FND	GESTIÓN INTEGRAL ORGANIZACIONAL	CODIGO: GIO-MR-07
		Versión: 2
	FORMATO MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL	FECHA: 23/05/2022

N°	CAUSAS DESCRIPCIÓN DE LA CAUSA (Debido a.....)	RIESGO	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DESCRIPCIÓN DE LA CONSECUENCIA (Lo que genera.....)	CLASE DE RIESGO	RIESGO INHERENTE				CONTROLES EXISTENTES							RIESGO RESIDUAL				OPCIONES DE MANEJO	PLAN DE MANEJO DEL RIESGO							INDICADOR PARA LA EVALUACIÓN DE ACCIONES IMPLEMENTADAS	SEGUIMIENTO ENERO -ABRIL-GTE	SEGUIMIENTO MAYO -AGOSTO - GTE	MONITOREO Y REVISION OFICINA CONTROL INTERNO	
						PROBABILIDAD	IMPACTO	NIVEL	VALOR	DESCRIPCION	TIPO DE CONTROL: TIPO DE CONTROL	TIPO DE CONTROL: DOCUMENTO	D O	AP	CE	EV	PUNTAJE (DO+AP+CE+EV)	PROBABILIDAD	IMPACTO	NIVEL	VALOR		CONTROL PROPUESTO O ACCIONES A TOMAR	TIPO DE CONTROL: TIPO DE CONTROL	TIPO DE CONTROL: DOCUMENTO	RESPONSABLE: CARGO	RESPONSABLE: DEPENDENCIA	FECHA DE IMPLEMENTACION ACCIONES: INICIA	FECHA DE IMPLEMENTACION ACCIONES: TERMINA				FECHA	ACCIONES REALIZADAS
1	1. Desactualización de los aplicativos internos (orfeo, syman) 2.Ausencia de mecanismos de control tanto del operador como de la FND. 3. repositorio de la información. 4. Incumplimiento a las políticas de seguridad de la información 5. Falta de mecanismos de control.	Posibilidad de perdida reputacional por pérdida de bases de datos y fuentes de información	No ejecutar el debido respaldo de toda la información y no contar con la protección de ésta.	1.Perdida de autenticidad en la información que se maneja 2.Perder la continuidad en el buen funcionamiento de las areas. 3.Demora en la entrega de información a organismos de control 4.Perdida de recursos 5. Pérdida de información financiera por inexistencia de parametros de seguridad por parte de la Gerencia de Tecnología. 6. Posibles hallazgos 7. Materialización de riesgos. 8. Toma de decisiones erradas	TECNOLOGICO	5	5	25	15	Extrema	1. Copias de seguridad alojadas en Drive 2. Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND	Preventivo		25	25	25	25	100	0	0	1	5	5	15	Alta	evitar	1. Copias de seguridad alojadas en Drive 2. Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND	Preventivo		GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	1. Copias de seguridad de la información. 2. Con la implementacion del Gestor de documentos electronicos de archivo AZ DIGITAL se garantiza la trazabilidad de los documentos, integridad, confidencialidad y disponibilidad de la informacion. 3. Asistencia a capacitaciones: Tansformacion Digital, Analisis de Datos. **Evidencia:** https://drive.google.com/drive/folders/1UYjE7fSdFILc9uxMdGSBHPvUTaSVR0JY	**22/09/2022**	**revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que e riesgo residual sigue siendo ALTO.**
2	1. Fallas en la autenticacion de usuarios 2.Falta de mecanismos de control (LOGIN,ROL, CONTRASEÑAS, ROLES) 3,. Capacitación	Posibilidad de perdida de integridad por ausencia de controles en los sistemas de información	1. Manejar información restringida. 2. Acceder a perfiles no autorizados.	1. Manipulacion de las cuentas . 2 . Perdida de información 3. Perdida de credibilidad 4. posibles hallazgos de entes de control 5. pérdida de contraseñas 6. Exposición de información clasificada o reservada de la entidad	TECNOLOGICO	4	3	12	43	Alta	1. Claves unicas para trabajadores. 2. Manejo de información por areas o procesos. 3. Actualizaciones y cambios periodicos de las contraseñas	Preventivo		23	25	25	25	98	2	0	1	3	3	13	Moderado	Reducir	1. Claves unicas para trabajadores. 2. Manejo de información por areas o procesos. 