PLAN DE CONTIGENCIA Y CONTINUIDAD DEL NEGOCIO

OBJETIVO: Planificar y describir la capacidad para respuestas rápidas, requerida para el control de emergencias. Paralelo al plan se debe identificar los distintos tipos de riesgos que potencialmente podrían ocurrir, afectando la calidad de servicio que se ofrece a los clientes y partes interesadas, para dar continuidad al negocio.

OBJETIVOS ESPECIFICOS:

- Evaluar, analizar y prevenir los riesgos en la empresa a nivel de prestación del servicio.
- Evitar o mitigar las lesiones que las emergencias puedan ocasionar a los colaboradores y a terceros.
- Evitar o minimizar el impacto de los siniestros sobre la salud y el medio ambiente.
- Reducir o minimizar las pérdidas económicas y daños que puedan ocasionar a nuestra unidad operativa por afectación a su infraestructura.
- Capacitar permanentemente al personal en prevención de riesgos físicos, tecnológicos y entrenamientos en acciones de respuestas ante situaciones de emergencias de desastres.

ALCANCE: Este plan es de cumplimiento de todos los colaboradores de RISKS INTERNATIONAL S.A, S, la empresa, quienes se comprometerán a darle aplicabilidad, para minimizar los riesgos internos y externos, que pueden presentar en la prestación de los servicios y así ofrecer un servicio de calidad a los clientes y partes interesadas, proceso que debe quedar debidamente documentado.

DEFINICIONES:

CLIENTES: Entidad o persona que utiliza los servicios de una empresa

PARTES INTERSADAS EN CALIDAD: Son los clientes, usuarios, socios, colaboradores, proveedores externos, entidades del gobierno.

PROVEEDORES: Alianzas estratégicas que suplen acciones laborales a la empresa.

PERSONAL O COLABORADORES: Hace referencia al personal que se encuentra vinculado en la empresa y realiza los procesos para satisfacer las necesidades de los clientes y partes interesadas.

ERRORES Y OMISIONES: proporciona protección legal ante la responsabilidad en que pudiera incurrir un profesional que cometiera un acto, error u omisión que ocasione una pérdida financiera a un cliente.

SISTEMA DE INFORMACION: Un Sistema Informático utiliza ordenadores para almacenar los datos de una organización y ponerlos a disposición de su personal.

RIESGO: El riesgo es una medida de la incertidumbre

CONTIGENCIA: contingencia es un evento inesperado o una situación que afecta a la salud financiera, la imagen profesional o la cuota del mercado de una empresa.

PLAN DE CONTIGENCIA: Identifica la exposición de la organización a amenazas externas e internas, y sintetiza las medidas a tomar para prevenir y recuperarse de dichas amenazas en caso de producirse por lo que se establece un conjunto de procedimientos alternativos a la operatividad normal de cada institución, basado en un análisis de riesgo.

PLAN DE CONTINUIDAD DE NEGOCIOS: Los planes de continuidad de negocios cubren una serie de situaciones, eventos de crisis que amenazan con cerrar las operaciones del negocio por un período, crisis financiera o evento inesperado que amenace con destruir o dañar la empresa.

MANEJO DE CRISIS: Existen muchos tipos de crisis que pueden afectar el bienestar de una compañía, como las que derivan de desastres naturales, ataques terroristas, incendios en el almacén, lesiones en el trabajo o incluso clientes enojados

MITIGACION: El propósito de la mitigación es la reducción de la vulnerabilidad, es decir la atenuación de los daños potenciales sobre la vida y los bienes causados por un evento o la materialización de un riesgo.

RECUPERACION: Vuelta de una persona o una cosa a su estado normal después de atravesar una situación negativa, de emergencia o vulnerable.

PROBALIBILDAD: La probabilidad es una medida de la incertidumbre asociada a un suceso o evento futuro.

AMENAZA EXOGENA: Aquella originada por actividades ajenas a la construcción y operación del proyecto, sumadas a fenómenos naturales y que pueden llegar a ser perturbadores del medio ambiente y posibles generadores de emergencia.

AMENAZA ENDOGENA: Hace referencia a algo que se origina o nace en el interior, o que se origina en virtud de causas internas.

GOBERNANZA PROYECTIVA: Gobernanza proyectiva, implica los procesos que deben darse en forma eficiente y con calidad para lograr un proyecto exitoso.

PLANIFICACION DE LA RECUPERACION ANTE DESASTRES: Desarrollo de estrategias y planes que soporten la recuperación de los sistemas en caso de una interrupción. Provee la metodología para identificar y mitigar potenciales puntos de fallos.

NO CONFORMIDAD: Queja o reclamo, inconformidad, sobre las causas de un proceso o prestación de un servicio, que presenta falencias o fallas.

MEJORA CONTINUA: A partir de las no conformidades, riesgos que se presentan en la empresa, capacidad e idoneidad para minimizarlos y subsanarlos.

HERRAMIENTA AMFE o AMEF: Se utiliza en la gestión de riesgos y en la planificación de la calidad.

RISKS INTERNATIONAL S.A.S. Establecerá estrategias, procedimientos preventivos y reactivos que permiten minimizar y subsanar cualquier inconveniente que se presente de improviso, en el normal desarrollo de la prestación de servicios de las plataformas en sistemas de información.

METODOLOGIA.

- Realizar análisis de riesgos a través de matrices
- Dotar de los elementos necesarios para la adecuada prestación de los servicios.
- Hacer auditoria internas
- Hacer planes de acción preventivos y de mejoramiento
- Capacitar al personal.

FORMA DE DESARROLLO:

- **Nivel preventivo:** De carácter educativo y se ha destinado a preparar a los colaboradores para el desarrollo de las actividades ya sean directas o indirectas.
- Nivel de atención: Actividades o acciones de intervención directa y oportuna ante la ocurrencia de un evento que afecte el normal desarrollo de la ejecución de las actividades de RISKS INTENATIONAL S.A.S.
- **Nivel de recuperación:** Actividades tendientes a la recuperación del normal desarrollo y superar la o las eventualidades presentadas procurando minimizar la alteración y causar el menor traumatismo a la operación.

El esquema general del plan de contingencias de los sistemas de información, está constituido por fases:

FASE 1. IDENTIFICACION Y REDUCCION DE RIESGOS: Fase de Identificación de Riesgos, busca minimizar las fallas generadas por cualquier caso en contra del normal desarrollo de la prestación de los servicios que ofrece la empresa.

- Análisis de los riesgos a los que está expuesta la organización, su probabilidad de ocurrencia e impacto.
- La vulnerabilidad y criticidad, proporciona una herramienta independiente para medir el grado de exposición de la institución a hechos potencialmente destructivos, priorizándolos para establecer plan operativo, preventivo y correctivo de intervención de estrategias de recuperación y mejora.
- Evaluar y minimizar la probabilidad de que suceda y reduciendo el efecto de la misma, este debe ser revisado y actualizado de forma periódica, de acuerdo a las innovaciones que se establezcan en los servicios que presta la empresa.
- El nivel de riesgo aceptado por una empresa, orienta la asignación de recursos humanos, técnicos y económicos para superarlos.

