI): es el poder directo e inmediato sobre un objeto o bien, por la que se atribuye a su titular la capacidad de disponer del mismo, sin más limitaciones que las que imponga la ley. Es el derecho real que implica el ejercicio de las facultades jurídicas más amplias que el ordenamiento jurídico concede sobre un bien

Terceros: Todos aquellos grupos de interés que no están directamente relacionados con los procesos de la organización.

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1 CUMPLIMIENTOS DE LOS REQUISITOS LEGALES</p> <p>4.1.1 Identificación de la legislación aplicable</p> <p>Identificar todos los requisitos normativos y contractuales para cada sistema de información y de la organización en el RC-CAL-22 y mantenerlo actualizado por parte del asesor jurídico; de acuerdo a los cambios que se generen en la legislación colombiana.</p> <p>Asignar a todos los colaboradores, las responsabilidades y funciones individuales para cumplir con dichos requisitos gestión.</p>	<p>Asesor Jurídico</p> <p>Jefe de Talento Humano</p> <p>Colaboradores</p>	<p>RC-CAL-22</p> <p>Inventario de requisitos legales y otros</p> <p>MC-HUM-01</p> <p>Manual de funciones</p>
<p>4.1.2 Aseguramiento del cumplimiento de los requisitos legales</p> <ul style="list-style-type: none"> • Adquirir software a través de fuentes conocidas y acreditadas asegurando que 		<p>RC-SIS-08</p> <p>Control de visitantes y equipos</p>

<p>no sean vulnerados los derechos de autor y requerir los soportes que constaten la legalidad de las mismas</p> <ul style="list-style-type: none"> • Custodiar las licencias físicas y claves de acceso • Realizar periódicamente por parte del Gestor SI-TI un control en todos los equipos de cómputo de la organización con el fin de identificar el uso de programas no autorizados • Considerar dentro del proceso disciplinario sanciones aplicables a la instalación y uso de programas sin autorización o ilegales. • Controlar el ingreso de equipos de cómputo a las instalaciones por parte de terceros • Suscribir acuerdos de confidencialidad con todos los grupos de interés de acuerdo a lo indicado en el PR-PRO-08 	<p>Auxiliar Administrativa</p> <p>Jefe de Talento Humano</p> <p>Director Operativo</p> <p>Gestor SI-TI</p>	<p>RC-HUM-16 Acuerdo de confidencialidad de la información y código de buena conducta</p> <p>FO-PRO-09 Acuerdo de confidencialidad</p> <p>PR-HUM-05 Proceso Disciplinario</p> <p>PR-PRO-08 Control de servicios contratados externamente</p>
<p>4.2 Cumplimiento de los derechos de propiedad intelectual (DPI).</p> <p>Con el fin de asegurar el cumplimiento de los requisitos sobre el uso de material y software con derechos de propiedad intelectual o patentes, la organización dispone:</p>	<p>Gestor SI-TI</p>	<p>PC-SIS-01 Plan de calidad para el control de actualización de los programas ofimáticos.</p> <p>RC-SIS-41 Inventario de los</p>

<ul style="list-style-type: none"> • Identificar los tipos de software utilizados, alcances y usos dentro de la ley de propiedad intelectual • Monitorear licencias adquiridas por la compañía en cuanto a la vigencia y usuarios permitidos • Renovar las licencias utilizadas antes de la fecha de vencimiento. • Restringir la reproducción, cesión o transformación del material protegido por normas de propiedad intelectual • Prohibir estrictamente la descarga y el uso de programas informáticos sin la correspondiente licencia y permisos de autor • Prohibir la reproducción de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización 		<p>activos de información</p> <p>PR-HUM-05 Proceso disciplinario</p> <p>PO-SIS-02 Cumplimiento de los derechos de propiedad intelectual</p> <p>FO-PRO-09 Acuerdo de confidencialidad</p>
<p>4.3 Protección de los registros de la organización.</p> <p>4.3.1 Identificación y clasificación de los registros importantes:</p> <p>Cada proceso debe identificar estos documentos en el listado maestro de registros, teniendo en cuenta las siguientes consideraciones</p> <ul style="list-style-type: none"> ✓ Identificación 		

<ul style="list-style-type: none"> ✓ Clasificación del tipo de información ✓ Versión ✓ Almacenamiento ✓ Protección ✓ Recuperación ✓ Tiempo de retención ✓ Disposición final 		
<p>4.3.2 Protección contra pérdida, destrucción y/o falsificación:</p> <ul style="list-style-type: none"> ✓ Registros virtuales: Implementación de mecanismos para bloquear y restringir el acceso de códigos maliciosos y virus ✓ Registros físicos: Disponer dentro de las instalaciones mobiliario acondicionado para custodiar y proteger la información importante. Contratar con un agente externo la custodia del archivo inactivo y documentos de gran valor para la organización. ✓ Establecer un inventario de información relacionado con claves criptográficas y programas asociados con archivos encriptados o firmas digitales 	<p>Líderes de proceso</p> <p>Gestor SI-TI</p> <p>Directora Administrativa y Financiera</p>	<p>PR-SGI-02 Control de Registros</p> <p>RC-SIS-15 Matriz de identificación de documentos confidenciales y estrictamente confidenciales</p> <p>RC-SIS-41 Inventario de los activos de información</p>

<p>4.4 Protección de los datos y privacidad de la información personal.</p> <p>Con el fin de garantizar la privacidad de la información personal, la organización determina:</p> <p>Establecer mediante documento escrito el compromiso por parte de la organización de darle tratamiento a la información personal de acuerdo con la legislación,</p> <p>Solicitar autorización al colaborador para divulgar la información que él mismo haya catalogado como confidencial e informado a la empresa de dicha consideración.</p> <p>Custodiar las hojas de vida del personal</p>	<p>Jefe de Talento Humano</p>	<p>RC-HUM-16 Acuerdo de confidencialidad de la información y código de buena conducta</p> <p>RC-HUM-06 Hojas de vida</p> <p>PO-SIS-03 Protección de los datos personales</p>
<p>4.5 Medidas de prevención por uso inadecuado de los servicios de procesamiento de información</p> <p>Capacitar a los administradores de la información sobre el uso adecuado de los servicios de procesamiento de la información.</p> <p>Implementar el procedimiento disciplinario en</p>	<p>Jefe de Talento Humano</p> <p>Gestor SI-TI</p>	<p>FO-CAL-04 Asistencia a eventos de capacitación y/o formación</p> <p>RC-HUM-03 Inducción-Reinducción al personal</p>

<p>el cual se establecen medidas sancionatorias por el uso inadecuado de la información</p>		
<p>4.6 Reglamentación de los controles criptográficos.</p> <p>Aplicar gestión de contraseñas en los documentos clasificados como confidenciales y estrictamente confidenciales con control criptográfico.</p> <p>Mantener actualizada la matriz de identificación de documentos confidenciales y estrictamente confidenciales de acuerdo al PR-SIS-06 Adquisición, desarrollo y mantenimiento de los sistemas de información</p> <p>Las contraseñas, códigos o números de identificación personal son encriptados durante la transmisión y en su medio de almacenamiento.</p> <p>Las contraseñas, códigos, firmas digitales y demás son asignadas por el Gestor SI-TI.</p>	<p>Gestor SI-TI</p>	<p>RC-SIS-15 Matriz de identificación de documentos confidenciales y estrictamente confidenciales</p> <p>PR-SIS- 06 Adquisición, desarrollo y mantenimiento de los sistemas de información</p> <p>PO-SIS-04 Uso de controles criptográficos</p>
<p>4.7 Cumplimiento de las políticas y las normas de seguridad y cumplimiento</p>	<p>Gestor SI-TI</p>	<p>PC-SIS-05</p>

<p>técnico</p> <p>Verificación del cumplimiento técnico</p> <p>Ejecutar un plan anual para verificar periódicamente que los sistemas de información cumpla con las políticas y procedimientos de seguridad con el fin de aplicar los controles de hardware y software para su correcta implementación.</p> <p>Auditar periódicamente y de acuerdo al plan de auditorías los procesos responsables de políticas y normas de seguridad.</p>		<p>Plan de auditorías a los sistemas operativos y de información</p>
<p>4.8 Controles de auditoría de los sistemas de información.</p> <p>Realizar un plan de verificación de los sistemas operativos y de información, el cual incluya hora y tiempo de duración de la auditoría con el fin de minimizar los riesgos de interrupciones del negocio.</p> <p>Compartir el plan de verificación y acordar con los jefes de áreas involucradas, la ejecución del mismo para establecer medidas de contingencia en el caso de la suspensión del servicio.</p>	<p>Gestor SI-TI</p> <p>Audidores internos</p>	<p>PC-SIS-05</p> <p>Plan de auditorías a los sistemas operativos y de información</p>

<p>Monitorear y registrar todos los accesos para producir un histórico de referencia; considerar como mínimo:</p> <ul style="list-style-type: none"> -Fecha y hora - Usuario - Tipo de acceso - Programa y/o función utilizada <p>Limitar las verificaciones a un acceso de “sólo lectura” al software y los datos.</p> <p>Permitir un acceso diferente al de “sólo lectura” para copias aisladas de los archivos del sistema, los cuales se puedan borrar cuando termine la auditoría, o se les pueda proteger apropiadamente si existe la obligación de mantener dichos archivos como parte de la evidencia de la auditoría.</p> <p>Considerar el principio de auditoría, el cual indica que la(s) personas(s) que llevan a cabo la auditoría deben ser independientes a las actividades auditadas.</p> <p>Gestionar con terceros que deban realizar actividades en las cuales se utilicen los activos de información de la organización, los trámites pertinentes con el fin de que se</p>		
---	--	--

<p>acojan a la política de seguridad y den el cumplimiento técnico corporativo que le aplique.</p>		
<p>4.9 Protección de las herramientas de auditoría de los sistemas de información</p> <p>Asignar a todos los colaboradores que tengan acceso a los sistemas operativos y de información cuentas de usuario estándar con el fin de limitar los privilegios y evitar el uso inadecuado de las herramientas de auditoría.</p>	<p>Gestor SI-TI</p>	

8.2.11 Procedimiento Mantenimiento de activos de información

<u>Procedimiento Mantenimiento de activos de información</u>	<u>Código: PR-SIS-08</u>
	<u>Versión:01</u>

1. OBJETO

Mantener la operación correcta de los equipos de la Organización

2. ALCANCE

Este procedimiento debe aplicarse a todos los equipos de cómputo que tiene procesos directamente relacionados con la seguridad de la información y sistemas de información de la organización.

3. DEFINICIONES Y/O CONVENCIONES

Mantenimiento preventivo: es el destinado a la conservación de los equipos de cómputo mediante su revisión y reparación, con el fin de asegurar su buen funcionamiento y fiabilidad.

Mantenimiento Correctivo: es una forma de mantenimiento destinado a corregir un fallo o problema que surge en un equipo de cómputo, con el objetivo de restablecer la operatividad del mismo.

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
4.1 Manteniendo Preventivo	Coordinador	PC-SIS-02

<p>Periodicidad El mantenimiento preventivo se realiza de acuerdo al plan establecido para tal labor</p> <p>Responsabilidad El Coordinador TIC está al tanto de la ejecución y efectividad del plan; y en caso de que dicho mantenimiento sea contratado externamente debe velar por el cumplimiento de lo estipulado en el PR-PRO-08 “Control de servicios contratados externamente” suscribiendo el acuerdo de confidencialidad con el proveedor del servicio.</p>	<p>TIC</p>	<p>Plan de calidad para el mantenimiento de los equipos tecnológicos y accesorios.</p> <p>RC-SIS-07 Mantenimiento de los equipos y accesorios y/o instalación de software</p> <p>PR-PRO-08 Control de servicios contratados externamente</p>
<p>4.2 Mantenimiento Correctivo</p> <p>4.2.1 Identificación y reporte de las fallas Informar mediante los canales de comunicación al Coordinador TIC las fallas que presentan en el activo de información por parte del propietario.</p>	<p>Auxiliar Administrativa</p> <p>Jefe de Talento Humano</p> <p>Director Operativo</p>	<p>RC-CAL-04 Acciones correctivas, preventivas y de mejora y seguimiento</p> <p>FO-CAL-01 Diagrama Causa y Efecto</p>

<p>4.2.2 Análisis de fallas</p> <p>Registrar y analizar las fallas presentadas en los activos de información</p> <p>Nota: Si en el análisis, se concluye que la falla del activo es total, este es dado de baja de acuerdo, se guardan las copias de respaldo y se procede a eliminar de forma segura la información.</p> <p>4.2.3 Resolución de las fallas</p> <p>El área de sistemas cuenta con un tiempo de respuesta máxima de 4 horas para resolver las fallas reportadas.</p> <p>Cuando dicha reparación depende de terceros, el plazo de resolución será el acordado con el proveedor del servicio.</p>	<p>Gestor SI TI</p>	<p>PR-SGI-04</p> <p>Acciones correctivas, preventivas y de mejora y seguimiento</p>
--	---------------------	---

8.2.12 Procedimiento Copias de Respaldo

<u>Procedimiento Copias de Respaldo</u>	<u>Código: PR-SIS-09</u>
	<u>Versión:01</u>

1. OBJETO

Proteger y garantizar que los recursos del sistema de información (aplicaciones críticas) de la organización se mantengan respaldados y sean fácilmente recuperables en el momento que se necesite.

2. ALCANCE

Inicia con la programación que se tiene definida para hacer copias de seguridad de las bases de datos de los sistemas de información y termina con la verificación del Backup y posterior custodia de dichas copias de seguridad.

3. DEFINICIONES Y/O CONVENCIONES

Backup: Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o CD`s o disco duro), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto. Es conveniente realizar copias de seguridad a intervalos temporales fijos (diario o semanal, por ejemplo), en función del trabajo y de la importancia de los datos manejados.

Copia de Respaldo o Seguridad: Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales.

Copias de Seguridad: copias de la información en un medio magnético que se almacena en un lugar seguro.

Contingencia: Conjunto de procedimientos de recuperación. Las acciones a contemplar aplican para Antes- Durante- Después con el fin de reducir las pérdidas.

Plan de Contingencia: procedimientos alternativos de una organización cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando alguna de sus funciones se vean afectadas por un accidente interno o externo.

Recuperación: Hace referencia a las técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

Restauración: Volver a poner algo en el estado inicial.

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Integridad: Se refiere a la corrección y complementación de los datos en una base de datos. Cuando los contenidos se modifican con sentencias INSERT, DELETE o UPDATE, la integridad de los datos almacenados puede perderse de muchas maneras diferentes. Pueden añadirse datos no válidos a la base de datos, tales como un pedido que especifica un producto no existente.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista. De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Disponibilidad: Es una medida que nos indica cuanto tiempo está ese equipo o sistema operativo respecto de la duración total durante la que se hubiese deseado que funcionase. Típicamente se expresa en porcentaje. No debe de ser confundida con la rapidez de respuesta.

Encriptación: Es el proceso para volver ilegible información considerada importante. La información una vez encriptado sólo puede leerse aplicándole una clave.