3. Actualizaciones y cambios periodicos de las contraseñas	Preventivo		GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	4. Con la implementacion del Directorio Activo y el Procedimiento de Control de Acceso se diferenciaron politicas de contraseñas para usuarios, periodicidad de tiempo para cambiarla (cada 60 dias). 5. El sistema de AZ DIGITAL está encriptado con el Hash SHA-256 y cada usuario ingresa con el nombre de usuario y contraseña con la que se ingresa al equipo de la PND y los usuarios son inactivados por directorio activo cuando se retiran o cambian de cargo. 6. El acceso a la informacion en cada sistema de Informacion esta definido por roles, permisos de usuarios Evidencia: https://drive.google.com/drive/folders/1UYjE7fSdFILc9uxMdGSBHPvUTaSVR0JY	**22/09/2022**	**1. Los controles propuestos para bajar la valoración del riesgo residual con los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Alta, y con los mismos controles la valoración es moderado (riesgo residual).** **2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos,**
3	1. Hacking de la informacion privilegiada 2. Desconfiguracion de las plataformas con informacion 3. Falta de mecanismos controles 4.Falta de roles definidos 5. Ausencia de mecanismos de control	Manipulación, modificacion o alteracion sin autorizacion de la informacion registrada en los sistemas de la FND	1. Manejar información restringida. 2. Acceder a perfiles no autorizados.	1. Perdida de informacion 2.Posibles sanciones por no reportar informacion y 3. Uso inadecuado de la información 4. Pérdida de credibilidad 5. Hallazgos de entes de control.	TECNOLOGICO	4	4	16	44	Extrema	1.Actualizaciones 2.Cambios periodicos de contraseñas 3. Capacitar a los funcionarios para la solicitud de requerimientos	Preventivo		25	25	25	25	100	2	0	1	4	4	14	Alta	Evitar	1.Actualizaciones 2.Cambios periodicos de contraseñas 3. Capacitar a los funcionarios para la solicitud de requerimientos	Preventivo		GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	6. Políticas implementadas en el directorio Activo y procedimiento de Control de Acceso: - Contraseñas Seguras (Mayusculas, minuscules, numeros, simbolo alfanumericos) - Solicitud de Cambio de contraseña: Cada 60 dias - Usuarios: NOMBRE.APELLIDO 7.Clausulas de confidencialidad de la información en los contratos de proveedores.	**22/09/2022**	**1. Los controles propuestos para bajar la valoración del riesgo residual con los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Extrema, y con los mismos controles la valoración es Alta(riesgo residual).** **2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos,**
4	1. Desconocimiento normativo vigente sobre plataforma tecnologica y comunicaciones. 2.Incumplimiento de los lineamientos en materia de la gestión plataformas tecnológica y comunicaciones. 3. falta de supervisión 4. Alta rotación de personal 5. Capacitación	Errones gestión de la infraestructura tecnológica de la FND	Gestionar y los distintos procesos de infraestructura tecnologica de la FND y sus activos.	1. Fallas en la conectividad de los sistemas de información tanto interno como externo. 2. Fallas en la conectividad, página Web, correo electrónico y demas sistemas de comunicacion. 3. perdida de recursos 4. Posibles sanciones de organismos de control, CGN, DIAN 5. Perdida de credibilidad 6. Posibles Hallazgos entes de control	TECNOLOGICO	4	3	12	43	Alta	1.Actualizacion y mantenimiento de las herramientas. 2.Mantenimiento de los activos de la FND y los proveedores.	Preventivo		20	20	20	20	80	2	0	2	3	6	23	Moderado	Evitar	1.Actualizacion y mantenimiento de las herramientas. 2.Mantenimiento de los activos de la FND y los proveedores.	Preventivo		GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	1. Proceso de implementación de la mesa de ayuda para reporte de requerimientos e incidentes. 