FASE 2. ESTABLECER MATRIZ DE RIESGOS LEGALES Y MATRIZ DE RIESGO POR AREAS:

Se empleará la Matriz de Riesgos AMFE, que se caracteriza por:

- Carácter preventivo: Donde nos anticiparnos a la ocurrencia del fallo, tenemos la oportunidad de actuar con carácter preventivo ante posibles problemas, identifica y prioriza los sitios críticos y alternativas de solución, evitando una interrupción del servicio y la indisposición o perdida de los clientes

- Sistematización: Con un enfoque estructurado, el AMFE garantiza que todas las posibilidades de fallo se han tenido en cuenta o han sido consideradas.

- Participación: Promueve el trabajo en equipo, además requiere de la puesta en común de los conocimientos de cada una de las áreas afectadas, como matriz legal, determina la normatividad, soporte legal determinados en el Sistema de Gestión de calidad, los no contemplados en la norma, pero que sean reglamentarios aplicables a la empresa, como leyes, resoluciones, instructivos, políticas y darles aplicabilidad a los procedimientos prestablecidos para afrontar de manera oportuna, adecuada y efectiva, ante la eventualidad de incidentes, accidentes y/o estados de emergencias que pudieran ocurrir tanto en las instalaciones, operatividad, negociaciones, de seguridad con los colaboradores

FASE 3. RECUPERACION DE RECURSOS DE CONTIGENCIA Y CONTINUIDAD DEL NEGOCIO: A partir del análisis de la matriz de riesgos, se promueve la continuidad operativa del punto de alta criticidad de acuerdo a los niveles de servicio objetivos previamente definidos, por medio de las siguientes etapas:

A PARTIR DE LA CREACION DE LA POLITICA DE SEGURIDAD, DE ESTABLECER JEFE DE SEGURIDAD DE LA INFORMACION Y DE CREAR EL COMITÉ DE SEGURIDAD DE LA INFORMACION: Identificar los riesgos que se generan o los que se pueden generar, como control preventivos, medidas que se pueden adoptar para reducir las interrupciones del sistema y reducir costos de contingencia, liderado por el Gerente CEO, Subgerente, ubicados en la carrera 43 No 22ª-62 Barrio Quinta paredes.

AMENAZAS PRESENTES: Para la elaboración del presente análisis se tomaron en cuenta las amenazas tanto endógenas como exógenas, estas amenazas se valoran en criterios de probabilidad de ocurrencia y la afectación causada.

De acuerdo con el origen o con las causas que pueden generar las amenazas, se clasifican en: exógenas, cuando provienen del exterior de la organización, que a su vez pueden ser antrópicas o naturales; y endógenas, cuando tienen lugar al interior del proyecto y son provocadas por procesos de operación o técnicas utilizadas.

Para nuestro Plan de contingencia, las valoraciones dadas a los niveles de importancia y gobernabilidad se tomaron de acuerdo a los factores de probabilidad de ocurrencia vs afectación que puedan tener en la organización.

IMPORTANCIA	GOBERNANZA PROYECTIVA
(0-5) teniendo en cuenta que 0 es el nivel menor de importancia y 5 el nivel máximo	(0-5) teniendo en cuenta que 0 es el nivel menor de gobernabilidad y 5 el nivel máximo

TIPO DE AMENAZA	AMENAZAS
Endógenas	*Proceso de Planificación, e implementación del Sistema de Gestión de calidad de la empresa *Proceso de Atención al cliente en la prestación del servicio

	*Incumplimiento de normatividad *Proceso Inadecuados del personal *Recurso humano Calificado y Competente *Inasistencia del personal *Confiabilidad e integridad en la prestación de los servicios *Sabotaje. *Proceso de selección de personal
Exógenas	*Proceso de Catástrofes naturales *Seguridad empresarial
Plan de recuperación	Plan de recuperación

ACTIVIDADES PARA AMENAZAS ENDÓGENAS

PLANIFICACION DEL PLAN DE CONTIGENCIA:

AMENAZA	**PROCESO DE PLANIFICACION**		**RESPUESTA A LA AMENAZA**
Definición de la amenaza: No establecer una adecuada planificación de los procesos de que se implementan para asegurar la prestación de un óptimo servicio en la empresa.	**Objetivo**: Establecer una adecuada planificación en la implementación del sistema de gestión integral de la empresa, que permita minimizar riesgos.		Atender las amenazas a través de planes de mejora continua
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	**ACCION DE MEJORA**
Se planeo y estructuro, el Sistema de gestión de calidad, en el que se contempla lo relacionado a la seguridad de la información y a todos los aspectos importantes para la certificación en la Norma ISO: 9001:2015.	5	5	a. Se dio capacitación en la Norma ISO.9001:2015, por parte de las asesoras externas. b. Se realizó un boletín No Uno complementando la información, sobre la norma, dada por la asesora del Sistema de Calidad. c. Está en proceso la implementación del Sistema de Gestión de Calidad, para lo cual cada colaborador tiene el sistema DRIVE- Gestión de Calidad. donde se encuentra todo el contenido actualizado.
Fomentar un mecanismo de comunicación a los afectados e interesados en la mejora continua, como son los jefes de área de la empresa, que facilite el intercambio de la información o escalamiento del inconveniente, como: *Fallas del internet. *Caídas de plataforma. al Gerente CEO, Subgerente, área	5	5	Se hará la socialización de este Plan de Contingencia y continuidad del negocio a todos los colaboradores, para su conocimiento, por medio de correo y a través del DRIVE Gestión de Calidad y el Área de Calidad en coordinación con el área de Formación de la empresa capacitaran a los colaboradores de la empresa.

de tecnología, para dar respuesta inmediata y efectiva a los clientes.			
Este plan de contingencia, que se activara una vez sea aprobado por la Gerencia CEO y Subgerencia, cuando se presente lo siguiente: *Daños en los equipos de cómputo o el sistema operacional de las plataformas * Caídas de Internet. * Daños eléctricos * Deterioro de las instalaciones.	5	5	Los requerimientos o PQR, quejas de los clientes o partes interesadas, serán resueltos de la siguiente forma: a. Si el colaborador que recibe el requerimiento está en capacidad de resolverlo, lo hace de inmediato. b. Si el requerimiento es por fallas en el sistema, se hace escalamiento al área de tecnología. c. De requerirse autorización especial, se escala a Gerencia CEO y subgerencia. d. Por orden de la Subgerencia, se Planea y se realiza, semestralmente inspección de las instalaciones por parte del Comité de Evacuaciòn y Atenciòn de Emergencias, Seguridad y Salud en el Trabajo y COPASST
Carencia de un comité de Seguridad de la información dirigido por la Gerencia CEO, Subgerencia, Jefe Administrativo y Financiero, Representante Legal, jefes de áreas; quienes serán los responsables de evaluar la naturaleza y el alcance de los daños al sistema, tan pronto como se presente el suceso, diseñando e implementando los procesos y acciones a desarrollar, como estrategias de recuperación rápida. *Estableciendo la causa de la emergencia o la interrupción. *Área afectada por la emergencia, inventariando el estado de los equipos o clientes perdidos. *Estado de la infraestructura física e informática, bajones de energía eléctrica, daño de equipos de cómputo. * Estableciendo el tiempo estimado para restablecer los servicios con normalidad.	5	5	Acta de conformación de comité de crisis ante emergencias, representado por el Gerencia CEO, Subgerencia y un colaborador que ellos designen. a. Existe un procedimiento FSG-004 Procedimiento de gestión de riesgos. b. En la Política de Seguridad de la Información FGE-023, está establecido: Que la Gerencia CEO y Subgerencia, en coordinación con el área tecnológica, participan activamente en la elaboración, prueba, ejecución y de las plataformas y dan respuesta de forma inmediata, ante daños o alteraciones que se presenten.
Establecer mecanismos de protección de datos personales y sensibles, de acuerdo con la	5	5	a. En la Plataforma de la página web de la empresa, encuentra el aviso de privacidad, en