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p style="text-align: center;">POLÍTICA DE RESPALDO</p> <p><input type="checkbox"/> No podrán subirse a las copias de seguridad: Archivos de música, información personal, software (salvo debida autorización).</p> <p><input type="checkbox"/> Cada líder de proceso o propietario del activo de información, es el responsable de la información a la cual se le realiza la copia de respaldo, y por el correcto funcionamiento y</p>		<p>PO-SIS-08 Respaldo</p>

<p>actualización de la misma.</p> <p>Nota: en caso de desastre véase el plan de continuidad y disponibilidad del servicio PC-DIR-05.</p>		
<p>4.1. Gestionar el backup</p> <p>Determinar e identificar en la matriz de respaldo las aplicaciones y la información sensible que requieren copias de seguridad, la cual contiene el tipo de copia (incremental, diferencial, completa).</p>	<p>Coordinador TIC</p> <p>Líderes de procesos</p>	<p>RC-SIS-10</p> <p>Matriz de respaldo de información.</p>
<p>4.1.1 Copias de seguridad servidores</p> <p>Realizar copias completas de configuración cada 6 meses a los servidores si estos no han tenido ningún cambio relevante, o inmediatamente después de haber realizado un cambio significativo y este haya sido satisfactorio.</p> <p>Realizar copia de seguridad de la información mínimo 1 vez a la semana con el fin de salvaguardar los archivos subidos o actualizados recientemente.</p>	<p>Coordinador TIC</p>	
<p>4.1.2 Copias de seguridad a las aplicaciones</p>	<p>Coordinador TIC</p>	

<p>Realizar semanalmente una copia de respaldo completa a las aplicaciones Geminus y sistema UNO.</p>		
<p>4.1.3 Copias de seguridad a las contraseñas de encriptación</p> <p>Realizar mensualmente una copia de respaldo en la cual se contemple el documento “Matriz de identificación de documentos confidenciales y estrictamente confidenciales”.</p>	<p>Coordinador TIC</p>	
<p>4.1.4 Copias de seguridad a la información almacenada en los equipos de computó</p> <p>Realizar copias de seguridad a la información precisada por los líderes de los procesos.</p> <p>Realizar las copias de seguridad a la información de los equipos de cómputo de los siguientes cargos:</p> <ul style="list-style-type: none"> • Coordinador TIC • Auxiliar de ingeniería • Contadora (a) • Director (a) administrativa y financiera. • Asistente contable • Gerente General • Director Operativo 	<p>Coordinador TIC</p> <p>Líderes de procesos</p>	

<ul style="list-style-type: none"> • Ejecutivo de cuenta • Coordinadora SGI <p>Realizar el backup así:</p> <p>1. Configuración de las carpetas Crear un directorio (carpeta) en el cual se van a ubicar toda la información precisada a la cual hay que realizarle el Backup</p> <p>2. Configuración del Software Para la realización de dicha copia requerimos de un software que lo realice, y este debe ser configurado apuntando al lugar que nos va a almacenar los Backup por determinado tiempo.</p> <p>3. Configuración de la recepción de Backup Para cumplir esta actividad, debemos crear una carpeta en el servidor, en este caso (192.168.1.65), dicha carpeta debe ser creada con el nombre de usuario y debe ser compartida con protección por inicio de sesión.</p> <p>4. Configuración de Acronis -Abrimos el programa -Click en “Other backups” y file backups -En la sección “Source”, buscamos o</p>		
--	--	--

<p>seleccionamos los archivos a los cuales les vamos a realizar el Backup.</p> <p>-En la sección “Destination”, seleccionamos la opción que dice: “Browse...” y allí buscamos la carpeta que hemos creado y compartido con anterioridad.</p> <p>Ejemplo: \\cyfo_server\nombre_carpeta\</p> <p>5. Inicio de sección para conexión con la carpeta.</p> <p>En el anuncio siguiente “This location may require credentials”, damos click en enter credentials y allí ingresamos el nombre de usuario y la contraseña que fueron signados.</p>		
<p>4.2 Verificar la ejecución del backup</p> <p>Verificar a través de un correo electrónico automático a la cuenta backup@cyfo.net, el éxito o falla del backup.</p> <p>Verificar los archivos logs del servidor, si este nos indicar error es necesario volver a realizar copia por segunda vez.</p> <p>Comprimir los archivos en formato .zip o .rar si la copia se realiza correctamente y verificar las copias comprimidas, para verificar que se pueden descomprimir cuando se necesiten.</p>	<p>Coordinador TIC</p>	

<p>4.3 Controles de seguridad a las copias de seguridad</p> <p>Realizar semanalmente una copia de seguridad incremental en un dispositivo de almacenamiento (disco duro) a todas las copias de seguridad realizadas y enviarla a custodiar por un ente externo.</p> <p>Realizar semanalmente una copia de seguridad completa a la información de los servidores, equipos de cómputo, aplicaciones y contraseñas; almacenarla en un dispositivo (CD) y enviarla a custodiar por un ente externo.</p> <p>Controlar el envío de las copias de seguridad al ente externo, diligenciando el registro “control de las copias de seguridad” donde se describa la información enviada, fecha de creación (respaldo) y fecha de envío.</p> <p>Y como protección adicional se sube la información crítica de la organización a un sistema en la nube (DropBox).</p>	<p>Coordinador TIC</p>	<p>RC-SIS-01 Backup</p>
--	------------------------	-------------------------

<p>4.4 Actividades de Restauración de la información</p> <p>-Configuración de carpetas: Identificar la carpeta que contiene el backup de la información a restaurar.</p> <p>-Configuración del Software: Para la realización de dicha restauración requerimos de un software que lo realice, y este debe ser configurado apuntando al lugar en el que esta almacenada la copia de seguridad.</p> <p>-Carga del backup: Damos click en “recuperar” y seleccionamos la carpeta que contiene la copia de seguridad, el sistema realiza un escaneo de las versiones anteriores, y nos muestra un consolidado de información.</p> <p>-Restauración: Damos click en “recuperar”, y acto siguiente seleccionamos el destino donde queremos restaurar dicha información.</p>	<p>Coordinador TIC</p>	<p>RC-SIS-11 Restauración Backup</p>
<p>4.5 Pruebas de Restauración de la información</p> <p>Realizar un simulacro mensual para la restauración de la información a dos equipos</p>	<p>Coordinador TIC</p>	<p>RC-SIS-45 Prueba de restauración de información.</p>

tomados aleatoriamente con el fin de verificar el estado de dicha información y estar preparados ante una situación real.		
---	--	--

8.2.13 Procedimiento Manejo de Medios

<u>Procedimiento Manejo de Medios</u>	<u>Código: PR-SIS-11</u>
	<u>Versión:01</u>

1. OBJETO

Mantener el control y seguridad de los medios de almacenamiento removible estableciendo responsabilidades y procedimientos para la gestión y operación de los mismos.

2. ALCANCE

El presente documento incluye las disposiciones para gestionar los medios removibles y el tratamiento que se debe aplicar a los activos de información para procurar la disponibilidad, confidencialidad e integridad de la información.

3. DEFINICIONES Y/O CONVENCIONES

Medio removible: Son aquellos medios de almacenamiento diseñados para ser extraídos de la computadora sin tener que apagarla

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
4.1 Manejo de los medios 4.1.1 Procedimiento para la gestión de medios removibles. El uso de medios de almacenamiento		

<p>removibles (ejemplo: CDs, DVDs, USBs, SD, discos duros externos, IPod, celulares, cintas, Tablet) sobre la infraestructura para el procesamiento de la información de la compañía, es autorizado solo para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera, tales como:</p> <p>Gerencia General Director Operativo Director Comercial Directora Admón. Y financiera Coordinador TIC.</p> <p>Se autoriza también a los coordinadores de proyectos el uso de medios removibles, ya que por razón de su trabajo</p> <p>Los cargos a quienes no se les autoriza el manejo de medios removibles, pueden utilizar estos medios, a través de los cargos autorizados.</p> <p>El Coordinador TIC es responsable de implementar los mecanismos y establecer los controles necesarios para asegurar los sistemas de información de CYFO, como:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Bloqueo de puertos USB-SD. <input type="checkbox"/> Bloqueo de unidad de cd-DVD-blue ray. <p>Así mismo, es responsabilidad del</p>	<p>Coordinador TIC</p> <p>Directores</p> <p>Gerente General</p> <p>Coordinador de proyecto.</p>	<p>RC-SIS-12 Bloqueo de puertos en equipos.</p> <p>RC-SIS-13 Destrucción de medios con información sensible.</p>
---	---	--

<p>funcionario autorizado para el uso de medios removibles, la seguridad física y lógica a fin de evitar la pérdida, el daño, la divulgación, modificación y destrucción de la información de la compañía que éste contiene.</p> <p>Para el retiro de medios removibles se aplica lo estipulado en el #4.1.2 de este procedimiento, dejando con ello registro de lo sucedido en el RC-SIS-13 Destrucción de medios con información sensible.</p> <p>En caso de manejar información vital en medios removibles, dicha información es copiada al equipo para realizar la copia de seguridad de la misma, de ser posible incluirla en la carpeta para tal fin.</p>		
<p>4.1.2 Eliminación de los medios.</p> <p>Llevar al comité de bajas todos los medios identificados en el anterior numeral y dejar un registro RC-COM-16 de su disposición final.</p> <p>Se tendrá en cuenta para dicho proceso, lo estipulado en el instructivo de bajas de inventario IN-COM-06</p>	<p>Coordinador TIC</p> <p>comité de bajas</p>	<p>IN-COM-06</p> <p>Comité de Bajas de Inventario</p> <p>RC-COM-16</p> <p>Actas de bajas</p> <p>RC-SIS-13</p> <p>Destrucción de medios con</p>

<p>Las acciones a realizar sobre medios que contengan información sensible pueden ser:</p> <ul style="list-style-type: none"><input type="checkbox"/> Eliminar por incineración o trituración.<input type="checkbox"/> Formateo a bajo nivel para evitar el uso por parte de otra aplicación.		información sensible.
--	--	-----------------------

8.2.14 Procedimiento Gestión de incidentes de seguridad de la información y de servicios TI

<u>Procedimiento Gestión de incidentes de seguridad de la información y de servicios TI</u>	<u>Código: PR-SIS-13</u>
	<u>Versión:01</u>

1. OBJETO

Recuperar el nivel habitual de funcionamiento de los servicios TI y minimizar en todo lo posible el impacto negativo en la organización de forma que la seguridad de la información y la disponibilidad del servicio se mantengan, mediante la identificación proactiva, el análisis de las causas y la gestión de los problemas.

2. ALCANCE

Este procedimiento cubre todos los incidentes que se presenten en la gestión de la seguridad de la información y en la operación de los servicios TI.

3. DEFINICIONES Y/O CONVENCIONES

Activo: cualquier cosa que tiene valor para la organización.

Activo de información: recurso del sistema de información o relacionado con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la Dirección.

Incidente: Violación de una política de seguridad que puede desencadenar en un evento que no hace parte de la operación normales de un servicio, el cual causa, o puede causar, una interrupción o reducción de la calidad del servicio.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los

activos.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Incidencia grave: es una incidencia que tiene mayor urgencia debido a su alto impacto en el negocio.

Problema: causa de una o más incidencias.

SI Seguridad de la información: Preservación de la confidencialidad, integridad y accesibilidad de la información

Error conocido: Problema que tiene identificados una causa raíz o un método para reducir o eliminar su impacto sobre un servicio mediante un arreglo provisional

Impacto: Se basa en la escala del daño potencial o real para el usuario. El impacto está a menudo basado en cómo serán afectados los niveles de servicio. El impacto y la urgencia se emplean para asignar la prioridad.

Urgencia: Una medida del tiempo en que una incidencia, un problema o un cambio tendrán un impacto significativo para el negocio. Se basa en el tiempo que transcurre entre la detección del incidente o el problema y la solución del incidente

Riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos

Base de datos de errores conocidos KEDB: Base de datos que contiene todos los registros de errores conocidos. Esta base de datos es utilizada por gestión de Incidencias y gestión de problemas y hacer parte del sistema de gestión de configuración.

Elemento de configuración CI (Configuration Item): Elemento que es necesario controlar con el fin de prestar uno o varios servicios.

Éstos son algunos elementos de configuración CI:

- Dispositivos de hardware: como PCs, impresoras, routers, monitores, así como sus componentes: tarjetas de red, teclados, lectores de CDs.
- Software: sistemas operativos, aplicaciones, protocolos de red, etc.
- Documentación: manuales, acuerdos de niveles de servicio SLA, etc.

Base de Datos de Gestión de la Configuración CMDB: (Configuration Management Data Base), Base de datos utilizada para registrar atributos de los elementos de configuración CI, y las relaciones entre los elementos de configuración durante todo su ciclo de vida del servicio.

Esta base de datos debe incluir:

- Información detallada de cada elemento de configuración
- Interrelaciones entre los diferentes elementos de configuración, como por ejemplo: relaciones “padre-hijo” o Interdependencias tanto lógicas como físicas

Solicitud de cambio (request for change): Propuesta de un cambio en un servicio, un componente del servicio o del sistema de gestión de servicio.

Nota: un cambio en un servicio incluye la provisión de un servicio nuevo o el retiro de un servicio que ya no se requiere.

Causa Raíz: La causa original o subyacente de una incidencia o problema

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>POLÍTICA DE GESTIÓN DE INCIDENTES DE SI</p> <p>Es política de Cyfo Comunicaciones</p> <ul style="list-style-type: none"> ➤ Adoptar medidas de seguridad eficientes para proteger sus activos de información. ➤ Informar de forma completa e inmediata al Gestor de la SI la existencia de un potencial incidente de seguridad información que afecte los activos de información de la organización. ➤ Responder por la integridad de la información generada o en su poder. ➤ Aprender de los incidentes de seguridad de la información, para prevenir nuevas ocurrencias.. ➤ Empezar actividades post-incidente, como mejoras a los procesos de SI y asegurar la retención de evidencias. 	<p>Colaboradores</p> <p>Contratistas</p> <p>Terceras partes</p>	<p>PO-SIS-05</p> <p>Gestión de incidentes de SI</p>

<p>4.1 Registro y clasificación de los incidentes y/o problemas de SI</p> <p>Recibir por parte de colaboradores las solicitudes de servicio por el siguiente canal de comunicación: http://192.168.1.65/cmdb/web/pages/UI.php</p> <p>Evaluar por parte del Gestor SI-TI la solicitud de servicio y en caso de clasificarse como un incidente de seguridad, registrarlo en el módulo de incidentes del aplicativo ITOP para tratarlo de acuerdo al siguiente procedimiento:</p>	<p>Gestor de SI –TI</p>	
<p>4.1.1 Priorizar la resolución de los incidentes y/o problemas</p> <p>Determinar, dependiendo del impacto, un nivel de criticidad del incidente de acuerdo a la siguiente clasificación:</p> <ul style="list-style-type: none"> •Nivel de criticidad 1: Leve <p>Debe ser resuelto, pero su nivel de urgencia es bajo. En este caso, la</p>	<p>Gestor de SI –TI</p>	<p>RC-SIS-32</p> <p>Matriz del nivel de criticidad de los incidentes</p>

<p>organización experimenta poco o ningún daño, pero tal incidente es un indicador claro de que alguien o algo está intentando penetrar a los sistemas o encontrar vulnerabilidades que explotar, o fallas puntuales que no interrumpen la prestación de los servicios TI.</p> <p>•Nivel de criticidad 2: Moderado</p> <p>Implica que el daño está ocurriendo a la organización, por ejemplo, ha sido expuesta información de cuentas de usuario que pueden ser utilizadas para realizar un acceso no autorizado o una interrupción de los servicio TI.</p> <p>•Nivel de criticidad 3: Grave</p> <p>Indica que la organización está corriendo peligro. Por ejemplo, un acceso no autorizado o borrado de la información almacenada, que no suspende el servicio TI por lo que se requiere atención inmediata para prevenir que el incidente escale a un nivel muy grave.</p> <p>•Nivel de criticidad 4: Muy Grave</p> <p>Indica que la organización está corriendo peligro. Por ejemplo, un acceso no autorizado o borrado de la información</p>		
---	--	--

<p>almacenada en un servidor crítico, una suspensión de los servicio TI. Durante una crisis, todo el tiempo y recursos deben ser destinados a remediar el problema.</p> <p>Registrar en el RC-SIS-32, la siguiente información para determinar el nivel de la criticidad de los incidentes presentados a fin de tomar las decisiones y acciones apropiadas:</p> <ul style="list-style-type: none"> • Número y fecha del incidente • Descripción del incidente • Efecto negativo producido (grave, moderado, leve) • Criticidad de los recursos afectados (alta, media, baja) y • Nivel de criticidad del incidente.(Muy grave, grave, moderado, leve) <p>Es responsabilidad del Gestor del SI- TI, mantener informado a la Gerencia general de la presencia de incidentes Muy graves.</p>		
--	--	--

<p>4.1.2 Determinar, dependiendo del nivel de criticidad, el tiempo de resolución de acuerdo de a la siguiente tabla</p> <table border="1" data-bbox="315 499 883 972"> <thead> <tr> <th data-bbox="315 499 508 638">Nivel de criticidad</th> <th data-bbox="508 499 883 638">Tiempo de resolución</th> </tr> </thead> <tbody> <tr> <td data-bbox="315 638 508 747">Leve</td> <td data-bbox="508 638 883 747">En las 48 horas siguientes a la detección</td> </tr> <tr> <td data-bbox="315 747 508 856">Moderado</td> <td data-bbox="508 747 883 856">En las 12 horas siguientes a la detección</td> </tr> <tr> <td data-bbox="315 856 508 932">Grave</td> <td data-bbox="508 856 883 932">En la 1 hora siguiente a la detección</td> </tr> <tr> <td data-bbox="315 932 508 972">Muy Grave</td> <td data-bbox="508 932 883 972">Inmediato</td> </tr> </tbody> </table>	Nivel de criticidad	Tiempo de resolución	Leve	En las 48 horas siguientes a la detección	Moderado	En las 12 horas siguientes a la detección	Grave	En la 1 hora siguiente a la detección	Muy Grave	Inmediato	Gestor de SI –TI	RC-SIS-32 Matriz del nivel de criticidad de los incidentes
Nivel de criticidad	Tiempo de resolución											
Leve	En las 48 horas siguientes a la detección											
Moderado	En las 12 horas siguientes a la detección											
Grave	En la 1 hora siguiente a la detección											
Muy Grave	Inmediato											
<p>4.1.3 Costos de los incidentes</p> <p>Calcular los costos de los incidentes reportados estimando un valor del incidente por:</p> <ul style="list-style-type: none"> ○ Pérdida de productividad ○ Pérdida de información ○ Recuperación de la información 	Gestor de SI –TI	RC-SIS-32 Matriz del nivel de criticidad de los incidentes										

<p>4.1.4 Análisis del incidente y/o problemas de SI</p> <p>Conformar un equipo de trabajo que involucre el Gestor de SI</p> <p>-TI y los implicados en el incidente, con el fin de realizar una lluvia de ideas sobre el incidente presentado, analizarlos e identificar la causa raíz que ocasiono el incidente.</p>	<p>Gestor de SI –TI</p>	<p>FO-CAL-01</p> <p>Diagrama Causa y Efecto</p>
<p>4.1.5 Tratamiento de los incidentes y/o problemas de SI</p> <p>Establecer un plan de acción para eliminar las causas reales y potenciales soportados en la metodología del procedimiento PR-SGI-05</p>	<p>Gestor de SI –TI</p>	<p>PR-SGI-05</p> <p>Acciones correctivas, preventivas y de mejora y seguimiento</p> <p>Información</p> <p>RC -CAL-04</p> <p>Acciones correctivas, preventivas y de mejora y seguimiento</p>
<p>4.1.6 Cierre del incidente</p> <p>El Gestor de SI-TI realiza el siguiente proceso para el cierre definitivo del</p>		

<p>incidente detectado:</p> <ul style="list-style-type: none"> • Informar al usuario que reporto la solicitud de servicio, la resolución del incidente. • Actualizar la información en la base de datos de gestión de configuraciones sobre los elementos de configuración implicados en el incidente. • Elaborar una solicitud de cambio (RFC) cuando se presente un cambio en un elemento de configuración CI • Cierre del incidente <p>Monitorear y revisar la eficacia de las acciones tomadas para los incidentes tratados, tres meses después del cierre de las acciones.</p>	<p>Gestor de SI –TI</p>	<p>Aplicación ITOP</p>
<p>4.1.7 Gestión de cambios</p> <p>Gestionar los cambios por el módulo de “cambios”, si se requiere para dar resolución a los incidentes reportados aplicando el procedimiento de gestión de cambios.</p>		<p>PR-SIS-15 Gestión de Cambios</p>
<p>4.2 Responsabilidad por el manejo del incidente de SI- TI</p> <p>Es responsabilidad del Gestor de la SI-TI, la administración de los incidentes,</p>		

<p>proporcionando una respuesta rápida, eficaz y ordena de los incidentes, atendiendo especialmente a los incidentes clasificados como graves.</p> <p>-Definir los recursos necesarios para su resolución y valoración del costo del incidente:</p> <ul style="list-style-type: none"> • En horas de trabajo del recurso humano • En costo de compra de equipos o software necesario para la gestión del incidente • En costo de contratación de servicios profesionales para la gestión del incidente (solo si es necesario) <p>- Mantener informado al usuario que reporta el incidente sobre el progreso del mismo.</p>	<p>Gestor de SI –TI</p>	
<p>4.3 Escalado de incidentes SI-TI</p> <p>Si los incidentes no se pueden resolver por el procedimiento anteriormente descrito en el numeral 4.1, es necesario realizar un escalamiento de acuerdo a los siguientes niveles de resolución</p> <p>Primer Nivel de Resolución</p>	<p>Gestor de SI –TI</p> <p>Gerente general</p>	

<p>Resolver los incidentes, peticiones de servicio y problemas por parte del Gestor SI-TI. Si éste no se puede resolverlos debe ser transferido al segundo nivel de resolución.</p> <p>Segundo Nivel de Resolución Resolver el incidente por parte de la Gerencia general quién podrá involucrar grupos de soporte especiales tales como: Asesores, abogados, proveedores y otros.</p> <p>Si no es posible corregir la raíz del problema, se trasfiere el caso a un tercer nivel de resolución.</p> <p>Tercer Nivel de Resolución Resolver el incidente por una tercera instancia de resolución externa y de tipo legal.</p>		
<p>4.4 Evidencias de Incidentes de SI</p> <p>Procurar que todo incidente SI-TI este acompañado de algún tipo de evidencia que respalde la información suministrada. Estas evidencias resultan fundamentales para la aplicación del proceso disciplinario PR-HUM-05.</p>	<p>Gestor de SI-TI</p>	<p>PR-HUM-05 Disciplinario</p>

<p>Almacenar el documento de soporte y/o evidencia del incidente, en las mismas condiciones de: almacenamiento, protección, tiempo de retención y disposición final del registro que lo referencia.</p> <p>Cuando el incidente implica acciones legales (civiles o penales) contra una persona o contra la organización, la evidencia se debe recolectar, retener y presentar para cumplir con las reglas de evidencia establecidas en la jurisdicción pertinente.</p> <p>Cuando se considere un incidente grave que requiera la investigación de un ente oficial, se debe dejar las evidencias vírgenes sin manipularlas para que se han recolectadas por expertos forenses.</p>		
---	--	--

8.2.15 Procedimiento Gestión de cambios

<u>Procedimiento Gestión de cambios</u>	<u>Código: PR-SIS-15</u>
	<u>Versión:01</u>

1. OBJETO

Asegurar que todos los cambios en la gestión de la seguridad de la información y de los servicios TI son registrados, evaluados, aprobados, implementados y revisados de manera controlada.

2. ALCANCE

Aplica a todos los cambios que se presenten en un servicio o componente del servicio TI y en las aplicaciones de misión crítica para la organización
No aplica para solicitudes de escasa importancia que no tienen un impacto significativo en la infraestructura TI y que se repiten periódicamente.

3. DEFINICIONES Y/O CONVENCIONES

Solicitud de cambio RFC (request for change): Propuesta de un cambio en un servicio, un componente de servicio o al sistema de gestión del servicio

Elemento de configuración CI (configuration item): Elemento que es necesario controlar para proveer uno o varios servicios

Base de datos de la configuración CMDB (configuration management database): Base de datos utilizada para registrar atributos de los elementos de

configuración, y las relaciones entre los elementos de configuración, a lo largo del ciclo de vida del servicio.

Componente del servicio (service component): Unidad individual de un servicio que cuando se combina con otras unidades provee un servicio completo, ejemplos: Hardware, software, herramientas, aplicaciones, documentación, información, procesos o servicios de soporte

Cambio: Adición, modificación o eliminación de algo que podría afectar a los servicios de TI. El alcance debe incluir cambios en todas las arquitecturas, procesos, herramientas, métricas y documentación, así como cambios en los servicios de TI y otros elementos de configuración.

Evaluación de cambios: Es el proceso responsable de la evaluación formal de un servicio de TI nuevo o modificado, para asegurar que los riesgos han sido gestionados y para ayudar a determinar si el cambio debe ser autorizado

Gestión de cambios: Proceso responsable del control del ciclo de vida de los cambios, permitiendo la ejecución de los cambios beneficiosos minimizando el impacto en los servicios de TI.

Cambio Estándar: Son cambios ya establecidos, preautorizados por la Organización y para los cuales ya existe un procedimiento definido. Por ejemplo el movimiento del PC de un usuario.

Cambio Normal: Estos cambios también tienen un procedimiento establecido pero requieren de valoración y autorización del CAB.

Cambio de Emergencia: Estos cambios solo se pueden realizar para reparar un error grave en un servicio de T.I. con un alto impacto para el Negocio.

Comité Asesor de Cambios (Change Advisory Board) CAB: Se trata de un grupo de personas que aconseja al Gestor SI-TI en la evaluación, establecimiento de prioridades y programación de cambios.

El CAB está compuesto por el Gestor SI-TI, Coordinador del SGI y el Gerente general.

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>POLITICA DE GESTIÓN DE CAMBIOS</p> <ul style="list-style-type: none"> ✓ Nivel de tolerancia cero para los cambios no autorizados ✓ Gestionar y controlar los elementos de configuración identificados para los servicios TI. ✓ Responsabilidad por el cambio durante todo el ciclo de vida del servicio TI. ✓ Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área. ✓ Evaluar el impacto de los cambios teniendo en cuenta la viabilidad, la pertinencia y urgencia del mismo. 	<p>Gestor SI-TI</p>	<p>PO-SIS-09 Gestión de cambios en los servicios TI</p>
<p>4.1 Registro, aceptación, clasificación, evaluación y aprobación de las solicitudes de cambio</p> <p>4.1.1 Registro de la solicitud de cambio</p>		

<p>Registrar todas las solicitudes de cambio que se reciban por el IT Service manager en el módulo de cambios.</p> <p>Registra</p> <ul style="list-style-type: none"> ✓ Nombre del solicitante ✓ Alcance del cambio ✓ Descripción del cambio propuesto <p>Nota: El Gestor SI-TI es el responsable de la gestión del cambio.</p> <p>Revisar semestralmente el módulo de los cambios, con el fin de detectar incrementos y tendencias en los cambios.</p> <p>Llevar el registro de cada una de las solicitudes de cambio a la base de datos RC-SIS-75 para tener una trazabilidad de los mismos.</p>	<p>Gestor SI-TI</p> <p>Colaboradores</p>	<p>RC-SIS-75</p> <p>Base de datos de los cambios en los servicios TI</p>
<p>4.1.2 Evaluación y aceptación de la solicitud de cambio</p> <p>El CAB Comité Asesor de Cambios (Change Advisory Board) es un grupo de personas que tienen la responsabilidad de evaluar, establecer prioridades y programar los</p>	<p>CAB</p>	

<p>cambios. El CAB está compuesto por el Gestor SI-TI, Director operativo o administrativo y el Gerente general.</p> <p>Evaluar la solicitud de cambio después de su registro inicial por parte del CAB.</p> <p>Rechazar una la solicitud, si se considera que el cambio no está bien justificado o si se considera que algunos aspectos de la misma son susceptibles de mejora o mayor definición.</p> <p>En cualquiera de los casos, devolver por correo electrónico por parte del Gestor SI-TI, la solicitud al proceso que la solicitó con el objeto de que se realicen nuevas propuestas a favor de dicha solicitud.</p> <p>Nota: La aceptación del cambio no implica su posterior aprobación por el CAB y es sólo indicación de que se ha encontrado justificado su posterior procesamiento.</p> <p>Evaluar por parte del CAB minuciosamente la aprobación de un cambio teniendo en cuenta las siguientes consideraciones:</p> <ul style="list-style-type: none"> ✓ ¿Cuáles son los beneficios esperados del cambio propuesto? ✓ ¿Justifican esos beneficios los costos 		
---	--	--

<p>asociados al proceso de cambio?</p> <ul style="list-style-type: none"> ✓ ¿Cuáles son los riesgos asociados? ✓ ¿Disponemos de los recursos necesarios para llevar a cabo el cambio con garantías de éxito? ✓ ¿Puede demorarse el cambio? ✓ ¿Cuál será el impacto general sobre la infraestructura y la calidad de los servicios TI? ✓ ¿Puede el cambio afectar los niveles establecidos de seguridad TI? <p>Si el cambio es aprobado por el CAB, se inicia la etapa de la planificación del cambio para su posterior implementación. En caso contrario, solicitar más argumentos a la solicitud inicial.</p> <p>Un cambio de la categoría preautorizado no necesita la aprobación del CAB y debe ser implementado directamente.</p>		
<p>4.1.3 Clasificación de la solicitud de cambio</p> <p>Asignar por el CAB la prioridad y la categoría dependiendo de la urgencia e impacto de la misma.</p> <p>Determinar la categoría y la prioridad de la solicitud para determinar la asignación de</p>	<p>Gestor SI-TI</p>	<p>RC-SIS-48 Cronograma de cambios</p>

recursos necesarios, los plazos previstos y el nivel de autorización requerido para la implementación del cambio

Determinar la categoría con base en el impacto sobre la organización y el esfuerzo requerido para su implementación, así:

CATEGORÍA DEL CAMBIO	DESCRIPCIÓN
MAYOR	Un impacto de gran importancia y/o cantidad muy grande de recursos necesarios, o un impacto probable sobre otras partes de la Organización.
MENOR	Sólo un impacto de poca importancia, y pocos recursos necesarios
PREAUTORIZADO	Un cambio recurrente, bien conocido, para el que existe un procedimiento predefinido a seguir, con un riesgo relativamente bajo.

Nota: una solicitud de cambio para eliminar un servicio o para transferirlo a un cliente o a un tercero se clasifica en la categoría “Mayor”

Gestionar mediante el procedimiento de “Diseño y transición de los servicios nuevos o

modificados” las solicitudes de cambio clasificadas en la categoría “Mayor”.

Determinar la prioridad y la importancia relativa de la solicitud de cambio respecto a otras solicitudes así:

PRIORIDAD	DESCRIPCIÓN	TIEMPO ATENCIÓN
URGENTE	Se necesita una acción inmediata. Puede ser necesario convocar reuniones urgentes del comité de cambios. Si es necesario se asignan recursos para desarrollar los cambios autorizados.	Minutos
MEDIA	Será asignada una prioridad media en cuanto a la asignación de recursos.	Día
BAJA	El cambio es justificable y necesario, pero puede esperar hasta la próxima entrega o actualización programada. Serán asignados unos recursos de acuerdo con esto.	Días

4.1.4 Cambios de emergencia

Encontrar una respuesta inmediata cuando se interrumpe un servicio TI, ya sea por el número de usuarios afectados o porque se han visto involucrados sistemas o servicios

Gestor SI-TI

<p>críticos para la organización</p> <p>Aplicar el siguiente procedimiento:</p> <ul style="list-style-type: none"> ✓ Convocar una reunión urgente del CAB ✓ Es válida una decisión del Gestor SI-TI si es imposible demorar la resolución del problema o éste sucede durante un fin de semana o periodo vacacional (lo que puede dificultar la reunión del CAB). ✓ Restaurar el servicio, aunque los registros en la CMDB y la documentación asociada al cambio se realicen posteriormente. ✓ Disponer al cierre del cambio de emergencia, la misma información de la que se dispondría tras un cambio normal. Si no se procede así, se pueden provocar situaciones de configuraciones registradas incorrectamente que serían fuente de nuevas incidencias y problemas. 		
<p>4.2 Planificación del cambio</p> <p>Acordar y definir el cronograma de cambios RC-SIS-48 para su entrega e implementación, diligenciando la siguiente información:</p> <ul style="list-style-type: none"> ✓ La descripción del cambio aprobado ✓ Categoría del cambio ✓ Prioridad del cambio 	<p>Gestor SI-TI</p>	<p>RC-SIS-48 Cronograma de cambios</p>

<ul style="list-style-type: none"> ✓ Fecha inicio ✓ Fecha terminación ✓ Responsable del cambio ✓ Fecha de evaluación de resultados ✓ Eficacia del cambio <p>Informar a los implicados el cambio aprobado, por correo electrónico con copia del cronograma del cambio una vez esté definido por el CAB.</p>		
<p>4.2.1 Identificación de riesgos y plan de continuidad</p> <p>Identificar los posibles riesgos que pueden vulnerar las actividades programadas en la planificación del cambio RC-SIS-48, una vez se identificados, definir las actividades de continuidad en: el antes, el durante y el después para cada actividad establecida en el cronograma de actividades.</p>	Gestor SI-TI	RC-SIS-48 Cronograma de cambios
<p>4.3 Ejecución y prueba de los cambios</p> <p>Supervisar y coordinar los cambios de acuerdo al “cronograma de cambios” para asegurar que se cumplen con las fechas previstas para el cambio.</p>	Gestor SI-TI	RC-SIS-48 Cronograma de cambios PR-SGI-05 Acciones

<p>Realizar simulaciones y pruebas reales del cambio en lo que respecta a su: funcionalidad, usabilidad y accesibilidad</p> <p>Actualizar los registros de la CMDB, después de un cambio exitoso.</p> <p>Aplicar en caso de un cambio no satisfactorio el ítem 4.3.1 de este procedimiento.</p>		<p>correctivas, preventivas y de mejora.</p>
<p>4.3.1 Planificación para revertir un cambio no satisfactorio</p> <p>Planificar y cuando sea posible probar las actividades para revertir o remediar una cambio no satisfactorio así:</p> <ul style="list-style-type: none"> -Considerar el backups de la última actualización del cambio antes de su fracaso. - Revisar las fallas del cambio no satisfactorio - Analizar las causas, encontrar la causa raíz de la falla - Establecer un plan de acción acordado con los usuarios afectados. -Aplicar el PR-SGI-05 Acciones correctivas, preventivas y de mejora. - Volver al ítem 4.2 planificación del cambio 		<p>PR-SGI-05 Acciones correctivas, preventivas y de mejora.</p>
<p>4.4 Determinar la eficacia del cambio</p> <p>Revisar la eficacia de los cambios</p>	<p>Gestor SI-TI</p>	<p>RC-SIS-48 Cronograma de cambios</p>

<p>diligenciando el registro RC-SIS-48 y acordar con las partes interesadas</p> <p>Analizar las solicitudes de cambio cada 6 meses para detectar tendencias e identificar las oportunidades de mejora en el FO-CAL-03 Análisis de datos.</p>		<p>FO-CAL-03</p> <p>Análisis de datos</p>
--	--	---

8.2.16 Procedimiento Gestión de las Relaciones con el Negocio y Gestión con los proveedores

<u>Procedimiento Gestión de las Relaciones con el Negocio y Gestión con los proveedores</u>	<u>Código: PR-SIS-19</u>
	<u>Versión:01</u>

1. OBJETO

Establecer y mantener una buena relación entre la organización y el cliente, basándose en el entendimiento mutuo y los fundamentos del negocio y gestionar las relaciones con los proveedores para garantizar la provisión sin interrupciones de los servicios TI.