normatividad legal vigente de HABEAS DATA.			cumplimiento de lo previsto en el la Ley 1581 del 2012 (Ley de protección de datos personales) reglamentada parcialmente por el decreto 1377 del 2013 desarrollando los derechos constitucionales de dar conocer, actualizar y rectificar, las informaciones que se hagan sobre ellos; De igual forma se encuentra el Link para para diligenciar los PQR, la autorización física o electrónica b. Política de Clasificación de la información OGE-007 c. Política de Tratamiento de la información OGE-008 d. MGE-002 Manual de procedimiento para el tratamiento y protección de datos personales. e. Registro normativo en la firma sobre la Ley 1581 de 2012, articulo 17 en el decreto 1377 del 2013.Protecciòn de datos personales. f. MGE-004 Manual de Políticas y procedimientos para el tratamiento y protección de datos personales. g. La empresa está registrada en la base de datos de protección de información en la Supe sociedades h. Se realizó el MGE-003 Manual SAGRLAFT g. RGE-001 Reglamento de Protección de datos sensibles. i. Creación de la Política de Seguridad de la información. OGE-023. j. Cuando se hace un contrato se solicita a los clientes y partes interesadas *Autorización para consulta y reporte ante operadores de información. *A las aseguradoras se le solicita copia de la autorización del asegurado.
Desconocimiento de las leyes y decretos de protección de datos personales y sensibles, por parte de los colaboradores	5	5	Estos documentos están socializados al personal a través de: a. DRIVE- GESTION DE CALIDAD b. Correos electrónicos c. Boletín Informativo No 11 Leyes y Decretos de protección de

			datos. d. OGE-021 Capsulas informativas. e. Capacitaciones que se establecerán entre el área de calidad y el área de Formación, donde quedara evidenciado las actas y registro de asistentes.
Sistema de alerta contra fallas en la prestación del servicio, identificando medidas, adoptadas para reducir las interrupciones en la prestación de los servicios de la empresa.	5	5	El procedimiento PSG.004 Procedimiento de gestión de riesgos, establece que cuando se presentan fallas tecnológicas, se hará lo siguiente: a. Cuando se presentan fallas técnicas: Se generan alertas y los responsables de las áreas de inmediato se comunican con el Gerente CEO y Subgerente a través de correo electrónico, WhatsApp. b. Se hace escalonamiento al área de tecnología. c. A través de correo masivo se le informa a los clientes y el tiempo en que se subsanara el evento. d. Superada la emergencia se reactivará el servicio
Establecer procedimientos documentales que establezcan las medidas de seguridad para asegurar la información de los procesos relevantes en la prestación de los servicios que presta la empresa	5	5	Se han realizado las siguientes actividades para proteger la información. a.PSG-001 Procedimiento Control de la información documentada b. Los colaboradores al firmar el contrato de ingreso a la empresa firman un acuerdo de confidencialidad. FGE-005 Acuerdo de confidencialidad empleados y contratistas. c. Al realizarse en contrato con el cliente se firma los contratos se firma los siguientes contratos *FCM-009 Acuerdo Master de confidencialidad y manejo de información sensible DEMO *FCM-010 Acuerdo Master de confidencialidad de la información sensible c. Se estableció IIF-002 Instructivo de Procedimiento para cifrar

			archivos, sistema de clave de archivos anexos para asegurar la información. e. Se realizó un manual de protección de datos el cual se socializo al personal a través de correos y el DRIVE- Gestión de calidad *MGE-002 Manual de Procedimientos para el tratamiento de datos personales d. Aplicabilidad al procedimiento PSG-004 Control de Riesgos
Control de calidad frente a los contratos que se envían a los clientes, a través de la Representante Legal.	5	5	Todos los contratos para la prestación de servicios son: a. Elaborados de acuerdo a parámetros establecidos por la empresa, por los asesores comerciales, Jefe de Gestión de Operaciones de Talento Humano, con copia a la Gerencia CEO y Subgerencia. b. Dicho contrato con tiene los formatos: *FCM-005 Acuerdo de confidencialidad y no divulgación para empleados y contratistas. b. Se le envía al cliente para su firma. c.Se entregan a la representante legal para que lo revise y lo firme. d. Mensualmente el Subgerente revisa los contratos, para verificar tengan toda la documentación requerida. e. Cada seis meses se le solicita la certificación de autorización para consulta y reporte ante operadores de información.
Existe de un archivo documental el cual no cuenta con los controles de seguridad adecuados, generándose el riesgo de pérdida de documentos.	5	5	a. De acuerdo con la Política de Archivo, OGE-019 El archivo documental está ubicado en: *Cajas reglamentarias, *Debidamente rotulado *Bajo llave, que la maneja el Jefe Administrativo y Financiero. b. En las áreas el tiempo que se requiera y luego en el Archivo Documental

Hacer auditorías internas por áreas, a través de simulacros evaluativos, monitoreando las posibles fallas y oportunidad de respuesta. Este debe ser dirigido por los auditores internos capacitados por la empresa, en colaboración con Gestión de Calidad, Gestión documental y jefes de área, quienes informaran los hallazgos a la Gerencia CEO. .	5	5	*Se estableció la importancia de hacer auditorias esporádicas, para lo cual se diseñaron los siguientes formatos para aplicar: a. FSG-007 Plan de Auditoria b.FSG-008 Programa de Auditoria. c.FSG-009 Lista de verificación. d.FSG-010 Informe Auditoria e.FSG-012 Plan de acción auditoria
Incumplimiento con la implementación de las acciones de mejora que se establecieron en el Plan de Acción, después de la auditoria interna.	5	5	Las áreas que, en la auditoria interna, se establecieron observaciones en Mcm, dieron aplicabilidad al formato FSG-011 Acciones correctivas y de mejoras
*Matriz legal de la empresa desactualizada.	5	5	Se realizó la matriz legal de la empresa, la cual se actualizará permanentemente
Procesos de soporte por área, para brindar una adecuada prestación de servicio.	5	5	Las áreas dentro del proceso de Gestión de Calidad establecieron sus cadenas de suministros, caracterizaciones con sus indicadores de gestión, matrices de riesgos, con sus respectivas acciones correctivas y procedimientos, para así blindar un adecuado servicio.
Realizar un plan de acción de mejora que permita minimizar los riesgos que se generen, partiendo de la matriz de riesgos de cada proceso	5	5	a.FSG-012 Plan de Acción de auditorias
Los derechos de petición de se reciben en la empresa, se contestan dentro de los términos legales a los peticionarios.	5	5	A través de la Pagina www.risksisntin.com. Se tiene un Link para que los peticionarios hagan su PQR y la Subgerencia, responde los derechos de petición, dentro de los términos establecidos por la ley
Establecer una infraestructura física segura y adecuada que permita al colaborador trabajar cómodamente, acompañada por los elementos que se requieren para ejercer las labores	5	5	Se realizó cambio de instalaciones el primero de noviembre del 2016 a una casa que ofrece comodidades, iluminación adecuada y bienestar en general para los colaboradores, se adquirió nuevo inmobiliario, sillas ergonómicas

CONTROLES DE SEGURIDAD DE LA INFORMACION

AMENAZA	PROCESO EN ATENCION AL CLIENTE EN LA PRESTACION DEL SERVICIO		ACCION DE MEJORA
Definición de la amenaza: No cumplir los protocolos de seguridad de la información.	**Objetivo**: Generar confianza ante los clientes y partes interesadas por los controles de seguridad que se implementan en la empresa		Desarrollo de acciones de mejora que permitan ofrecer seguridad de la información
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Controles de seguridad de la información	5	5	a. Se realiza análisis de la vulnerabilidad sobre las plataformas tecnológicas y se hacen permanentemente acciones de mejora. b. Se cuenta con sistemas de protección ante software de códigos maliciosos, por lo que se establecerá herramientas de protección antivirus antimalware, antispam, antispyware tanto en los dispositivos de computo. Por lo anterior Deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, cafés internet. c. Los colaboradores usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos d. Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato al área de tecnología. e. Back up, de copia de seguridad de la información: Como mecanismo de prevención ante VULNERABILIDADES e INCIDENTES, La Sugerencia, realiza mensualmente, una copia de seguridad de respaldo de la información, a través del almacenamiento de la misma, por

			medio de discos duros que se guardan externamente, en la casa del Gerente CEO y Subgerente. f. El Área de Tecnología debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro. g. A través del acuerdo de confidencialidad que se la hace firmar a los colaboradores, ellos se comprometen a guardar reserva absoluta de la información dentro de lo cual está inmerso no modificar las configuraciones de seguridad de los dispositivos móviles, que les han asignado para contacto con los clientes y partes interesadas. Por lo que la Subgerencia regularmente has inspecciones a los computadores de la empresa. h. Restricciones a conexiones remotas de los recursos de la plataforma tecnológica de la empresa, únicamente se deben permitir estos accesos a personal autorizado, para el desarrollo de sus labores de la empresa bajo su responsabilidad. Por lo que no se podrá utilizar sus equipos de cómputo para desempeñar las actividades personales. i. PSG-004 Procedimiento de gestión de riesgos, se determina, Protección de datos, hacen parte de los activos de la empresa, los equipos de cómputos impresoras, discos duros y demás elementos de comunicación, la información que se obtiene de las plataformas, que se procesa, almacenada, con carácter confidencial, remitida a los clientes y partes interesadas. Por lo anterior, se le dará buen uso por parte de los colaboradores y estarán bajo la supervisión de los jefes de área, dando aplicabilidad a las políticas de tratamiento de datos, la clasificación de la

			información de acuerdo con los controles requeridos para su protección, Política de comunicación, Manuales y reglamentos de protección de datos y las auditorias de control que se realicen al respecto para la mejora continua.
Carencia de un Oficial de Seguridad de la información.	5	5	La Gerencia CEO y Subgerencia, son comprometidos con los clientes y partes interesadas en la construcción e innovación de plataforma y prestación de servicios con los más altos estándares de calidad, bajo el precepto de prevención de riesgos, a través de: a. Establecer directrices de estándares de seguridad del acceso, manejo de la información, apoyando este proceso con la asignación de recursos adecuados para implementar, mantener las políticas de seguridad de la información, que generen confianza, satisfacción del cliente y las partes interesadas, toda vez que se brinda un servicio confiable, bajo los preceptos normativos. b. Determinar el nivel de protección de la información, estableciendo reglas de entrega de las contraseñas de usuario, entregadas por la Gerencia CEO y Subgerencia, a los colaboradores, la cual se bloquea al usuario, cuando este se encuentra incapacitado o se retira permanentemente de la empresa. Una vez está en proceso de separación de la empresa el área de Administrativo y Financiero, revisará los elementos que entrega y dará un Paz y Salvo, al colaborador, de que los equipos que entregan están en óptimas condiciones. c. Desarrollo de la promoción de las buenas prácticas hacia una activa cultura de seguridad de la información, haciendo monitoreo de consultas; de igual forma, se genera un control de seguridad de la información cuando se registran

			cambios. d. Asignación de responsabilidades de custodia operativas: A través de restricción, controles y análisis de riesgos, para preservar la información de las plataformas, a través del área tecnológica, para que los funcionarios en horas laborales hagan un uso responsable de los servicios y equipos proporcionados por la empresa. e. La información clasificada como reservada o restringida, que genere certificación de confiabilidad de los sistemas de almacenamiento de la información, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio, para lo cual se creó un instructivo acorde al nivel de clasificación de los activos que permite el sistema de cifrado de información para brindarle mayor seguridad, administrando el software o herramienta utilizado para tal fin, la administración de llaves de cifrado. f. La Subgencia, dio la orden explicita a los colaboradores de No almacenar videos, fotografías o información personal. g. Registro y monitoreo de parte de la Gerencia CEO, como coactar del diseño de las plataformas y aplicativos establecerá monitoreo, protección para accesos no autorizados a través de mecanismos de control de acceso lógico, que emitan alarmas de control, al igual ordenará, la aplicación de las buenas prácticas en la utilización de las mismas para la prestación del servicio, evitar accesos no autorizados a los sistemas administrados.

ATENCION A CLIENTES EN LA PRESTACION DEL SERVICIO

AMENAZA	PROCESO EN ATENCION AL CLIENTE EN LA PRESTACION DEL SERVICIO	ACCION DE MEJORA
Definición de la amenaza: No	**Objetivo**: Proporcionar un	Elaboración de instructivo y boletín,

cumplir los protocolos de una buena atención a los clientes y partes interesadas	eficiente y eficaz servicio que satisfaga las necesidades de los clientes y partes interesadas		que determinen las acciones a seguir para una adecuada atención al cliente y partes interesadas
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Falta de capacitación al personal sobre una adecuada atención de los clientes y partes interesadas	5	5	a. Se elaboró el Boletín No 6 atención al cliente, donde se dan parámetros de prestación de servicio eficiente y eficaz, cada colaborador lo tiene impreso en su carpeta de calidad. b. El Gerente CEO y Subgerencia, realiza periódicamente charlas informales, determinando la importancia de una adecuada atención al cliente.
Molestia y queja del cliente porque el asesor o colaborador que corresponda no atienda sus requerimientos.	5	5	a. Existe la orden de la Gerencia CEO, para todos los colaboradores, que cuando no esté el responsable de atender un cliente especifico, este debe ser suplido de inmediato, por otro integrante del área en que se presenta el requerimiento y registrar a través de correo electrónico, que se subsano la inconformidad. b. De ser un requerimiento tecnológico, se escala el evento al área de tecnología. c.La Gerencia CEO, ha realizado capacitación, en atención del cliente y cuando hay quejas, de inmediato realiza los respectivos llamados de atención. d. Se socializo a través del DRIVE-Gestión de Calidad, el Instructivo de atención al cliente. e. Se les entrego el Boletín No 6 atención al cliente y un segundo boletín informativo que se encuentra en DRIVE- GESTION DE CALIDAD.