2. ALCANCE

Aplica para los servicios TI que la organización ofrece a sus usuarios

3. DEFINICIONES Y/O CONVENCIONES

Indicadores del nivel del servicio SLA: Son métricas que permiten identificar el grado de cumplimiento de los acuerdos entre un proveedor de servicio y su cliente

SLA (Service Level Agreement) Acuerdo documentados entre el proveedor del servicio y el cliente que identifica los servicios y sus objetivos.

UC (Underpinning Contract) Contrato de soporte: Es un contrato entre la organización y un Tercero. El Tercero proporciona bienes o Servicios que soportan la entrega de un servicio al Cliente. El contrato de soporte define objetivos y responsabilidades que son requerirlas para alcanzar los objetivos de Nivel de Servicio en un SLA.

Gestor SI-TI: Administrador de la seguridad de la información y de los servicios de tecnología de la información.

Selección de proveedores: Proceso aplicado para elegir una o varias cosas entre otras demostrando una preferencia.

Re-evaluación de proveedores: Proceso para determinar si un proveedor activo ha cumplido y continúa como proveedor habitual de la organización

Proveedor potencial: Proveedor evaluado que potencialmente puede llegar ser proveedor habitual de la organización

Proveedor activo: proveedor seleccionado que suministra habitualmente recursos a la organización

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1 Gestión de las relaciones con el negocio</p> <p>4.1.1 Identificación de los clientes de los servicios TI</p> <p>Los clientes de los servicios de tecnología de la información son todos los colaboradores del área administrativa y algunos operativos que lo requieran para cumplir con sus funciones y responsabilidades.</p>	Gestor SI-TI	

<p>Es responsabilidad del Gestor SI-TI gestionar la relación y satisfacción de los clientes de los servicios TI.</p>		
<p>4.1.2 Comunicación con el cliente</p> <p>Utilizar “http://192.168.1.65/cmdb/web/pages/UI.php” como medio de comunicación con los clientes para realizar las solicitudes de servicio</p>	<p>Gestor SI-TI</p>	<p>PC-SIS-10 Catálogo y plan de gestión de servicios TI</p>
<p>4.1.3 Desempeño de los servicios TI</p> <p>Revisar mensualmente el desempeño de cada servicio frente a los objetivos planteados, documentar los resultados en el RC-SIS-42 Informes de desempeño de los servicios.</p> <p>Llevar el informe de desempeño al comité de gestión integral para revisar y considerar los resultados obtenidos del Informe para identificar las No conformidades, sus causas y determinar las acciones necesarias, aplicando el proceso de acciones correctivas,</p>	<p>Gestor SI-TI</p>	<p>RC-SIS-42 Informes de desempeño de los servicios.</p> <p>PR-SGI-05 Acciones correctivas, preventivas y de mejora y seguimiento</p>

preventiva y/o de mejora		
<p>4.1.4 Reclamación sobre el Servicio TI</p> <p>Gestionar y documentar los reclamos recibidos de los clientes sobre los servicios de tecnología de la información.</p> <p>Investigar, tratar, reportar, cerrar y escalar el incidente, de acuerdo al PR-SIS-13 Gestión de incidentes de seguridad de la información y de servicios TI.</p> <p>Informar a los clientes el mecanismo de escalado de los reclamos cuando este no se puede resolver por los canales normales.</p> <p>Ver numeral 4.5 del procedimiento PR-SIS-13 Gestión de incidentes de seguridad de la información y de servicios TI.</p>	Gestor SI-TI	PR-SIS-13 Gestión de incidentes de seguridad de la información y de servicios TI
<p>4.1.5 Satisfacción de los clientes de los servicios TI</p> <p>Enviar a los clientes bimestralmente por correo electrónico, la encuesta de satisfacción Online para ser diligenciada</p>	Gestor SI-TI	Encuesta Online de satisfacción RC-CAL-04 Acciones correctivas, preventivas y de mejora y

<p>Medir y analizar los resultados de la satisfacción del cliente y tomar acciones si los resultados están por debajo del nivel 4 de satisfacción.</p>		<p>seguimiento</p>
<p>4.2 Gestión de relaciones con los proveedores TI y con terceras partes</p> <p>Aplicar el formulario “Registro de evaluación de proveedores” para conocer las condiciones y posibilidades que tiene un proveedor para convertirse en proveedor potencial de la organización.</p> <p>Aplicar los criterios para seleccionar los proveedores TI en el registro RC-COM-02 apoyados del procedimiento de gestión de proveedores y compras.</p> <p>Seleccionar los proveedores de servicios TI o distribuidores de partes tecnológicas, que cumplan con el puntaje mínimo (≥ 70 puntos) establecido en la tabla de criterios de selección.</p> <p>Elaborar una base de datos de proveedores TI activos que son aquellos seleccionados a quienes se le van a realizar las compras.</p>	<p>Gestor SI-TI</p> <p>Coordinador SGI</p>	<p>RC-COM-01 Evaluación de Proveedores</p> <p>RC-COM-02 Criterios para selección</p> <p>RC-SIS-53 Contrato de soporte UC</p> <p>RC-SIS-02 Proveedores TI activos</p>

<p>4.2.1 Acuerdos con proveedores de servicios de tecnología de la información (UC)</p> <p>Acordar un contrato de soporte UC con los proveedores de servicios TI que intervengan directamente con la disponibilidad y continuidad de los servicios TI, teniendo en cuenta los siguientes aspectos:</p> <ul style="list-style-type: none"> ▪ El alcance del servicio a prestar ▪ Requisitos a cumplir por el proveedor ▪ El objeto del servicio ▪ Obligaciones contractuales que tiene el proveedor con los subcontratados. (Documentar la obligación con el subcontratado con UC) ▪ Excepciones del contrato y la forma cómo se van a manejar ▪ Autoridades y responsabilidades de las partes. ▪ Información y comunicación entregada por el proveedor ▪ Condiciones comerciales ▪ Actividades y responsabilidades para la finalización del contrato. 	<p>Coordinador TIC</p>	<p>RC-SIS-53 Contrato de soporte UC</p> <p>PR-SGI-03 Auditorías internas</p> <p>RC-CAL- 01 Plan para realizar la auditoria Interna</p> <p>RC-CAL-02 Lista de verificación</p> <p>PR-SIS-11 Gestión de cambios</p> <p>RC-SIS-03 Bitácora de proveedores TI</p>
---	------------------------	---

<p>Monitorear el desempeño del proveedor de servicios TI frente a los requisitos acordados en el UC mediante el seguimiento y medición de los indicadores establecidos en el UC cada seis meses o durante la vigencia del acuerdo.</p> <p>Diligenciar la ficha de seguimiento con los resultados de la medición de los indicadores, analizar el resultado y establecer planes de acción si lo amerita.</p> <p>Realizar seis meses después de firmado el acuerdo, una auditoria interna para verificar el cumplimiento de los requerimientos acordados en el contrato de soporte mediante metodología establecida en el PR-SGI-03 Auditorías Internas.</p> <p>Comunicar por correo electrónico al proveedor del servicio, los resultados obtenidos de la auditoria, en caso de que se reporten no conformidades menores o mayores, el proveedor de servicios deberá establecer las acciones correctivas necesarias.</p> <p>Llevar una bitácora de la gestión de los</p>		
--	--	--

<p>proveedores para registrar las fallas, eventos positivos y los aspectos a mejorar.</p> <p>Nota: Controlar los cambios en los UC mediante el proceso de gestión de cambios.</p>		
<p>4.2.2 Gestionar la compra o adquisición de bienes y servicios</p> <p>Tramitar las compras de acuerdo los lineamientos establecidos en el instructivo IN-COM-05 mecanismo para dar trámite a la adquisición de un bien o servicio, a través de un comité de compras.</p>	<p>Jefe de almacén y compras</p>	<p>IN-COM-05 Mecanismo para dar trámite a la adquisición de un bien o servicio, a través de un comité de compras</p>
<p>4.2.3 Seguimiento a compra o adquisición de los bienes y servicios</p> <p>El jefe de almacén y compras o quien este delegue, para todos los casos deberán recibir todos los bienes, revisando que los elementos relacionados en la factura hayan llegado en buen estado y que cumplan con las especificaciones y condiciones establecidas en la Orden de Compra.</p> <p>En caso de que el material, equipos,</p>	<p>Jefe de almacén y compras</p>	<p>PR-COM-01 Gestión de proveedores y compras</p>

<p>productos y/o servicios; no reúna las especificaciones requeridas, se realizará la devolución y notificación al proveedor. Diligenciar el registro RC-COM-07 “Verificación y Rechazo de suministros”.</p> <p>Ver PR-COM-01 Gestión de proveedores y compras</p>		
<p>4.2.4 Reevaluación de los proveedores TI activos</p> <p>Aplicar al finalizar la vigencia del contrato de soporte, la reevaluación de proveedores para determinar si continua como proveedor activo TI o si este debe ser amonestado o retirado.</p> <p>Enviar al proveedor los resultados obtenidos en la reevaluación.</p>	<p>Gestor SI-TI</p>	<p>RC-COM-09 Criterios para reevaluación de proveedores</p>

8.2.17 Procedimiento Gestión de la Capacidad de los servicios TI y de los sistemas de información

<u>Procedimiento Gestión de la Capacidad de los servicios TI y de los sistemas de información</u>	<u>Código: PR-SIS-20</u>
	<u>Versión:01</u>

1. OBJETO

Este procedimiento tiene como objetivo establecer las disposiciones para asegurar que la organización tiene, en todo momento, la capacidad suficiente para cubrir la demanda acordada, actual y futura, de las necesidades del negocio del cliente.

2. ALCANCE

Aplica a todos los servicios de Tecnología de la Información que la organización ofrece a sus clientes internos.

3. DEFINICIONES Y/O CONVENCIONES

Capacidad: Desempeño máximo que se puede obtener de un elemento de configuración o servicio de TI. Para algunos tipos de CI, la capacidad puede ser el tamaño o el volumen.

Gestión de la capacidad: Proceso responsable de asegurar que la capacidad de los servicios de TI y de los sistemas de información para cumplir con los requerimientos acordados.

Plan de capacidad: Un plan de capacidad se usa para gestionar los recursos requeridos para entregar los Servicios TI. El Plan contiene detalles sobre el uso actual y futuro de los servicios de TI y de sus componentes, así como también situaciones que requieren atención.

Elemento de configuración CI (Configuration Item): Elemento que es necesario controlar con el fin de prestar uno o varios servicios.

Éstos son algunos elementos de configuración CI:

- **Dispositivos de hardware:** como PCs, impresoras, routers, monitores, así como sus componentes: tarjetas de red, teclados, lectores de CDs.
- **Software:** sistemas operativos, aplicaciones, protocolos de red, etc.
- **Documentación:** manuales, acuerdos de niveles de servicio SLA, etc.

Base de Datos de Gestión de la Configuración CMDB: (Configuration Management Data Base), Base de datos utilizada para registrar atributos de los elementos de configuración CI, y las relaciones entre los elementos de configuración durante todo su ciclo de vida del servicio.

Esta base de datos debe incluir:

- Información detallada de cada elemento de configuración
- Interrelaciones entre los diferentes elementos de configuración, como por ejemplo: relaciones “padre-hijo” o Interdependencias tanto lógicas como físicas.

SLA (Service Level Agreement) acuerdo de nivel de servicios: acuerdo documentados entre el proveedor del servicio y el cliente que identifica los servicios y sus objetivos.

NOTA 1 Un acuerdo de nivel de servicio puede también establecerse entre un proveedor del servicio y un suministrador, un grupo interno o un cliente actuando como suministrador.

NOTA 2 Un acuerdo de nivel de servicio puede ser incluido en un contrato u otro tipo de acuerdo documentado.

Nivel de servicio: logro objetivo y medido contra uno o más objetivos de nivel de servicio. Este término se usa a veces de forma informal para referirse al objetivo de nivel de servicio

Desempeño: realizar, ejecutar, cumplir

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1 Planificación de la Capacidad de los sistemas de información y de los servicios TI</p> <p>Implementar y mantener el plan de la Capacidad PC-SIS-11 donde se definen los recursos humanos, técnicos, de información y financieros de acuerdo a los requisitos identificados y acordados con el cliente y/o partes interesadas.</p> <p>El plan de capacidad incluye:</p> <ul style="list-style-type: none"> • Activos /CIs Asociados • % Uso disco duro • %Uso de la memoria RAM • % Uso del CPU promedio 	<p>Gestor del SI-TI</p>	<p>PC-SIS-11 Plan de capacidad de los servicios TI y los sistemas de información</p> <p>PR-SIS-15 Gestión de cambios</p> <p>PR-SIS-16 Planificación, Diseño y Transición de servicios nuevos o modificados</p>

<ul style="list-style-type: none"> • Número de usuarios promedio • Costo estimado • % de crecimiento estimado <p>Nota:</p> <p>*El Gestor SI-TI debe participar en las primeras etapas del desarrollo de un servicio TI nuevo o modificado asegurando que se dispondrá de la capacidad necesaria para prestar el servicio.</p> <p>*Los cambios en el plan de Capacidad se gestionan mediante el proceso de Gestión de Cambios. Ver PR-SIS-15.</p>		
<p>4.1.2 Criterios de aceptación para nuevos sistemas de información</p> <p>Establecer los parámetros de aceptación para sistemas de información nuevos, para sus actualizaciones o nuevas versiones (Geminus, Sistema Uno). Estos deben reunir al menos dos de los siguientes criterios.</p> <ul style="list-style-type: none"> ✓ Compatibilidad ✓ Escalabilidad ✓ Trazabilidad 	<p>Coordinador TIC</p>	<p>RC-SIS-25 Criterios de aceptación de los sistemas de información</p>

<p>Considerar los siguientes controles:</p> <ul style="list-style-type: none"> -Los requisitos de rendimiento y capacidad del sistemas -Los procedimientos de recuperación de errores y reinicio -La preparación y pruebas de los procedimientos operativos de rutina <p>Se realiza una reunión con el gerente general, director operativo, directora administrativa y financiera, Coordinador TIC y el usuario del sistema a adquirir o actualizar según sea el caso, en dicha reunión se establecerá los criterios específicos que se requieren para la aceptación del sistema en cuestión.</p> <p>Se debe tener en cuenta que todo sistema nuevo debe cumplir los siguientes criterios generales que de igual manera serán evaluados en la reunión de aceptación del sistema:</p> <ul style="list-style-type: none"> - Compatibilidad con varios sistemas operativos - Soporte en caso de errores o daños - Impacto en la organización - Costo / beneficio 		
--	--	--

<p>- Solución a la necesidad encontrada</p> <p>Todo sistema de información nuevo o existente al que se le hagan cambios o adiciones significativas debe someterse a un período de prueba de 3 meses, en los cuales se trabaja en paralelo con el sistema antiguo dando así lugar a los ensayos pertinentes sin poner en riesgo la información procesada</p>		
<p>4.3 Monitoreo del uso de la capacidad de los servicios TI</p> <p>Realizar revisiones bimestrales al plan de capacidad de los servicios TI y los sistemas de información para verificar posibles desviaciones, además de analizar e identificar las nuevas proyecciones de capacidad.</p> <p>El comité de Gestión integral en la periodicidad de sus reuniones revisa el estado de la capacidad basado en las siguientes situaciones:</p> <ol style="list-style-type: none"> 1. Desviación de la capacidad real sobre la planificada 2. Incidentes atendidos y solucionados que son causados por capacidad insuficiente. 	<p>Gestor del SI-TI</p> <p>Comité de Gestión Integral</p>	<p>PC-SIS-11 Plan de capacidad de los servicios TI y los sistemas de información</p> <p>RC-DIR-01 Revisiones periódicas por la dirección al Sistema de Gestión Integral</p>

<p>4.3 Ajustes del desempeño de la capacidad</p> <p>Determinar, una vez se ejecute el monitoreo y el análisis de datos, los ajustes al plan de capacidad de los servicios TI y de los sistema de información.</p>	<p>Gestor del SI-TI</p>	<p>PC-SIS-11</p> <p>Plan de capacidad de los servicios TI y los sistemas de información.</p>
--	-------------------------	--

8.2.18 Instructivo Análisis del impacto en el negocio

<u>Instructivo Análisis del impacto en el negocio</u>	<u>Código: IN-DIR-02</u>
	<u>Versión:01</u>

1. OBJETO

Tiene como objetivo principal proporcionar las bases para la implementación y mantenimiento del plan de continuidad del negocio y de los servicios TI, identificar los procesos/servicios TI críticos y los activos que requieren el más alto nivel de protección. Proporcionar información para la identificación de estrategias y alternativas de recuperación.

2. ALCANCE

Este análisis aplica para todos los procesos/servicios catalogados como críticos para la organización

3. DEFINICIONES Y/O CONVENCIONES

Análisis del impacto en el negocio BIA: Tiene como objetivo principal proporcionar al negocio las bases para el plan de continuidad del negocio, identificando los procesos y activos que requieren el más alto nivel de protección. Este análisis proporciona información para la identificación de estrategias y alternativas de recuperación, estableciendo los objetivos de recuperación y el límite de tiempo.

Plan de continuidad del negocio: Son todas las actividades y procedimientos aprobados que hacen posible a una organización responder a un evento en tal

forma que las funciones críticas del negocio continúen sin interrupción o cambio significativo

Continuidad del servicio: Capacidad de gestionar riesgos y eventos que puedan tener un grave impacto en los servicios con el fin de prestar de forma continúa los servicios en los niveles acordados.

Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Interrupción: Acontecimiento ya sea previsto o imprevisto que causa una interrupción negativa no planificada respecto a la entrega de productos y/o servicios.

Procesos críticos: Actividades claves e imprescindibles para el negocio de la organización

Desastre: Cualquier evento que crea inhabilidad en una parte de la organización para proveer sus funciones críticas del negocio por algún periodo de tiempo

Plan de Recuperación: Contienen instrucciones detalladas para la restitución de los servicios a su fase operativa. Conjunto aprobado de actividades y procedimientos los cuales hacen posible a una organización responder a un desastre y reiniciar sus funciones críticas en una condición aceptable, en un marco de tiempo determinado

RPO Punto de Recuperación Objetivo: la cantidad máxima de información que puede ser perdida cuando el Servicio es restaurado tras una interrupción. El Objetivo de Punto de Recuperación se expresa como una longitud de tiempo antes del Fallo. Por ejemplo, un Objetivo de Punto de Recuperación de un día debe ser soportado por Copias de Seguridad diarias, y hasta 24 horas de información pueden ser perdidas. Los Objetivos de Punto de Recuperación para cada Servicio

de TI deberían ser negociados acordados y documentados, y utilizados como Requisitos para el Diseño del Servicio y los Planes de Continuidad de TI.

RTO Tiempo de Recuperación Objetivo: Es el máximo tiempo permitido que un proceso puede estar caído como consecuencia de un efecto catastrófico.

MTPOD (Máximo Periodo de Interrupción Tolerable)

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
<p>4.1 Análisis de criticidad de los procesos:</p> <p>Para determinar la criticidad de un proceso aplicar a todos los procesos de la organización la encuesta que encabeza el RC-DIR-10 Análisis del impacto en el negocio BIA.</p> <p>Para los procesos que respondan afirmativamente a una de las siguientes tres preguntas, aplicar el registro de Análisis del impacto en el negocio BIA.</p> <p>1. Tiene actividades en su proceso que en su concepto éstas puedan interrumpir la prestación normal de un servicio al cliente?</p> <p>2. La interrupción de una actividad que</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>

<p>realiza en su proceso, pueden ocasionar pérdidas económicas a la organización?</p> <p>3. En su concepto las actividades que realiza en su proceso pueden afectar la relación con el cliente</p>		
<p>4.1.1 Determinar los procesos críticos</p> <p>Identificar en cada proceso las actividades que se realizan, asignándole un nivel de prioridad mayor (3) a aquellos actividades que se consideran más críticos y menor prioridad (1) a aquellos que se consideran menos críticos:</p> <ol style="list-style-type: none"> 1. Prioridad Menor 2. Prioridad Medio 3. Prioridad Mayor 	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>
<p>4.1.2 Tipo y nivel de impacto en el negocio por la interrupción del proceso/servicio</p> <p>Calificar el impacto que puede causar una interrupción en el proceso/servicio así:</p> <p>-Regulatorio/Legal: Incluye pérdidas por no presentar reportes financieros o de impuestos en las fechas indicadas, demandas o penalizaciones al incumplir</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>

<p>requerimientos obligatorios en las actividades de la organización.</p> <p>- Financiero: Incluye pérdida de ingresos, pérdida de intereses, costos de pedir dinero prestado para hacer caja, pérdida de ingresos por préstamos no realizados, penalizaciones por no cumplir compromisos contractuales o niveles de servicio y pérdidas de oportunidades durante el tiempo inoperante.</p> <p>-Reputación: Incluye la pérdida de confianza por parte de los clientes, del mercado y de los entes de control, reclamaciones de responsabilidad, clientes insatisfechos por el servicio.</p> <p>Calificar: Ninguno (N), Bajo (B), Medio (M) o Alto (A) para cada tipo de los impactos antes mencionados y para cada uno de ellos una escala de tiempo de interrupción.</p>		
<p>4.1.3 Calculo de pérdidas monetarias para el negocio por la No continuidad del proceso/servicio.</p> <p>Definir, si se cuenta con la información, las posibles pérdidas económicas cuantitativas para cada escala de tiempo de interrupción.</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>

<p>4.1.4 Máximo periodo de interrupción tolerable MTPOD</p> <p>Indicar el tiempo máximo tolerable de recuperación que puede dejar de realizar tal actividad sin que ello cause pérdidas financieras, quejas de los clientes, y/o penalizaciones legales o contractuales.</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>
<p>4.1.5 Identificar tiempo de recuperación objetivo RTO</p> <p>Estimar el tiempo durante el cual un proceso/servicio puede estar sin operar antes de sufrir impactos considerables para la organización.</p> <p>Establecer el tiempo objetivo de Recuperación (RTO) después de una interrupción, mediante el cual la organización activa sus planes de contingencia y recuperación de las actividades críticas para evitar un impacto significativo.</p> <p>Utilizar la siguiente tabla de valoración en la cual se indica la calificación BIA, el tiempo objetivo de recuperación RTO y el valor del BIA.</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>

Tabla de valoración del BIA

Calificación BIA	Tiempo objetivo de recuperación	Valor del BIA
Nivel 1	< 2 horas	Crítica
Nivel 2	< 5 horas	Crítica
Nivel 3	< 8 horas	Medio
Nivel 4	< 12 horas	Medio
Nivel 5	< 16 horas	Medio
Nivel 6	< 24 horas	Bajo

<p>4.1.6 Identificación de punto de recuperación objetivo RPO</p> <p>Estimar el tiempo de información que estaría dispuesto a perder el proceso en horas, en el caso de interrupción del proceso/servicio.</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>
<p>4.1.7 Identificación de los activos críticos y sus prioridades</p> <p>Identificar los activos críticos: procesos, sistemas de información, aplicaciones, activos tecnológicos y documentación necesarios para soportar las actividades</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>

<p>del proceso.</p> <p>Establecer para cada activo los niveles de prioridad así:</p> <p>(1) menor, (2) medio, (3) mayor</p>		
<p>4.1.8 Grupo de trabajo</p> <p>Definir el grupo de trabajo necesario para recuperar los procesos críticos:</p> <p>Nombre</p> <p>Teléfono- extensión</p> <p>Dirección</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>
<p>4.1.9 Clientes y proveedores</p> <p>Definir los clientes y proveedores necesarios para recuperar los procesos/servicios críticos:</p> <p>Nombre</p> <p>Clientes o Proveedor</p> <p>Servicio prestado</p> <p>Teléfono</p> <p>Dirección</p>	<p>Líder del proceso</p>	<p>RC-DIR-10</p> <p>Análisis del impacto en el negocio BIA</p>
<p>4.2 Determinación de los procesos críticos del negocio</p> <p>Registrar en el RC-DIR-11 de acuerdo al análisis BIA, la siguiente información:</p> <ul style="list-style-type: none"> ▪ Las actividades valorados en los niveles 	<p>Comité de emergencias</p>	<p>RC-DIR-11</p> <p>Determinación procesos críticos</p>

<p>1 y 2 "crítico"</p> <ul style="list-style-type: none">▪ EI MTPOD▪ EI RTO▪ EI RPO▪ La identificación de los activos de información críticos y sus niveles de prioridad de recuperación		
---	--	--

8.2.19 Instructivo Análisis de riesgos para la continuidad y disponibilidad de los procesos críticos

<u>Instructivo Análisis de riesgos para la continuidad y disponibilidad de los procesos críticos</u>	<u>Código: IN-SIS-03</u>
	<u>Versión:01</u>

1. OBJETO

Establecer disposiciones para identificar y evaluar los riesgos y proponer opciones de tratamiento a los que están expuestos los procesos críticos de la organización y que por su interrupción no permitan la continuidad del negocio.

2. ALCANCE

Este procedimiento aplica a los servicios TI de los procesos críticos de la organización

Requisito 6.3 de la norma ISO/IEC 20000-1:2011 “Gestión de la continuidad y disponibilidad del servicio”

Dominio 14 de la norma ISO/IEC 27001:2005 “Gestión de la continuidad del negocio”

3. DEFINICIONES Y/O CONVENCIONES

Interrupción: Acontecimiento ya sea previsto o imprevisto que causa una interrupción negativa no planificada respecto a la entrega de productos y/o servicios.

Procesos críticos: Actividades claves e imprescindibles para el negocio de la organización

Riesgo: Efecto de la incertidumbre sobre los objetivos

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Análisis de riesgo: uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Impacto: resultados y consecuencias de que se materialice un riesgo. Consecuencia sobre un activo si se materializa una amenaza

Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo. Es el riesgo que permanece después de que se han implementado contramedidas y controles.

Aceptación de riesgo: decisión de asumir un riesgo

Tratamiento del riesgo: proceso de selección e implementación de medidas para modificar el riesgo

4. DESCRIPCIÓN DEL DOCUMENTO

ACTIVIDADES	RESPONSABLE	DOCUMENTO DE REFERENCIA
4.1 Análisis y evaluación de los riesgos Identificar y analizar las posibles amenazas y vulnerabilidades que podrían ocasionar riesgos de continuidad para la organización,		

<p>con el fin de medir el nivel del riesgo y reducir el impacto que puede provocar un evento de desastre o una interrupción significativa en los servicios.</p> <p>A continuación se detalla la metodología de análisis de riesgos, el cual cubre los aspectos relacionados con:</p> <ul style="list-style-type: none"> ✓ Proceso crítico ✓ Riesgos (vulnerabilidad y control existente) ✓ Probabilidad ✓ Impacto ✓ Valor (Niveles de Riesgo) ✓ Plan de tratamiento (acción, costo y alternativas de control) ✓ Riesgo residual actual ✓ Probabilidad ✓ Impacto ✓ Valor (Niveles de Riesgo) ✓ Riesgo residual futuro 	<p>Líderes de los procesos</p> <p>Coordinador TIC</p> <p>Gerencia General</p> <p>Coordinadora del SGI</p>	<p>RC-SIS-34</p> <p>Identificación, análisis y evaluación de riesgos</p>
<p>4.1.1 Identificación de los procesos críticos y los activos de información.</p> <p>El Líder de cada proceso identifica y analiza las características de su proceso con el fin de determinar su criticidad y los riesgos a que</p>	<p>Líder de proceso</p> <p>Coordinadora SGI</p>	<p>RC-SIS-34</p> <p>Identificación, análisis y evaluación de riesgos</p>

<p>está expuesto el mismo, como resultado del Análisis de Impacto del Negocio (BIA).</p>																										
<p>4.1.2 Probabilidad e impacto</p> <p>Aplicar para la probabilidad tres valores: alta media y baja dependiendo de la posibilidad de ocurrencia del riesgo. Así mismo aplicar tres valores para calificar el impacto que ese riesgo ocasionaría en la organización, así: alto medio y bajo.</p>	<p>Líderes de los procesos</p> <p>Coordinador TIC</p> <p>Gerencia General</p> <p>Coordinadora del SGI</p>																									
<p>4.1.3 Niveles de riesgo</p> <p>Aplicar el siguiente cuadro para valorar el nivel de riesgo, según su probabilidad e impacto, así por ejemplo: una probabilidad alta con un impacto medio, el nivel de riesgo es grave.</p> <table border="1" data-bbox="318 1329 964 1780"> <thead> <tr> <th colspan="2" rowspan="3"></th> <th colspan="3">NIVEL DE RIESGO</th> </tr> <tr> <th colspan="3">PROBABILIDAD</th> </tr> <tr> <th>BAJO</th> <th>MEDIO</th> <th>ALTO</th> </tr> </thead> <tbody> <tr> <th rowspan="3">IMPACTO</th> <th>BAJO</th> <td>LEVE</td> <td>LEVE</td> <td>MODERADO</td> </tr> <tr> <th>MEDIO</th> <td>LEVE</td> <td>MODERADO</td> <td>GRAVE</td> </tr> <tr> <th>ALTO</th> <td>MODERADO</td> <td>GRAVE</td> <td>GRAVE</td> </tr> </tbody> </table>			NIVEL DE RIESGO			PROBABILIDAD			BAJO	MEDIO	ALTO	IMPACTO	BAJO	LEVE	LEVE	MODERADO	MEDIO	LEVE	MODERADO	GRAVE	ALTO	MODERADO	GRAVE	GRAVE	<p>Líderes de los procesos</p> <p>Coordinador TIC</p> <p>Gerencia General</p> <p>Coordinadora del SGI</p>	<p>RC-SIS-34</p> <p>Identificación, análisis y evaluación de riesgos</p>
			NIVEL DE RIESGO																							
			PROBABILIDAD																							
		BAJO	MEDIO	ALTO																						
IMPACTO	BAJO	LEVE	LEVE	MODERADO																						
	MEDIO	LEVE	MODERADO	GRAVE																						
	ALTO	MODERADO	GRAVE	GRAVE																						

<p>Nivel de riesgo Leve: no se necesita mejorar la acción preventiva. Sin embargo se deben considerar soluciones más rentables o mejoras que no supongan una carga económica importante.</p> <p>Se requieren comprobaciones periódicas para asegurar que se mantiene la eficacia de las medidas de control.</p> <p>Nivel de riesgo moderado: se deben hacer esfuerzos para reducir el riesgo, determinando las inversiones precisas. Las medidas para reducir el riesgo deben implantarse en un periodo determinado.</p> <p>Cuando el riesgo moderado está asociado con consecuencias extremadamente dañinas, se precisará una acción posterior para establecer, con más precisión, la probabilidad de daño como base para determinar la necesidad de mejora de las medidas de control.</p> <p>Nivel de riesgo grave: no debe comenzarse el trabajo hasta que se haya reducido el riesgo. Puede que se precisen recursos considerables para controlar el riesgo. Cuando el riesgo corresponda a un trabajo que se está realizando, debe remediarse el problema en un tiempo inferior al de los</p>		
---	--	--

riesgos moderados.		
<p>4.1.4 Plan de acción para el tratamiento de los riesgos</p> <p>Considerar por cada riesgo identificado, analizado y evaluado, las correspondientes vulnerabilidades, los controles existentes y el plan de tratamiento de los riesgos que contempla las acciones que hay que adelantar, el respectivo responsable, los costos que son necesarios aplicar.</p> <p>La gerencia general es la responsable de definir la opción de tratamiento: aceptar, reducir o transferir; la fecha de implementación, el seguimiento al plan de acción y el seguimiento del avance en porcentaje.</p> <p>Evaluar las opciones para el tratamiento de los riesgos de acuerdo a lo siguiente:</p> <p>Reducir: Suprimir las causas del riesgo: activo, amenaza, vulnerabilidad; y mitigarlo mediante controles.</p> <p>Aceptar: Asumir los riesgos de tal manera que se satisfaga la política de la organización y los criterios de aceptación del riesgo</p> <p>Transferir: Cambiar un riesgo a un seguro o un contrato de outsourcing.</p>	<p>Líderes de los procesos</p> <p>Coordinador TIC</p> <p>Gerencia General</p> <p>Coordinadora del SGI</p>	<p>PO-DIR-01 Política de la Gestión Integral</p> <p>PR-SIS-19 Gestión de las Relaciones con el Negocio y Gestión con los proveedores</p> <p>PR-SIS-02 Gestión de activos de información (AI)</p> <p>PR-HUM-01 Vinculación, inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación.</p> <p>PR-SIS-03 Seguridad física y del entorno</p>