AREA ADMINISTRATIVA Y FINANCIERA:

AMENAZA	**INCUMPLIMIENTO DE NORMATIVIDAD**		**ACCION DE MEJORA**
Definición de la amenaza: No cumplir con la normatividad y procesos de gestión en el área Administrativa y financiera	**Objetivo**: Reducir riesgos en el Área Administrativa y Financiera, implementando la matriz legal y los procesos que competen a esta área.		Realizar las actividades contempladas en el procedimiento de la Jefatura Administrativa y Financiera
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	

Incumplimiento de la normatividad legal vigente	5	5	Se diseñó la matriz legal de la empresa, la cual el Jefe Administrativo y Financiero debe actualizarla permanentemente.
Incumplimiento del procedimiento del área Administrativa y Financiera	5	5	El jefe del Área Administrativa y Financiera DEBE, darle estricto cumplimiento al Procedimiento que el realizo para su área.
No enviar cuenta de cobro oportunamente	5	5	Se contrató a un profesional como auxiliar de contaduría, quien ayuda en las labores de elaboración de las cuentas al Jefe Administrativo y Financiero. b. Se contrató con la empresa de correos Envía, para enviar las facturas. c. Se reenvía correos electrónicos de recordatorio de pago de facturas.
Perdida de la información del sistema contable por daño o pérdida del computador	5	5	a. Se contrató externamente el sistema contable de la empresa a través de NUBIXAR. b. El jefe administrativo y financiero hace back up mensual y lo guarda en dos memorias una que está en la oficina del colaborador bajo llave y una externamente.
Carencia de un plan de recuperación de cartera vencida	5	5	a. Se realizará un plan de cobro de cartera donde se determinará desde que se recibe la novedad de la cuenta de cobro hasta cuando se actualiza que se ha recibido el dinero. Este proceso está plasmado el PAF-001 Administrativo y Financiera

AREA TALENTO HUMANO:

AMENAZA	PROCESO DE INADECUADOS DEL PERSONAL	ACCION DE MEJORA
Definición de la amenaza: Son las fallas que voluntariamente o de forma involuntaria el personal interviniente en el proyecto de forma directa o indirecta realizan y que puede verse comprometida con el incumplimiento del procedimiento de Talento Humano, donde está establecido el paso a paso para la selección de	**Objetivo**: Dar aplicabilidad al proceso de Talento Humano, garantizando una adecuada selección, contratación e inducción del personal de la empresa	Desarrollar paso a paso de las actividades establecidas en el procedimiento de Talento Humano PTH-001

personal			
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Validación y registro de los documentos en las hojas de vida de los colaboradores	5	5	a. Se elaboró el Formato FTH-001 Listado de personal para registrar los documentos, que los colaboradores aportan como requisito para su hoja de vida. b. Se estableció el formato FTH-017 Chek List de documentación en la hoja de vida. c. Se establecerá una base de datos de datos de posibles candidatos a suplir el retiro o ausencia temporal de un colaborador.
Realización de visita domiciliaria para establecer estado socioeconómico y familiar.	5	5	Se realiza visita Domiciliaria y recolección grafológica, a los colaboradores de la empresa FOT-002
Análisis de riesgos de los colaboradores		5	Se hace análisis reputacional a los aspirantes a ingresan a la empresa
Pruebas de poligrafía periódicas	5	5	Se coordina la realización de la poligrafía como requisito de ingreso, a personal que maneja información sensible. FOT-003 Informe Poligrafía *Se realiza anualmente Poligrafía al personal que maneja información sensible.
Cumplir con la reglamentación de realizar a los colaboradores los exámenes de salud ocupacional de ingreso, periódicos y de retiro	5	5	a. Se envía al aspirante al cargo a Cendiatra a realizar los exámenes pre ingreso, periódicos y de retiro. b. Cuando el colaborador no quiere hacerse los exámenes FAF-012 Paz y salvo b. El comité COPASST en coordinación con el Jefe de Talento Humano, harán el debido seguimiento al ausentismo laboral, e incapacidades medicas.
Proceso de inducción, que le permita a los colaboradores, el manejo adecuado de los procesos y la información que se implementan en la prestación de los servicios que ofrece la empresa.	5	5	La Gerencia CEO y Subgerencia, al igual que el coordinador del Sistema de Seguridad y Salud para el trabajo y jefe de área hacen la inducción del colaborador contratado, registrando documentalmente en el formato FTH-003 Inducción y reinducción al ingreso de personal
Evaluación de desempeñó, para determinar competencias de desempeño	5	5	Se da aplicabilidad al formato FTH-009 de Evaluación de desempeño
Diligenciamiento y firma de pactos de	5	5	Se le hace firmar al momento de la contratación al colaborador un acuerdo

confidencialidad			de confidencialidad, para asegurar que este no divulgue información de clientes, partes interesadas o de la empresa FGE-005 Acuerdo de confidencialidad a contratista y empleados.
Capacitaciones al personal en factores de riesgos, en procesos y temas relacionados con la prestación del servicio	5	1	Existe el formato FTH-006 cronograma de capacitación, el cual se le da cumplimiento. Por lo anterior el Jefe de Talento Humano, coordinara con la ARL Positiva estas capacitaciones.
Registro de las capacitaciones en cumplimiento a las políticas, instructivos establecidos en la empresa	4	5	Se registra la asistencia a las capacitaciones al personal a través del formato FSG-005 Registro de asistencia
Fortalecer el compromiso de responsabilidad de los colaboradores frente al sistema de gestión de calidad de la empresa, frente al servicio que presta y la acciones que desarrolla para cumplir las metas de la empresa	5	5	Acta de compromiso de los colaboradores con el proceso de implementación del sistema de Gestión de calidad. Registrado a través de FSG-005

RECURSO HUMANO CALIFICADO Y COMPETENTE:

AMENAZA	**RECURSO HUMANO CALIFICADO Y COMPETENTE**		**ACCIONES DE MEJORA**
Definición de la amenaza: No contar con el recurso humano, capacitado, calificado, para atender cualquier crisis, con habilidades de detectar los problemas y asumir parcial o toralmente la situación que se presente.	**Objetivo**: Contar desde la selección y capacitación permanente con un personal calificado para la labor a realizar en la empresa		Actividades que fortalezca los procesos formativos de los colaboradores, para que sean competentes en el desarrollo de sus labores.
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Se tiene establecido el mecanismo de requerimiento para ocupar cargos en la empresa	5	5	Se implementará el formato de Requisición de cargos
Se establecen parámetros de selección para perfil de cargos con persona idóneas que puedan responder a las actividades del cargo	5	5	Se implementó el formato FTH-013 Manual y Perfil del cargo, en el cual se contempla su perfil, funciones y compromisos con el Sistema de Gestión de calidad y Sistema de Seguridad y Salud en el trabajo
Proceso de inducción y reinducción de los colaboradores de la empresa	4	4	En el proceso de inducción y reinducción, a los colaboradores se les socializara las Políticas,

			instructivos, manuales y reglamentos de soporte de capacitación para crear conciencia en seguridad de la información, la cual estará en DRIVE-GESTION DE CALIDAD, para ser consultada cuando se requiera.
Programa de capacitación, el cual se va actualizando según las necesidades de capacitación de la empresa y los colaboradores.	5	5	a. La Gerencia CEO y Subgerencia y los jefes de área hacen capacitación a sus colaboradores sobre procesos a implementar en sus áreas. b. Se motiva frecuentemente a los colaboradores para que realicen diplomados sobre Gestión de Riesgos, SARLAFT c. Se envía a los colaboradores a capacitaciones de interés para el desempeño de sus labores.
Se fomenta en los colaboradores la cultura del reporte de quejas y reclamos, para lo cual se les capacita frecuentemente en prevención de riesgos, con el fin que sepan reconocer y reportar amenazas se presenten.	5	5	a. A través de correo y por medio del DRIVE- Gestión de Calidad, se les dio a conocer a los colaboradores el Análisis de contexto DOFA, donde se determina las amenazas y oportunidades de la empresa. b. Está dando aplicabilidad a la Misión donde se determina las buenas prácticas en el mejoramiento continuo, la cultura de la legalidad y la debida diligencia ética, para lo cual los colaboradores son conscientes de la importancia del registro de las quejas y reclamos realizadas por los clientes y partes interesadas, para establecer las mejoras que se requieran. c. Los jefes de área estarán supervisando las actividades e informes de los colaboradores que tienen a su cargo y serán los directos responsables de orientarlos para que desarrollen bien su labor. Por lo anterior cuando se presenta alguna PQR, esta se solucionará de inmediato y se enviara un correo al cliente informando que ya fue subsanada.

CONFIABILIDAD E INTEGRIDAD EN LA PRESTACION DE LOS SERVICIOS Y DE LOS COLABORADORES

AMENAZA	CONFIABILIDAD E INTEGRIDAD EN LA PRESTACION DE LOS SERVICIOS Y COLABORADORES	ACCIONES DE MEJORA

Definición de la amenaza: Fuga de información	Objetivo: A través de actividades concretar minimizar riesgos que afecten la confiabilidad e integridad de los servicios que se presta en la empresa		Actividades de control de fuga de información
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Que se filtre información de los servicios o de la empresa	5	5	a. En el contrato se establece un compromiso de confidencialidad a los colaboradores cuando se firma el contrato, el cual se extiende después de terminado el contrato. FGE-005 Confiabilidad a empleados y contratistas.
Sensibilización hacia una cultura de la legalidad y ética para los colaboradores hacia la empresa	5	5	a. Se creó la Política de Ética OGE-016, la cual está en el DRIVE-Gestión de calidad, Sistema de Gestión de calidad. b. Se elaboró el código de ética y se encuentra socializado a través del DRIVE- Gestión de Calidad. Formato OGE-017 Código de Ética
Establecer acuerdos de confiabilidad y soportes de preservar la confidencialidad	5	5	a. Existe los acuerdos de confidencialidad para clientes y proveedores *FCM-009 Acuerdo Master de confidencialidad y Manejo de información sensible DEMO *FCM-010 Acuerdo Master de confidencialidad *FGE-005 Acuerdo master de confiabilidad empleados y contratistas b. Se realizó el MGE-002 Manual de procedimientos para el tratamiento y Protección de datos personales c. Se realizo el MGE-004 Manual de Políticas y procedimientos para el tratamiento y protección de datos sensibles. d. RGE-001 Reglamento de Protección de datos sensibles. para la consulta y reporte ante operadores de información e. Cuando se realiza un contrato se solicita al cliente, la certificación de autorización para consulta y reporte ante operadores de información; de igual forma el área Unidad Antifraude solicita a sus clientes, copia de la autorización de los asegurados. Ley 1266 del 2008, Ley 1581 del 1012, Decreto 1377 del 2013

TECNOLOGIAS DE LA INFORMACION- SABOTAJE

AMENAZA	SABOTAJE		ACCIONES DE MEJORA
Definición de la amenaza: Sabotaje, por no contar con una Política de Seguridad de Información de la empresa.	Objetivo: Establecer acciones que propender por la preservación y seguridad de la información que se maneja en la información		Actividades preventivas de conservación de la información de la empresa, clientes y partes interesadas
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Diseño procedimientos de gestión de riesgos	5	5	Existe un área de soporte tecnológico, para la empresa, especialmente para las áreas manejan plataformas que han sido diseñadas en la empresa, permitiéndole registrar la información y protegerla de un posible sabotaje a. Área de Gestión de Operaciones en Talento Humano y Análisis de Riesgo: SIVDI Plataforma, Sistemas de información de visitas domiciliarias e investigaciones. b. Área Comercial: SIRIEST, COMPLIANCE c. Área Administrativa y Financiera: Sistema contable NUBIXAR d. Unidad Antifraude: Registra su información DRIVE y SIVDI para asignación de casos. e. Calidad: Sistema Gestión de Calidad tiene la información compartida a través del DRIVE a los colaboradores, de igual forma se maneja el Dropbox f. Gestión de Operaciones en Validación de Proveedores, maneja SIGPRO Sistema de información en gestión de validación de proveedores. g. Se adquirió una planta eléctrica.
Fallas técnicas de las plataformas	5	5	a. Cuando se presenta un Inconveniente con la plataforma, generalmente los clientes por llamada o chat indican que se está presentando fallas b. las comerciales hacen validación de la información del cliente, porque este se puede equivocar en la manipulación del mismo c.De no ser así, se le envía una alerta al área de tecnología que el sistema está generando un error.

Aplicabilidad a la Política de clasificación y protección de la información.	5	5	a. Se estableció como la Política OGE-007 Clasificación de la información en: *Confidencial *Reservado/secreto *Uso interno/Privado *Público b. Se realiza conservación de la información, hacer un back up y ubicación de los datos almacenados, la cual estará en un sitio seguro fuera de las instalaciones de la empresa. c. Se realizan acuerdos de confidencialidad a colaboradores *FGE-005 Acuerdo de confidencialidad a empleados y colaboradores. *FGE-009 Acuerdo Master de confidencialidad y Manejo de información sensible DEMO *FGE-010 Acuerdo Master de confidencialidad para la información sensible.
Aplicabilidad al instructivo IIF-002 Instructivo de Procedimiento para cifrar archivos	5	5	a. Se realizo el instructivo IIF-002 Instructivo de procedimientos para cifrar archivos, como un mecanismo para enviar la información por ser de clasificada como confidencial y que por su evaluación de riesgo sea necesario usar este tipo de control, usando la clave privada previamente establecida con los clientes, lo que garantiza la identidad del emisor y receptor de la información que ha sido generada, procesada, almacenada y transmitida desde sus plataformas tecnológicas. b. La responsabilidad de este procedimiento estará a cargo de los jefes de área sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen su uso es confiable
Permitir el acceso a la información, sin el debido seguimiento de seguridad de la información	5	5	a. Determinar el nivel de protección de la información, estableciendo reglas de entrega de las contraseñas de usuario, entregadas por la Gerencia CEO y Subgerencia, a los colaboradores, la cual se cambia cuando este se encuentra incapacitado o se retira permanentemente de la empresa. Una vez está en proceso de separación de la empresa el área de Administrativo y Financiero, revisará