<p>Así mismo, para el tratamiento de los riesgos de la seguridad de la información y los servicios TI, la organización ha establecido las siguientes disposiciones:</p> <p>Dominio 5 Política de seguridad de la información: PO-DIR-01 Política de la Gestión Integral</p> <p>Dominio 6 Organización de la seguridad de la información: PR-SIS-19 Gestión de las Relaciones con el Negocio y Gestión con los proveedores</p> <p>Dominio 7:Gestión de activos PR-SIS-02 Gestión de activos de información</p> <p>Dominio 8: Seguridad de los recursos humanos PR-HUM-01 Vinculación, inducción, reinducción, entrenamiento, desempeño, incentivos y desvinculación.</p> <p>Dominio 9: Seguridad física y del entorno PR-SIS-03 Seguridad física y del entorno</p> <p>Dominio 10: Gestión de comunicaciones y operaciones PR-SIS-04 Gestión de comunicaciones y operaciones</p> <p>Dominio 11: Control de acceso PR-SIS-05 Control de acceso a la información</p>		<p>PR-SIS-04 Gestión de comunicaciones y operaciones</p> <p>PR-SIS-05 Control de acceso a la información</p> <p>PR-SIS-06 Adquisición y mantenimiento de sistemas de información</p> <p>PR-SIS-13 Gestión de incidentes de seguridad de la información y de servicios TI</p> <p>PR-DIR-04 Gestión de la Continuidad y Disponibilidad del negocio y de</p>
--	--	---

<p>Dominio 12: Adquisición, desarrollo y mantenimiento de sistemas de información PR-SIS-06 Adquisición y mantenimiento de sistemas de información</p> <p>Dominio 13: Gestión de incidentes de seguridad de la información PR-SIS-13 Gestión Incidentes, Peticiones de servicio y Problemas de la seguridad de la Información y de los Servicios TI</p> <p>Dominio 14: Gestión de la continuidad del negocio PR-DIR-04 Gestión de la Continuidad y Disponibilidad del negocio y de los servicios TI</p> <p>Dominio 15: Cumplimiento PR-SIS-07 Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información.</p>		<p>los servicios TI</p> <p>PR-SIS-07 Cumplimiento de requisitos legales, reglamentarios y contractuales de la seguridad de la información</p> <p>RC-SIS-35 Plan de acción para el tratamiento de los riesgos</p>
<p>4.1.4 Riesgo residual</p> <p>Con base en los resultados del plan de tratamiento, se estiman los riesgos residuales, es decir, el nivel de riesgo restante después del respectivo tratamiento.</p>	<p>Líderes de los procesos</p> <p>Coordinador TIC</p> <p>Gerencia General</p> <p>Coordinadora del SGI</p>	<p>RC-SIS-60</p> <p>Identificación, análisis y evaluación de los riesgos para los procesos críticos</p>

<p>4.1.5 Análisis Post PDA</p> <p>Una vez aplicado el plan de tratamiento y estimado el riesgo residual, volver a analizar los riesgos de los procesos críticos, sus vulnerabilidades, la probabilidad de ocurrencia, el impacto y el riesgo residual futuro</p>	<p>Líderes de los procesos</p> <p>Coordinador TIC</p> <p>Gerencia General</p> <p>Coordinadora del SGI</p>	<p>RC-SIS-60</p> <p>Identificación, análisis y evaluación de los riesgos para los procesos críticos</p>
---	---	---

8.2.20 Política de Gestión de la Seguridad de la Información

<u>Política de Gestión de la Seguridad de la Información</u>	<u>Código: PO-DIR-05</u> <u>Versión:01</u>
---	---

CYFO Comunicaciones y Fibra Óptica CIA S.A. tiene como política de seguridad para el mantenimiento del S.G.S.I., salvaguardar y asegurar la autenticidad de la información sensible y necesaria para la prestación de soluciones integrales a la infraestructura eléctrica y de telecomunicaciones.

Propender por la disponibilidad de los activos tecnológicos y de la información controlando los riesgos de daño, hurto o pérdida; velando también por el cumplimiento de los requisitos del negocio, legales, reglamentarios y contractuales.

Es también nuestra intención generar conciencia en los colaboradores con el propósito de preservar la integridad y confidencialidad de la información.

8.3.3 FO-PRO-09 Registro Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD N° _____ SEGÚN CONTRATO N°

D E C L A R A C I O N E S

I. Declara EL CONTRATANTE por conducto de su representante legal que:

- a) *(Nombre de la empresa)* es una empresa debidamente constituida de conformidad con las leyes de la República de Colombia.
- b) Cuenta con las facultades necesarias para la celebración del presente contrato, mismas que no les han sido revocadas ni modificadas en forma alguna, por lo que se encuentra debidamente facultada para la celebración del presente contrato.

II. Declara EL CONTRATISTA por conducto de su representante legal que:

- a) Su representada es una sociedad debidamente constituida de conformidad con las leyes de la República de Colombia.
- b) Su representante cuenta con las facultades necesarias para la celebración del presente contrato, mismas que no le han sido revocadas ni modificadas en forma alguna, por lo que se encuentra debidamente facultado para la celebración del presente contrato.

III. Declaran las partes por conducto de sus representantes legales que:

1. Desean celebrar el presente **CONTRATO**, cuyo objeto es *(objeto del contrato)*.
2. En virtud de lo anterior, las partes se obligan a guardar la más estricta confidencialidad respecto de la Información a proporcionarse mutuamente.

Conformes que estuvieron Las Partes, convienen en otorgar las siguientes:

CLÁUSULAS

PRIMERA. Las partes en este acto reconocen que en el desarrollo de **EL CONTRATO**, tendrán acceso e intercambiarán entre ellas información confidencial de origen propio o de terceros. Para efectos de este contrato las partes convienen en que “Información Confidencial” significa cualquier información o dato que sea proporcionado por alguna de las partes a la otra parte, incluyendo de manera enunciativa y no limitativa, todos aquellos datos, registros, planos, diseños, estudios, proyectos, programas de computación (software) y conocimientos de naturaleza propietaria, de desarrollo, de mercadotecnia, técnicos, de ventas, de operación, de desempeño, de costos, know-how, de negocios, administrativo, legal, financiero, comercial y de procedimiento, así como todo medio de información que contenga o revele dicha información y técnicas. Así mismo toda información revelada en forma oral será considerada como Información Confidencial, y toda la información que haya recibido la parte receptora con anterioridad a la firma del presente instrumento será considerada como Información Confidencial.

Para proteger la confidencialidad de la Información obtenida o proporcionada, se exigirá a cada una de las partes que tome medidas más severas de las que toma para normalmente proteger la confidencialidad de su propia información de naturaleza similar.

SEGUNDA. Ninguna de las partes estará obligada a revelar a la otra ningún tipo de Información Confidencial, y la revelación de cualquier tipo de Información Confidencial será completamente voluntaria.

Cada una de las partes se obliga a que en ningún momento y por ningún motivo estará facultada para copiar, editar, reproducir por cualquier medio, elaborar extractos, o revelar a cualquier persona, total o parcialmente, dicha Información

Confidencial o cualquier otra que se relacione con las actividades desarrolladas por cada parte, para fines distintos de **EL CONTRATO**.

TERCERA. El objeto del intercambio de Información Confidencial a que se refiere el presente contrato, es mantener confidencial toda la Información de la otra que se pueda obtener de cualquier fuente como resultado de **EL CONTRATO**. Para proteger la confidencialidad de la Información que aquí se menciona, cada una de las partes se obliga a no revelarla o ponerla a disposición de ningún tercero no autorizado expresamente, o a ninguna compañía o empresa; también se obligan las partes a no reproducir, transmitir, ni usar para su propio beneficio o para el beneficio de terceros, dicha Información Confidencial, sin haber primero obtenido el consentimiento por escrito de la otra parte.

CUARTA. Cada una de las partes responderá por cualquier violación a la obligación de confidencialidad pactada en este contrato, ya sea por conducto de sus trabajadores, consultores, u otras personas que contraten, que de manera directa o indirecta tengan acceso a la Información Confidencial. Ninguna de las partes podrá emitir comunicados de prensa u otro tipo de anuncios en relación con **EL CONTRATO**, sin el consentimiento previo y por escrito de la otra parte.

QUINTA. Las Partes manifiestan que no se considerará Información Confidencial bajo lo establecido en este contrato: (i) la información que fuere del dominio público en el momento de la divulgación o se convierta del dominio público sin que se violen las disposiciones de este contrato por cualquiera de las partes; (ii) la información previamente conocida por cualquiera de las partes, siempre que la fuente de dicha información no se encontrara en el momento de divulgarla sujeta a obligaciones de confidencialidad; o (iii) la información a la que tenga acceso cualquiera de las partes proveniente de una fuente distinta a las partes, o un tercero, cuya fuente no se encuentre en el momento de divulgarla sujeta a obligaciones de confidencialidad.

SEXTA. EL CONTRATISTA se obliga a devolver a **EL CONTRATANTE**, toda la Información confidencial, incluyendo en forma enunciativa, pero no limitativa, todos los documentos, materiales, manuales, medios audiovisuales, electrónicos, magnéticos, discos ópticos registros, diseños, programas, planos, especificaciones, u otros materiales tangibles y todas las copias de los mismos que contengan la Información confidencial, que haya sido proporcionada, obtenida o derivada de **EL CONTRATO**, en la fecha de su terminación por cualquier causa o en cualquier otro momento que lo solicite **EL CONTRATANTE**.

Lo anterior se efectuará por parte de **EL CONTRATISTA** mediante solicitud del **CONTRATANTE**, para lo cual **EL CONTRATISTA** certificará por escrito que ha devuelto toda la Información Confidencial, que no conserva copia de la misma y que no ha sido proporcionada o divulgada de manera alguna a terceros o de manera alguna modificada para su uso posterior.

SÉPTIMA. En caso de que cualquiera de las partes reciba un requerimiento u orden de revelar en todo o en parte la Información Confidencial en términos de una orden judicial o de una autoridad administrativa, dicha parte se obliga a: (i) notificar inmediatamente a la otra parte de la existencia, términos y circunstancias de tal requerimiento a fin de que ésta pueda realizar todos los actos que a su derecho convenga, y en la medida de sus posibilidades, tomar todas las medidas necesarias para evitar dicha revelación sin afectar los derechos y obligaciones de la parte que deba hacer la revelación; y (ii) realizar sus mejores esfuerzos para asegurarse de que a la Información Confidencial revelada se le dará un tratamiento confidencial por parte de las autoridades judiciales o administrativas en cuestión.

OCTAVA. Las partes reconocen que la obligación de confidencialidad contemplada en este contrato subsistirá durante el periodo de cinco (5) años siguientes a que **EL CONTRATO** concluya.

NOVENA. Cada parte además reconoce y conviene que en caso de incumplimiento de cualquiera de sus obligaciones o a cualquiera de las disposiciones de este contrato de confidencialidad, la otra parte tendrá derecho a reclamar el resarcimiento y pago de daños y perjuicios causados, además de la reparación del daño mismo, y a resarcir todos los gastos y costos en que la otra parte incurra para obtener el pago de dichos daños y perjuicios, incluyendo en forma enunciativa, pero no limitativa, honorarios de abogados; esto con independencia de las posibles sanciones que se pudieren derivar de dicha violación o amenaza de violación, incluyendo las acciones legales que procedan, por violación a los derechos de propiedad intelectual o industrial, entre otros.

DÉCIMA.- Para todo lo relativo al presente contrato y para todos los efectos legales correspondientes, las Partes señalan como sus domicilios los que aparecen a continuación:

CONTRATANTE:

CONTRATISTA:

DÉCIMA PRIMERA.- Para la interpretación, ejecución y cumplimiento de este contrato, las partes convienen expresamente en someterse a la jurisdicción y competencia de las leyes y tribunales de la República de Colombia, renunciando a cualquier otro fuero que por razón de domicilio presente o futuro llegaren a adquirir, o por cualquier otra causa.

Leído que fue por las partes el presente contrato y por contener los términos y condiciones en que cada una desea obligarse, lo firman y ratifican por duplicado en la ciudad de *(ciudad)* a *(Fecha)*.

EL CONTRATANTE

EL CONTRATISTA

(Nombre del representante legal)

(Nombre del representante legal)

Representante Legal

Representante Legal

(Nombre de la empresa)

(Nombre de la empresa)

NIT:

NIT:

8.3.4 RC-DIR-01 Registro del comité de Seguridad de la información

Figura 9. Registro del comité de Seguridad de la información

COMITÉ DE GESTIÓN INTEGRAL PARA LA REVISIÓN DEL SIS						RC-DIR-01
REVISIONES PERIÓDICAS POR LA DIRECCIÓN AL SISTEMA DE GESTIÓN INTEGRAL						
ACTA N°						
OBJETIVO:						
LUGAR:						
FECHA:						
HORA:						
ASISTENTES:						
ASUNTO:						
PUNTO A TRATAR						
OBJETIVO DE REVISIONES PERIÓDICAS POR LA DIRECCIÓN	ANÁLISIS	DECISIONES Y ACCIONES	TAREAS/COMPROMISOS	FECHA DE ENTREGA	RESPONSABLE	ESTADO
COMPARACIÓN DE LOS RECURSOS Y COMPROMISO DEL PROYECTO Y/O REVISIÓN	ANÁLISIS	DECISIONES Y ACCIONES	TAREAS/COMPROMISOS	FECHA DE ENTREGA	RESPONSABLE	
Seguimiento y control de las actividades y planes de trabajo de los procesos de Seguridad de la Información y de Servicios						
Seguimiento y control de los planes de continuidad y resiliencia de servicios						
Identificación y gestión de riesgos relacionados con la seguridad para el uso de datos						
REVISIÓN LAS APM	ANÁLISIS	DECISIONES Y ACCIONES	TAREAS/COMPROMISOS	FECHA DE ENTREGA	RESPONSABLE	
Seguimiento y control de las acciones APM de sus áreas afines de servicios						
REVISUALIZACIÓN DEL CUERPO Y LAS PARTES INTERESADAS	ANÁLISIS	DECISIONES Y ACCIONES	TAREAS/COMPROMISOS	FECHA DE ENTREGA	RESPONSABLE	
Plan de las actividades y acciones relacionadas con la calidad, integridad de la información y servicios						
Medición de la satisfacción del cliente por parte de personal y la medición anual de la percepción de la satisfacción de los clientes						
REVISIÓN DE LAS ACTIVIDADES	ANÁLISIS	DECISIONES Y ACCIONES	TAREAS/COMPROMISOS	FECHA DE ENTREGA	RESPONSABLE	
Verificar y evaluar de regularidad de las actividades con normas SIS, ISO, ISO						
CAMBIO QUE PUEDE AFECTAR EL SIS Y LOS RECURSOS Y RECOMENDACIONES POR LA DIRECCIÓN	ANÁLISIS	DECISIONES Y ACCIONES	TAREAS/COMPROMISOS	FECHA DE ENTREGA	RESPONSABLE	
Estado de la Política de la Unidad Integral						
Seguimiento y control de los Capítulos Dependientes						
Seguimiento y control de los Capítulos de la Calidad, de Seguridad de la Información y de Servicios						
Control de cambios de la seguridad, las actividades de negocio, la disponibilidad de recursos, las capacidades técnicas y humanas, las condiciones legales y el entorno físico						
Tarjetas, planes y procedimientos que se aplican con el sistema de gestión para mejorar el desempeño y eficacia del SIS						
CONCLUSIONES SOBRE LA ASISTENCIA, COMPARACION Y EFICACIA DEL SIS	ANÁLISIS	DECISIONES Y ACCIONES	TAREAS/COMPROMISOS	FECHA DE ENTREGA	RESPONSABLE	
Conclusión de la revisión por la Dirección						
PROXIMA REVISIÓN						

Fuente: Elaboración propia

8.3.6 Registro RC-HUM-16 Acuerdo de confidencialidad de la información y código de buena conducta

ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN Y CÓDIGO DE BUENA CONDUCTA

De una parte: **LUIS FELIPE RAMIREZ OSSA**, mayor de edad, identificado con la cédula de ciudadanía número **9.868.093**, quien actúa en su calidad de Gerente y por ende en nombre y representación de **CYFO COMUNICACIONES Y FIBRA ÓPTICA CIA S.A.**, sociedad debidamente constituida y existente bajo las leyes de la República de Colombia, tal y como consta en el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio de Dosquebradas que se adjunta como Anexo 1 y quien en adelante y para los efectos del presente acuerdo se denominará **CYFO COMUNICACIONES Y FIBRA ÓPTICA CIA S.A. y/o EL EMPLEADOR** y, de la otra **XXXXX**, mayor de edad, identificado (a) como aparece al pie de su firma, quien actúa en su propio nombre y representación y quien en adelante y para los efectos del presente acuerdo se denominará **EL TRABAJADOR**, han decidido suscribir el presente ACUERDO, el cual hace parte integral del contrato individual de trabajo suscrito entre las partes y se rige por las siguientes cláusulas y lo no previsto en ellas en las disposiciones legales que se encuentren vigentes:

CLAUSULA PRIMERA. Aspectos relativos a las comunicaciones electrónicas

Cualquier comunicación electrónica, telefónica, a través de correo electrónico, la red de área local, Internet o en general, que haga uso de sistemas de propiedad, gestionados o contratados por **EL EMPLEADOR** está considerada como propiedad de **EL EMPLEADOR** Teniendo en cuenta lo anterior, **EL TRABAJADOR** de forma clara y expresa autoriza a que dichas comunicaciones y sus contenidos subyacentes puedan ser monitoreados, grabados, y/o auditados en cualquier momento y sin previa notificación por parte de **EL EMPLEADOR**, sin que ello constituya una violación al artículo 15 de la Constitución Política de Colombia.

EL TRABAJADOR tiene las siguientes responsabilidades:

- Prestar especial atención a la hora de enviar o reenviar información confidencial de la compañía para evitar la distribución de la misma a destinatarios no deseados de forma accidental.
- Hacer uso racional de los recursos de la empresa en las tareas relacionadas con la actividad de la compañía y en el desempeño de su puesto de trabajo
- Adicionalmente, aunque no exclusivamente, queda prohibida la utilización de los sistemas de información de **EL EMPLEADOR** con los siguientes fines:
 - Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet como un todo (esté o no detallada en este Acuerdo sobre Uso de la Información y Código de Buena Conducta). **EL EMPLEADOR** a su discreción, se reserva el derecho de determinar si una conducta en particular viola dichas normas y/o usos aceptables.
 - Participar y apoyar cualquier comunicado que sea ilegal o una violación de cualquier política o estándar de **EL EMPLEADOR**, incluyendo entre otros, aquellos comunicados que sean difamatorios, obscenos, racistas, sexistas o que evidencien tendenciosidad religiosa.
 - Uso sin autorización de contraseñas, propias o de terceros, para conseguir el acceso a la información o conseguir acceso a cualquiera de los sistemas de software, datos privados o comunicaciones de terceros.
 - Usar los sistemas de **EL EMPLEADOR** para interferir el normal desarrollo de la entidad.
 - Utilizar los sistemas de **EL EMPLEADOR** para solicitar o gestionar cualquier negocio o asunto ajeno a los propios de **EL EMPLEADOR**
 - Requerir el apoyo o apoyar asuntos, causas u organizaciones de cualquier tipo en el caso de que tal requerimiento o apoyo sea de naturaleza personal y no pueda considerarse como una mejora en la reputación o en los intereses de **EL EMPLEADOR**
- Realización de actividades fraudulentas de cualquier tipo.

- Usar un servicio o cuenta de **EL EMPLEADOR** para cometer, ayudar o incitar la violación de Copyright, patentes, Trademark, Trade Secret o leyes de propiedad intelectual.
- El uso excesivo para asuntos personales que interfiera en la actividad de la entidad o en la productividad de **EL TRABAJADOR**.
- Usar los sistemas de comunicaciones de **EL EMPLEADOR** a título personal para manifestar partido u opinión sin expresar de manera clara y taxativa que las opiniones expresadas por ese medio son las opiniones de **EL TRABAJADOR** y no las de **EL EMPLEADOR**
- Creación, reenvío, colocación o distribución de mensajes en cadena (Chain Messages) de cualquier tipo.
- Tratar de evitar o alterar los procesos o procedimientos de medida del tiempo, utilización del ancho de banda o cualquier otro método utilizado por **EL EMPLEADOR** para registrar el uso de los productos y servicios.
- Violar la seguridad de los sistemas, sites o hosts sin previa autorización del dueño.
- Está prohibido a los usuarios interferir o tratar de interferir con los servicios de cualquier otro usuario, host o red dentro de Internet (Denial of Service Attacks). Ejemplos de estas actividades prohibidas incluyen sin limitaciones: (a) Envío de cantidades excesivas de datos (como el rebozar con cualquier tipo de tráfico que exceda las normas aceptables en cuanto a tamaño y/o frecuencia) con la intención de sobrecargar los sistemas, llenar los circuitos y/o hacer fallar los hosts; (b) Tratar de atacar o deshabilitar a un usuario, host o site; (c) Uso, distribución o propagación de cualquier programa, script o comando diseñado para interferir con el uso, funcionalidad o conectividad de cualquier usuario, host, sistema o site dentro de Internet (como el propagar vía Email mensajes conteniendo virus, caracteres de control, etc.); (d) El acceso no autorizado a datos, recursos, sistemas o redes, cualquier intento de verificar la existencia de vulnerabilidades, o la violación de medidas de seguridad y autenticación; (e) El monitoreo no autorizado de datos o tráfico de cualquier red o sistema sin la correspondiente

autorización del propietario; (f) La interferencia con el servicio de cualquier usuario, huésped o red, incluyendo, sin limitación alguna mailbombing, flooding y explotación de vulnerabilidades; (g) La falsificación de cualquier encabezado del protocolo TCP/IP o de cualquier información contenida en los encabezados de los correos electrónicos o grupos de noticias.

- Cambiar la información de identidad con el objetivo de hacerse pasar por otra persona o entidad. Sin embargo no está prohibido el uso de alias o remailers anónimos para cualquier propósito legítimo.
- Configurar una página del Web para actuar de manera maliciosa contra los usuarios que la visiten.
- Enviar correo electrónico no solicitado (Unsolicited bulk e-mail, UBE) o Spamming.
- Enviar una cantidad excesiva de mensajes con el objetivo de rebosar una o varias cuentas de Email (Email Bombing).
- **EL EMPLEADOR** será el único árbitro en cuanto a qué constituye una violación de estas disposiciones.

CLÁUSULA SEGUNDA. Aspectos Relativos al uso del Correo Electrónico (Email)

El uso del correo electrónico es generalizado en **EL EMPLEADOR** Un correo electrónico es un documento cuyo uso indebido puede acarrear las mismas consecuencias que el uso indebido de cualquier otro documento escrito.

La utilización del correo electrónico por EL TRABAJADOR ha de seguir las siguientes directrices:

- El correo electrónico pertenece a **EL EMPLEADOR** y no es personal o privado. **EL EMPLEADOR** se reserva el derecho de inspeccionar buzones y puede emplear software para realizar de forma aleatoria esta función.

- El contenido del correo electrónico no será difamatorio o representará discriminación, ataque o amenaza.
- El correo electrónico no contendrá material que pueda ser considerado pornográfico, ofensivo o xenofóbico.
- No se debe usar el correo electrónico para comunicar datos personales que pudieran ser sensibles.
- **EL TRABAJADOR** no debe enviar mensajes personales vía correo electrónico de la empresa.
- Todo correo electrónico enviado a un cliente o proveedor tiene la misma relevancia legal que cualquier otra forma escrita de comunicación. Un contrato comercial se puede establecer mediante el intercambio de correos electrónicos.
- Toda información confidencial contenida en un correo electrónico debe ser identificada como tal por el emisor del mensaje.
- Cualquier uso del correo electrónico que pudiese violar derechos de terceras personas y/o conllevar acciones civiles o penales está prohibido.
- El envío no solicitado de material comercial o publicitario está prohibido.
- Todo texto estándar (avisos legales, etc.) que **EL EMPLEADOR** acompaña al correo electrónico enviado desde sus instalaciones no puede ser eliminado, editado ni alterado total o parcialmente.

CLÁUSULA TERCERA. Sobre los Antivirus

Todos los servidores y computadores tienen instalados programas antivirus.

Se asumirá que todos los programas o datos provenientes del exterior pueden estar infectados con virus y se analizarán antes de ser empleados. Esto es aplicable al correo electrónico, archivos adjuntos, descargas de Internet, disquetes, CD, DVD, Blue Ray, memorias USB, en fin cualquier unidad de almacenamiento externo.

No se abrirá correo electrónico no solicitado proveniente de una persona y compañía desconocidas.

No está permitido desactivar la protección antivirus que está instalada en el computador.

CLÁUSULA CUARTA. Seguimiento y Control

Hay o habrá software en la red corporativa con la siguiente funcionalidad:

- Limitar el acceso externo a las redes instaladas en **EL EMPLEADOR**
- Vigilar el correo electrónico saliente y entrante en cuanto a contenidos inadecuados o comercialmente sensibles.
- Bloquear el acceso a sitios Web que puedan herir la sensibilidad, así como realizar un seguimiento del acceso a Internet de usuarios individuales para prevenir y monitorear el uso no productivo del mismo.
- Tanto los correos electrónicos de entrada y de salida, como el contenido de su buzón de correo, pueden ser auditados en cualquier momento por un miembro autorizado por **EL EMPLEADOR**
- Verificar que la navegación por sitios Web se realice en relación o conexión con el negocio de **EL EMPLEADOR**. Se hará un seguimiento periódico del registro de actividad para comprobar su cumplimiento.

CLÁUSULA QUINTA. PARTES. EL EMPLEADOR y EL TRABAJADOR de forma clara y expresa, mediante la suscripción del presente acuerdo, declaran que la primera de ellas constituye la PARTE REVELADORA de la información sometida a reserva, mientras que la segunda constituye la PARTE RECEPTORA de dicha información confidencial.

CLÁUSULA SEXTA. DECLARACIÓN DEL TRABAJADOR. EL TRABAJADOR de forma clara y expresa, mediante la suscripción del presente acuerdo reconoce y acepta que en ejercicio de la labor que desempeña en **EL EMPLEADOR** tiene y/o

tendrá acceso a información de carácter confidencial, independientemente del medio en el cual se encuentre consignada.

CLÁUSULA SÉPTIMA. INFORMACIÓN CONFIDENCIAL. Para todos los efectos del presente acuerdo se considerará INFORMACIÓN CONFIDENCIAL, entre otras, toda la información de propiedad de **EL EMPLEADOR** y/o licenciada por un tercero a favor de la misma y/o de cualquiera de sus clientes y/o potenciales clientes, como la relacionada con cifras, tarifas, precios, sistemas de información y contabilidad, los comprobantes contables, pagos, planes de negocios y desarrollo, proyecciones, procedimientos, estrategias comerciales y publicitarias, informes de mercadeo, políticas; marcas, patentes, nombres comerciales, diseños industriales, fórmulas y procesos, estén los mismos o no registrados antes las autoridades competentes, procesos industriales, las políticas de ventas y de descuentos; las promociones; los márgenes; el listado de accionistas y sus proporciones; la nómina de personal y el valor de los salarios; las formulaciones; el listado de proveedores y los costos de las materias primas.

PARÁGRAFO 1. Para todos los efectos del presente contrato, la información conservará la calidad de confidencial, independientemente de la forma y/o medio mediante el cual haya sido relevada a **EL TRABAJADOR**, es decir, resulta indiferente si la información ha sido revelada en forma escrita, oral, visual, medio magnético, correo electrónico e internet, o en cualquier otro medio que permita su divulgación

PARÁGRAFO 2. En el momento en que la INFORMACIÓN CONFIDENCIAL sea revelada a **EL TRABAJADOR** o en el momento en que éste tenga acceso a la misma por cualquier medio, **EL EMPLEADOR** no deberá advertir que la información revelada o conocida por **EL TRABAJADOR** es confidencial.

CLÁUSULA OCTAVA. OBLIGACIÓN DE CONFIDENCIALIDAD Y/O RESERVA.
Que durante la vigencia del presente acuerdo, **EL TRABAJADOR** de forma

expresa se obliga a manejar con absoluta confidencialidad y mantener en reserva toda la información de carácter confidencial que obtenga, por haber sido suministrada por **EL EMPLEADOR** o por los demás empleados de ésta, y/o por haber sido obtenida en el ejercicio del contrato individual de trabajo, sea que la información haya sido revelada de forma oral, escrita, en CD, DVD, o en cualquier otro medio que permita su divulgación.

PARÁGRAFO. EL TRABAJADOR sólo podrá revelar y/o divulgar la INFORMACIÓN CONFIDENCIAL si el inmediato superior jerárquico lo ha autorizado de forma, escrita, expresa y previa.

CLÁUSULA NOVENA. OBLIGACIÓN ESPECIAL RESPECTO DEL USO DEL SOFTWARE. EL TRABAJADOR mediante la suscripción del presente acuerdo se obliga a no usar el o los aplicativos o sistemas de software de propiedad de **EL EMPLEADOR** o sobre los cuales ésta tenga licencia para su uso, para fines personales, no comprendidos dentro de sus obligaciones laborales. De igual forma, EL TRABAJADOR no podrá reproducir ni divulgar los programas antes mencionados, así como tampoco podrá revelar las claves asignadas por **EL EMPLEADOR** para acceder a los sistemas de computación.

CLÁUSULA DÉCIMA. SANCIONES PENALES. EL EMPLEADOR de forma expresa mediante la suscripción del presente acuerdo declara que la INFORMACIÓN CONFIDENCIAL que **EL TRABAJADOR** se obliga a mantener en estricta reserva, tiene además carácter de reserva industrial o comercial, como resultado de lo cual el uso, revelación o divulgación de dicha información confidencial conllevará también las sanciones penales establecidas en el artículo 308 del Código Penal y/o las normas que se encuentren vigentes al momento de la ocurrencia de la violación.

CLÁUSULA DÉCIMA PRIMERA. JUSTA CAUSA. La violación por parte de **EL TRABAJADOR** de una cualquiera de las obligaciones contenidas en el presente acuerdo, constituye justa causa para dar por terminado el contrato de trabajo por

parte de **EL EMPLEADOR**, de conformidad con lo previsto en el artículo 62 del Código Sustantivo del Trabajo, en concordancia con lo previsto en los artículos 58 y 60 del mismo ordenamiento jurídico.

CLÁUSULA DÉCIMA SEGUNDA. PRESUNCIÓN. Durante la vigencia del presente acuerdo se presume como violación de las obligaciones previstas en el mismo, cualquier utilización o divulgación de la **INFORMACIÓN CONFIDENCIAL** con la intención de obtener un provecho personal, directa o indirectamente, lo cual incluye la utilización de la información confidencial en la realización de trabajos o la prestación de servicios a personas naturales o jurídicas que desarrollen actividades similares o conexas al objeto social de **EL EMPLEADOR** y que puedan considerarse competencia de ésta. Esta presunción se entiende además sin perjuicio de la obligación de exclusividad que tiene **EL TRABAJADOR**, en virtud del contrato individual de trabajo suscrito entre las partes.

CLÁUSULA DÉCIMA TERCERA. DEVOLUCIÓN INFORMACIÓN CONFIDENCIAL. A la terminación del contrato individual de trabajo, por cualquier causa, **EL TRABAJADOR** deberá devolver a **EL EMPLEADOR** toda la **INFORMACIÓN CONFIDENCIAL**, sin reservarse **EL TRABAJADOR** copia alguna de dicha información.

CLÁUSULA DÉCIMA CUARTA. SANCIÓN. Que cualquier violación de una o varias de las obligaciones que **EL TRABAJADOR** adquiere con la suscripción del presente acuerdo, y sin perjuicio de las sanciones penales a las que haya lugar, generará una pena, la cual equivale a **QUINIENTOS (500) salarios mínimos mensuales vigentes** o **DOSCIENTOS CINCUENTA (250) salarios mensuales** que devengue **EL TRABAJADOR**, lo que resulte más alto. La generación de la pena no limita a **EL TRABAJADOR** en la persecución del cumplimiento de la obligación principal y de la indemnización plena de perjuicios. El incumplimiento del presente acuerdo de confidencialidad será declarado por la empresa a su entera discreción.