			los elementos que entrega y dará un Paz y Salvo, al colaborador, de que los equipos que entregan están en óptimas condiciones. b. Los colaboradores, en el acuerdo de confidencialidad que firman, se comprometen a no compartir con nadie sus cuentas de usuario y contraseñas, por lo que serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido, de acuerdo con las políticas establecidas en protección de datos personales y sensibles, generados en la empresa.
Establecer un Plan de actualización de los softwares, el antivirus, previniendo códigos maliciosos	5	5	a. El área Administrativa y Financiera, en su procedimiento, establecerá realizar un cronograma de actualización de las licencias del Softwares y de antivirus, para protección ante software de códigos maliciosos. b. Deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, cafés internet. c. Se realiza mantenimiento a los equipos cuando presentan daños, bajo la supervisión del Jefe Administrativo y Financiero. d. Los colaboradores usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos e. Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato al área de tecnología.
Verificación de las consultas realizadas por los colaboradores a páginas que	5	5	a. Permanentemente el Gerente CEO y Subgerente, ingresa con sus claves a supervisar el trabajo que

no tengan que ver con la labor desarrollada			están desarrollando los colaboradores como mecanismo de validación de la información b. Se estableció un mecanismo de protección de la información para lo cual se diseñó el paso a paso c. La Gerencia CEO y Subgerencias, dispondrá controles que restrinjan el uso de medios de almacenamiento removibles, que impidan copiar información (USB, Unidad CD, disco duro externo), por lo que solo ellos elaborarán una copia de respaldo mensual de información Back up, la cual la realiza la Gerencia CEO, o Subgerencia, esta información será almacenada y guarda fuera de la empresa, donde estará disponible cuando se requiera, con control físico y medioambiental, que cumpla la norma de integridad y disponibilidad.

ACTIVIDADES PARA AMENAZAS EXÓGENAS AL SST

AMENAZA	**CATRASTROFES NATURALES**		**ACCIONES DE MEJORA**
Definición de la amenaza: Eventos naturales, como terremotos, incendios, tormentas eléctricas, vendavales, que puedan afectar las instalaciones de la empresa o a los colaboradores	**Objetivo**: Desarrollar actividades de prevención y atención en desastres, reduzcan riesgos y protejan la integridad de los colaboradores y la información que maneja la empresa.		Actividades que propendan por la implementación del Sistema de Gestión de Seguridad y Salud en el trabajo
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Participación de los colaboradores en los programas de Seguridad y Salud en el trabajo	5	5	Se creó los siguientes comités: a. COPASSTT b. Seguridad y Salud en el trabajo y medioambiental. c.Evacuación y Atención de emergencias d. Comité de Convivencia laboral. e. Comité de Higiene y Seguridad Industrial
Creación de un manual de Atención y Prevención de emergencias	5	5	Se realizó el manual de Evacuación y Atención de emergencias.
Aplicabilidad a la inspección de las estructuras de la	5	5	La presidenta del Comité COPASST, del comité de Seguridad y Salud en el

empresa y equipos para evitar riesgos			trabajo y el presidente o delegado del comité de Atención y Prevención de desastres de la empresa, se encargan de hacer una inspección semestral de las instalaciones de la empresa, cuyo reporte se entregará a la Gerencia CEO, Subgerencia. Lo anterior permitirá problemas estructurales y hacer FAF-009 Hoja de inspección de seguridad e instalaciones y equipos. Por orden de la Subgerencia se hará semestralmente.
Socialización del plan de evacuación y atención de emergencias, por parte de los colaboradores	5	5	Se diseñó un plan de evacuación de emergencias IGE-001, donde se establece: a. Un Plano de ubicación de las áreas y rutas de evacuación de la empresa, dispuesto en un sitio estratégico y visible. b. Teléfonos de emergencia. Dicho plan se dio a conocer a través de un correo electrónico que se les envió a todos los colaboradores y se encuentra en el DRIVE- Sistema de Gestión de calidad. c. En la inducción se da información sobre los temas de Seguridad y Salud en el trabajo.
Implementar dispositivos de alarma ante una emergencia	5	5	a. Se dispuso de un dispositivo de alerta como una alarma- timbre y una alarma que está en el área del lavadero de la casa con dispositivo para que sea escuchada por todos los colaboradores b. Se colocó un botón de pánico en que permite al personal del área comercial activarlo en caso de emergencia.
Disponer de todos los elementos de supervivencia, para hacer simulacros, periódicamente.	5	5	Se realiza permanentemente la solicitud de los elementos que se requieren para implementar el Sistema de Seguridad y Salud en el trabajo FAF-016 Pedido elementos de SST
Capacitación en condiciones de seguridad y atención de emergencias, por parte de los colaboradores.	5	5	Se realiza capacitación a los colaboradores en temas como: a. Se realizo y entrego el Plan de Evacuación y Atención de desastres b. Primeros Auxilios. c. Manejo de extintores d. Condiciones de Seguridad vial

			e. Condiciones de Seguridad personal f. Política OGE-010 Política de Seguridad Vial. g. Se colocaron los Planos de evacuación en diferentes sitios y se entregó a los colaboradores h. Se realizó el Boletín de Seguridad No 5 i. Se harán capsulas informativas, las cuales se enviarán por correo, se subirán al DRIVE- GESTION DE CALIDAD y se le dará impresas.
Establecer un centro alterno de operación especifico por áreas, para que laboren en caso que en las instalaciones principales, no permita el ingreso por razones físicas y técnicas.	5	5	La Gerencia CEO, dispuso que el personal podrá trabajar en las casas con sus computadores en caso de que se presente una emergencia, labor que estará controlada.
Diseñar instructivos de saneamiento básico	5	4	Se crearon instructivos: IGE-001 a. Manejo de residuos b. Importancia de lavarse las manos c. Política Medio-Ambiental, donde se dan parámetros *Para la separación de residuos de la fuente. *Racionamiento de agua *Uso racional de la energía *Cuidado de las plantas ornamentales *Se colocó sitio ecológico para reciclar botellas, pilas y tapas *Se compraron las canecas reglamentarias, para separar los residuos, papel y vidrio
Planear el presupuesto para compras de elementos que contribuya al desarrollo de acciones de felicidad organizacional.	5	4	a. Mensualmente el área Administrativa y Financiera elabora un Adecuación de instalaciones para genera bienestar b. Adquisición de elementos como mouse ortopédico a quienes lo han solicitado. c. Se compró de sillas ergonómicas. d. Se implementó el programa de Felicidad Organizacional, para lo cual se diseñó un cronograma de actividades que propender por generar motivación y sentido de pertenencia con el personal de colaboradores de la empresa para lo cual se hace lo siguiente: * Seleccionar e incentivar el personaje del mes