Para efectos de hacer efectivo el pago de la pena aquí acordada, el presente documento presta mérito ejecutivo y será exigible sin el procedimiento de la constitución en mora y previo requerimiento judicial.

EL TRABAJADOR mediante la suscripción del presente acuerdo, de forma expresa autoriza a **EL EMPLEADOR** para descontar, deducir y/o compensar el valor de la pena aquí pactada, de los salarios y/o prestaciones pendientes de pago a la fecha de la declaración de incumplimiento.

CLÁUSULA DÉCIMA QUINTA. VIGENCIA. El presente acuerdo rige desde el momento de su suscripción y tendrá una vigencia igual a la duración del contrato individual de trabajo, adicionada en cinco (5) años, contados a partir de la terminación del contrato individual de trabajo suscrito entre las partes.

En constancia de lo anterior, las partes suscriben el presente acuerdo en un (1) ejemplar del mismo tenor literal, el día XX de XXX de 201X.

LUIS FELIPE RAMIREZ OSSA

XXXXXXX

REPRESENTANTE LEGAL

C. C .XXXXX de XXXXX.

**CYFO COMUNICACIONES Y FIBRA
ÓPTICA CIA S.A.**

Colaborador

8.3.7 Registro RC-HUM-25 Roles, responsabilidades y autoridades de SI

Figura 11. Registro Roles, responsabilidades y autoridades de SI.


MATRIZ DE AUTORIDADES Y RESPONSABILIDADES																							RC-HUM-25				
PROCESO CARGO	GERENTE GENERAL	DIRECTOR OPERATIVO	DIRECTORA ADMINISTRATIVO	DIRECTOR COMERCIAL	EJECUTIVO DE CUENTA	COORD. SGI	COORD. DE PROY.	CONTADORA	JEFE DE PERSONAL	JEFE DE TRANSPORTE	JEFE DE SISTEMAS	JEFE DE ALMACÉN Y COMPAS	JEFE DE TALENTO HUMANO	AUXILIAR DE INGENIERIA	SUPERVISOR DE CUADRILLA	ASISTENTE CONTABLE	PROYECTISTA	TÉCNICO DE FO	DEBUJANTE	AUXILIAR DE ALMACÉN	AUXILIAR ADMINISTRA TIVO	TÉCNICO INSTALADOR DEFO	TÉCNICO DE OBRA CIVIL	AYUDANTES	CONDUCTOR ES	AUXILIAR SERVICIOS GENERALES	MENSAJERO
DIR	AR	R	R	R	R	R	R	R	R	R	R	R	R	R	I	I	I	I	I	I	I	I	I	I	I	I	I
PRO	AR	AR	R	R	R	R	R	I	R	R	I	R	I	R	R	I	I	R	I	I	I	I	I	I	I	I	I
SIS	AR	I	I	I	I	R	I	I	I	I	AR	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I
MER	AR	AR	I	AR	AR	R	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I
DS	R	AR	I	I	I	R	R	I	R	I	I	I	I	AR	I	I	I	I	A	I	I	I	I	I	I	I	I
MON	R	AR	I	I	I	R	R	I	R	I	I	I	I	I	I	I	I	R	I	I	I	I	I	I	I	I	I
MAN	R	AR	I	I	I	R	R	I	R	I	I	I	I	I	I	I	I	R	I	I	I	I	I	I	I	I	I
INT	R	AR	I	I	I	R	R	I	R	I	I	I	I	I	I	I	I	R	I	I	I	I	I	I	I	I	I
ASE	R	AR	I	I	I	R	R	I	R	I	I	I	I	I	I	I	I	R	I	I	I	I	I	I	I	I	I
COM	R	AR	I	I	I	R	R	R	R	I	I	AR	I	I	I	I	I	I	I	A	I	I	I	I	I	I	I
ASE	R	AR	I	I	I	R	R	I	R	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I
ADM	AR	R	AR	R	I	R	I	AR	I	I	AR	I	AR	I	I	R	I	I	I	I	AR	I	I	I	I	AR	AR
HUM	R	R	AR	I	I	R	R	R	R	I	I	I	AR	I	I	I	I	I	I	I	I	I	I	I	I	I	I
LOG	R	AR	I	I	I	R	R	R	R	AR	I	I	I	I	I	I	I	I	I	I	I	I	I	I	AR	I	I
MEI	I	I	AR	I	I	R	I	I	I	I	I	I	I	I	I	I	I	I	I	AR	I	I	I	I	I	I	R
CAL	AR	R	R	I	R	AR	R	I	I	R	R	R	R	R	I	I	I	I	I	I	R	I	I	I	I	I	I

Conveniones:
A Autoridad
R Responsabilidad
I Interacción

Fuente: Elaboración propia

8.3.8 Registro RC-MEI-05 Mantenimiento a la Infraestructura Interna









Figura 12. Registro Mantenimiento a la Infraestructura Interna.




	REGISTRO MANTENIMIENTO A LA INFRAESTRUCTURA INTERNA			CÓDIGO: RC-MEI-05
MANTENIMIENTO REALIZADO:				
FECHA:		SERVICIO INTERNO		SERVICIO EXTERNO
OBSERVACIONES:				
EJECUTADO POR:	FIRMA:	REVISADO POR:	FIRMA:	

Fuente: Elaboración Propia

8.3.11 Registro RC-SIS-32 Matriz del nivel de criticidad de los incidentes

Figura 15. Registro Matriz del nivel de criticidad de los incidentes.


MATRIZ CÁLCULO NIVEL DE SEVERIDAD INCIDENTES SI - TI					RC-SIS-32 Versión: 1
DESCRIPCIÓN DEL INCIDENTE	IMPACTO DEL INCIDENTE				**VALOR IMPACTO (Sumatoria I-L-C-P)
	PÉRDIDA DE IMAGEN	LEGAL- CONTRACTUAL	CLIENTES	PÉRDIDAS FINANCIERAS	
					 0
					 0
					 0
					 0
					 0
					 0
					 0
					 0

FÓRMULA	INTERVALO		NIVEL DE SEVERIDAD	DESCRIPCIÓN	TIEMPO DE RESOLUCIÓN
$Vr Max * (1-3/3)$	0	3	 BAJO	Debe ser resuelto, pero su nivel de urgencia es bajo. En este caso, la organización experimenta poco o ningún daño, pero tal incidente es un indicador claro de que alguien o algo está intentando penetrar a los sistemas o encontrar vulnerabilidades que explotar, o fallas puntuales que no interrumpen la prestación de los servicios TI.	En las 48 horas siguientes a la detección
$Vr Max * (1-2/3)$	4	7	 MEDIO	Implica que el daño está ocurriendo a la organización, por lo que se requiere atención inmediata para prevenir que el incidente escale a un nivel crítico. Por ejemplo, ha sido expuesta información de cuentas de usuario que pueden ser utilizadas para realizar un acceso no autorizado o una interrupción de los servicios TI.	En las 12 horas siguientes a la detección
$Vr Max * (1-1/3)$	8	12	 GRAVE	Indica que la organización está corriendo peligro. Por ejemplo, un acceso no autorizado o borrado de la información almacenada en un servidor crítico, una suspensión de los servicios TI. Durante una crisis, todo el tiempo y recursos deben ser destinados a remediar el problema	En la 1 hora siguiente a la detección

Fuente: Elaboración propia

8.3.13 Registro RC-SIS-61 Reporte de vulnerabilidades encontradas


Figura 17. Registro Reporte de vulnerabilidades encontradas.

	PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				CODIGO:
	REPORTE DE VULNERABILIDADES ENCONTRADAS				RC-SIS-61
SISTEMA DE INFORMACION	FECHA	VULNERABILIDAD ENCONTRADA	DESCRIPCION	CRITICIDAD	CONTACTO DE SOPORTE

Fuente: Elaboración propia

8.3.15 Registro RC-SIS-68 Inventario de Sistemas de información.

Figura 19. Registro Inventario de Sistemas de información.

 PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y DE LOS SERVICIOS TI									Código: RC-SIS-68
									Versión: 01
INVENTARIO DE SISTEMAS DE INFORMACION									Fecha: 25-08-2014
NOMBRE	VERSION	PROVEEDOR	DIRECCION	TELEFONOS DE SOPORTE TECNICO	E-MAIL	PERSONA DE CONTACTO	FECHA DE COMPRA	CANTIDAD DELICENCIAS	USUARIOS
Sistema UNO	8.1	SIESA	Calle 7 Nro. 15-37 Pereira	3400540 ext 6316	yennifer.hoyos@siesa.com andres.candela@siesa.com	Yennifer Hoyos Salazar Andres Candela	15/10/2009	Ilimitado local	Claudia Espinosa Valentina Gomez Sandra Ramirez Johana Monsalve
Geminus	2.0	GEMINUS	Edificio Diario del otun Oficina 20-07	3312857- 3104210508	jpineda@geminus.com.co carbelaez@geminus.com.co	John Pineda Carolina Arbelaez	03/08/2010	Ilimitado local	Rodrigo Arenas Alexander Gutierrez Jorge Cardona Catalina Rincon Juan David Aguirre Cardona Claudia Espinosa Norma Lilliana Arias Mauricio Agudelo Luis Felipe Ramirez
Telefonia Siptelco	11	SIPTELCOMUNICACIONES	Carrera 49 # 49-73 Ofic. 1207	3014361066-604991	jueguen@siptelecomunicaciones.com joanramirez@siptelecomunicaciones.com	Johan Ramirez Ramon Jueguen	19/08/2014	Ilimitado local	Todos los colaboradores que tienen telefono fisico y aplicación.

Fuente: Elaboración propia

8.3.16 Registro RC-SIS-69 Concesión y Verificación de acceso a los SI.

Figura 20. Registro Concesión y Verificación de acceso a los SI.

	PROCESO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN						CODIGO:
	CONCESIÓN Y VERIFICACIÓN DE ACCESO A LOS SI						RC-SIS-69
USUARIO	SISTEMA	PRIVILEGIOS					
		Eliminar	Modificar	Crear	Imprimir	Ver	Crear usuarios
Juan David Aguirre Cardona	Geminus	X	X	X	X	X	X
Rodrigo Arenas	Geminus	0	X	X	X	X	0
Cristian Cataño	Geminus	0	X	X	X	X	0
Jorge Cardona	Geminus	0	0	X	0	0	0
Catalina Rincon	Geminus	0	0	0	X	X	0
Cristhiam Pelaez	Geminus	0	0	0	X	X	0
Mary Luz Cardona	Geminus	0	0	0	X	X	0
Alexander Gutierrez	Geminus	0	X	X	X	X	0
Yeison Montoya	Geminus	0	X	X	X	X	0
Carolina Bernate	Geminus	0	X	X	X	X	0
Luis Felipe Ramirez	Geminus	0	0	0	X	X	0
Daniela Ramirez	Sistema UNO	0	X	X	0	X	0
Melissa Gutierrez	Sistema UNO	X	X	X	X	X	X
Valentina Gomez	Sistema UNO	0	X	X	X	X	0
					X	Permitido	
					0	No Permitido	

Fuente: Elaboración propia

9. CONCLUSIONES

De acuerdo al diagnóstico realizado, se evidencia que la organización solo tiene estandarizados un 9% de requisitos de seguridad de la información con base en la norma ISO 27001:2005; enfocados a las fases del planear y verificar, teniendo en cuenta que en la fase del hacer, no se han documentado y estandarizado los controles de seguridad que requieren los activos de información para lograr minimizar los riesgos que puedan afectar los principios de confidencialidad, integridad y disponibilidad.

Aunque la organización tiene la intención de controlar la seguridad de la información de acuerdo al diagnóstico, la fase del “hacer” está al 0% lo que evidencia la falta de documentación para definir el método que se aplicará para el correcto desarrollo, sino que se realiza empíricamente sin tener una base documentada del porqué, del cuándo, del cómo y del quién debe realizarlo.

Se determinan los procedimientos y registros necesarios para controlar los riesgos a los que está expuesta la información y los medios en que estos se almacenan y procesan, considerando que los datos son el activo más importante para la organización y los cuales pueden ser vulnerados tanto por un error humano como por un acto fraudulento que ocasione un impacto negativo para la organización que puede afectar no solo la imagen corporativa sino sus factores económicos.

Se establece guía documental donde se definen los controles necesarios para gestionar los dispositivos móviles y el teletrabajo, la gestión de activos, el control de acceso a la información tanto físico como lógico, los controles criptográficos, la

seguridad en las operaciones, la protección contra el código malicioso, la gestión de las vulnerabilidades técnicas, la gestión de incidentes, las copias de respaldo de la información y el cumplimiento de los requisitos legales., bajo el modelo PHVA con el fin de adoptar buenas prácticas y directrices que minimicen los riesgos, se gestione la seguridad de la información y se tomen acciones cuando se evidencie una vulnerabilidad que afecte la integridad, disponibilidad y confiabilidad de los activos.

10. RECOMENDACIONES

Identificar un método eficaz para controlar y asignar los activos de información de acuerdo a su nivel de criticidad con el fin de dar un tratamiento y protección adecuada.

Realizar análisis periódicos a los riesgos de seguridad de la información con el fin de verificar el nivel de criticidad y velar porque estos sean tratados adecuadamente hasta que su nivel de riesgo pueda ser asumido por el propietario del riesgo.

Establecer un comité de recuperación ante posibles contingencias y que estas responsabilidades y funciones queden documentadas en procedimientos claros para cada uno de los miembros del comité se instruyan del mismo y se pueda asegurar la continuidad de los servicios.

Poner en práctica los procedimientos, instructivos, políticas, planes y registros establecidos para controlar la seguridad de la información.

Certificar el estándar ISO 27001:2005 porque además de propender por la seguridad de la información de la organización, de sus clientes y proveedores, permite mejorar la imagen corporativa y a estar preparados para afrontar los riesgos a que está expuesta la organización.

Extender el SGSI a todos los procesos de la organización para su contribución y aplicación, sin embargo es primordial centrarse en los procesos donde se concentra la mayor parte de las actividades relacionadas con la gestión de la

información, que suelen coincidir con el área de sistemas, donde se da inicio a las directrices para gestionar la seguridad de la información en todas las actividades críticas de la organización

BIBLIOGRAFIA

1. Desarrollo de un modelo de sistema integrado de gestión mediante un enfoque basado en procesos [en línea]. En: XIV Congreso de Ingeniería de Organización, 8 septiembre de 2010. [Consulta: 10 septiembre 2013]. Disponible en internet: http://adingor.es/congresos/web/uploads/cio/cio2010/QUALITY_MANAGEMENT/1555-1564.pdf
2. UNAD. Ciclo PDCA (Edward Deming) [en línea]. En: Universidad Nacional Abierta y a Distancia. [Consulta: 28 noviembre 2013]. Disponible en internet: [http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/21 leccin 6 la organizacin iso y la familia de normas iso.html](http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/21%20leccion%206%20la%20organizacion%20iso%20y%20la%20familia%20de%20normas%20iso.html)
3. MONOGRAFIAS.COM <http://www.monografias.com/trabajos85/seguridad-informacion-realidad-o-utopia/seguridad-informacion-realidad-o-utopia.shtml> [Consulta: 8 junio de 2014].
4. Seguridad Informática. Encarna González. <https://seguinfo.wordpress.com/category/riesgos/page/12/>
5. MONOGRAFIAS.COM. CARHUAMACA, Zereceda David. Seguridad de la información: realidad o utopía [en línea]. En: Monografias.com. [Consulta: 18 febrero de 2014]. Disponible en internet: <http://www.monografias.com/trabajos85/seguridad-informacion-realidad-o-utopia/seguridad-informacion-realidad-o-utopia.shtml#ixzz2yGDI2raR>
6. ISMS FORUM SPAIN. La necesidad de la certificación ISO 27001 acaparó la atención de la 1 jornada de internacional de ISMS Forum Spain [en línea]. En: Asociacion Española para el fomento de la seguridad de la informacion.

[Consulta: 15 enero de 2014]. Disponible en internet:
<http://www.ismsforum.es/noticias/146/conclusiones-de-la-i-jornada-internacional-de-isms-forum-spain/>

7. ANTON, Peregrina Enrique, Seguridad informática: protección de activos lógicos [en línea]. En: Estrategia Financiera.es, Abril de 2005. [Consulta: 31 marzo de 2014]. Disponible en internet:
<http://pdfs.wke.es/6/6/2/4/pd0000016624.pdf>

8. Norma Técnica Colombiana NTC-ISO/IEC 27001:2005