			* Celebrar los cumpleaños de los colaboradores en su día * Encuentros deportivos *Se adquirió un parques y una mesa de Juego de Ping Pong, para que los colaboradores se recreen en los descansos. * Desayunos y almuerzos de compañeros en restaurante, ofrecidos por la Gerencia Ceo y Subgerencia. * Dotación elementos de trabajo * Dotación de vestuario * Permisos para cursar estudios universitarios *Celebración de fechas especiales *Adecuación de las instalaciones *Regalos para los niños en navidad *Celebración de novenas navideñas *Asados de integración

SEGURIDAD EMPRESARIAL

AMENAZA	**SEGURIDAD EMPRESARIAL**		**ACCIONES DE MEJORA**
Definición de la amenaza: Actividades realizadas por personas internas o externas tendientes a perturbar las actividades.	**Objetivo**: Implementar acciones que permitan a la empresa, minimizar los riesgos en seguridad de las instalaciones y asegurar la información, ante sabotaje que una persona interna o externa de la empresa quiera realizar, afectando la continuidad de negocio		Acciones tendientes a mejorar la seguridad de la empresa
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Aplicabilidad a los sistemas de seguridad en la empresa	5	5	Se utiliza sistemas de seguridad, para prevenir robos y atracos: a. Control de acceso físico, por medio de llaves eléctricas, para acceder a las dos puertas principales de la empresa. b. Identificación y registro de visitantes. c. Se establece como normatividad portar el carné de la empresa al ingresar a la empresa y durante el tiempo de dure la jornada laboral d. Cámaras y circuito cerrado de televisión e. Malla eléctrica f. Sensor de movimiento
Prevenir el acceso no	5	5	Aislamiento y control de acceso zonas seguras de las áreas

autorizado a ciertas áreas de la empresa			restringidas a través de un letrero, que indica solicitar autorización para ingresar, con archivos controlados bajo llave.
Entrega de claves para los celulares corporativos, en el desempeño de las labores.	5	5	Se creó un instructivo IGE-001 Entrega y uso de celulares corporativos
Disponer de lugares físicos con llaves de seguridad para archivo de información confidencial.	5	5	Instructivo numero OGE-001 Manejo y control de llaves eléctricas y manuales, cerraduras y CCTV
Falta de información sobre los teléfonos de emergencia, con las autoridades locales, cuadrante Policía Nacional, a los colaboradores	5	5	Cada colaborador tiene en su carpeta los teléfonos de contacto con las autoridades locales y de socorro

FASE 4. REORGANIZACION Y EL PLAN DE RECUPERACION Y CONTINUIDAD OPERATIVO DEL NEGOCIO:

AMENAZA	**PLAN DE RECUPERACION**		**ACCIONES DE MEJORA**
Definición de la amenaza: Permitir que factores internos y externos afecten el buen desarrollo de las operaciones en la prestación de servicio de la empresa, por no haber implementados acciones preventivas y correctivas a tiempo	**Objetivo**: Fortalecer los procesos que permitan tener continuidad de negocio en la empresa, a través de planificación, inducción, capacitación, auditorias de simulacro, y acciones correctivas y de mejora continua.		Actividades internas y externas que permitan superar las No conformidades
Acciones	**Valoración**		
	Importancia	**Gobernabilidad**	
Fallas tecnológicas en la prestación del servicio	5	5	a. Una vez se presente una falla técnica que afecte el servicio, se generan alertas y los responsables de área, de inmediato se comunicaran vía telefónica, o a través de WhatsApp o la Gerencia CEO, y Subgerente. b. Se hará escalonamiento al área tecnológica, quien de inmediato se dispone a subsanar la falencia. c.A través de correo masivo, informara la novedad a los clientes y el tiempo en subsanarse. d. Superada la emergencia, se

			reactivará el servicio. **PSG-004 Procedimiento de gestión de riesgos**
Registro documental de las fallas tecnológicas y procedimientos realizados de control para no repetición	5	5	Se elaboró el PSG-005 Procedimiento de mejora, No conformidad y Acción correctiva, donde se establece los registros: a. Los responsables del registro b. La No conformidad y sus, causas c.Acciones correctivas y de mejora implementadas. Por lo anterior se dará aplicabilidad al formato
Capacitación permanente con los colaboradores actuales y los que ingresen posteriormente.	5	5	a. En el proceso de inducción a los colaboradores, para el manejo de las plataformas y alternativas de solución ante emergencias, actividades que quedan registradas en el Formato FTH-003 Inducción e inducción al personal. b. En coordinación con Formación de la empresa se socializará los temas de calidad y demás temas de relevancia para la empresa.
Implementación de un sistema de auditoria interna, que permita el mejoramiento continuo y la prevención de riesgos.	5	5	*Se planeó realizar semestralmente auditorías internas. *Se contrató un auditor externo quien realizara la primera auditoria interna, así: a. Previa selección de auditores internos. b. Capacitaron de los mismos. c. Se establece Plan de auditoria, con objetivos de la auditoria.FSG-007 d. Se determina la metodología, lista de verificación, por parte de los auditores internos de la empresa. e. Determinar acciones correctivas y preventivas. f.Se realizará un informe a la Gerencia CEO

			g. Se realizó FSG-012 Plan de acción de Auditorias, para subsanar las No conformidades. h. Registro documental de la auditoria que queda a disposición de los colaboradores, Gerencia CEO, Subgerencia y entes de auditoria externa, a través de correo y DRIVE Gestión de Calidad I. Se aplicará el formato FSG-011 Acción correctivas y de mejora.
Revisión periódica por parte de la Gerencia CEO, en los procesos de Gestión de Calidad de la empresa.	5	5	* Planeación y diseño de Políticas, Instructivos y reglamentos que sean necesarios para el buen funcionamiento de la empresa. *Revisión periódica del Sistema de Gestión de calidad de la empresa, así: a. Evaluación del cumplimiento de los indicadores de gestión de las áreas y sus procesos. b. Encuesta de satisfacción de las necesidades de los clientes y partes interesadas, se hace a través de un Link una vez se envía el informe y la Gerencia CEO, hace una masiva cada seis meses c. Revisión de las no conformidades que se generan por área, así: * Verificación del registro documental de las No conformidades, quejas y reclamos, analizando las causas, estableciendo la necesidad acciones correctivas de mejora que se hayan implementado. *Disposición de recursos que se requirieran para suplirlas.

			d. Disposición de orden y verificación que los jefes de área tengan al día, las carpetas de los clientes, proveedores, con las que se hagan alianzas estratégicas para que tengan toda la documentación de los requisitos pertinentes. e. Registro documental de los resultados de las revisiones realizadas por la dirección estratégica y de las oportunidades de mejora, así: * Innovar con nuevos servicios o mejoras a través de cambios en las plataformas existentes para cumplir las expectativa y requisitos prestablecidos por los clientes y partes interesadas, lo cual se verá reflejado en la fidelización de los mismos. *Mejora permanente del Sistema de Gestión de calidad y el Sistema de Gestión de la Seguridad y Salud en el trabajo y medioambiental, para: * Satisfacción de los colaboradores con su labor y su trabajo se vea reflejado en un servicio de calidad. * Compromiso empresarial con el medio ambiente, los derechos humanos y la sociedad en general.

MARIANO SANCHEZ ABRIL
Gerente CEO
Fecha: 31 Mayo del 2017