2. implementacion del procedimiento GTE-PO 10 Seguridad de los equipos cuyo objetivo consiste en definirnos las medidas necesarias para evitar la pérdida, daño, robo o el compromiso de los equipos y sistemas de información. **Evidencia:** https://drive.google.com/drive/folders/1UYjE7fSdFILc9uxMdGSBHPvUTaSVR0JY	**22/09/2022**	**1. Los controles propuestos para bajar la valoración del riesgo residual con los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Alta, y con los mismos controles la valoración es moderado (riesgo residual).** **2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos,**
5	1. Falta de controles a los elementos informáticos de la infraestructura tecnológica de la FND. 2. No se tienen los suficientes elementos tecnológicos en Hardware y Software para control de la FND: 3. Falta de supervisión 4. Falta de mecanismos de control	No cumplir con los lineamientos del Modelo de Seguridad y Privacidad de la información y de las Políticas Gobierno Digital	Supervisión de los contratos con terceros que prestan los servicios de infraestructura tecnologica de los sistemas de información de la FND. Estudio de normatividad Gobierno Digital	1.Posibles Sanciones por Mal manejo de la política de la seguridad de la información 2.Actualizaciones del documento base de la política de la seguridad de la información 3.Plan de mejora continua de la Sefuridad Digital 4. Posibles hallazgos 5. Perdida de credibilidad 6. Pérdida de Recursos 7. Reprocesos	TECNOLOGICO	4	4	16	44	Extrema	1.Ejecucion al plan de trabajo de la Politica digital 2.Entrega de informes y porcentaje de avances 3.Creacion del PETI 4.Plan de tratamiento de Riesgos de la Seguridad Digital	Preventivo	Preventivo	24	24	24	24	96	2	0	2	4	8	24	Alta	Evitar	1.Ejecucion al plan de trabajo de la Politica digital 2.Entrega de informes y porcentaje de avances 3.Creacion del PETI 4.Plan de tratamiento de Riesgos de la Seguridad Digital	Preventivo	Preventivo	GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	1. Actualizacion de la politica de Seguridad de la Informacion de acuerdo a los lineamientos de la norma ISO 27001, a la espera de aprobación por Comite de Desempeño. 2. Implementacion del procedimiento GTE-PO 11 Requisitos de Seguridad, en el que se define la sistematica establecida por la FND para identificar y controlar los requisitos de seguridad que deben tenerse en cuenta en los sistemas de información que se adquieran en la organización. 3. Elaboracion del Instuctivo de Evaluacion y analisis de Riesgos por Activo, Procedimiento de Gestion y Administracion de Riesgos por	**22/09/2022**	**1. Los controles propuestos para bajar la valoración del riesgo residual con los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Extrema, y con los mismos controles la valoración es Alta(riesgo residual).** **2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos,**
6	1. Ausencia de personal calificado. 2.No cumplimiento en la gestión misional y administrativa de la FND. 3.Fallas técnicas e incumplimiento en el mantenimiento del sistema de información. 4.Ausencia de Documentación 5. Falta de recursos para la actualización de la tecnología en la FND 6. No recibir adecuada capacitacion a los colaboradores	No disponibilidad de los sistemas tecnologicos y los de información.	Tomar medidas preventivas y reactivas de la FND y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos	1. Mal manejo de todos los activos de tecnologia de la FND. 2. No devolucion de los activos de la FND. 3. Reprocesos 4. Pérdida de Credibilidad 5. Utilización de los sistemas tecnologicos e información obsoletos 6. Posibles hallazgos	TECNOLOGICO	4	3	12	43	Alta	1. Listado de activos físicos de tecnologia 2. Listado de inventario intangible (Sistemas de información) 3. Controles de fechas de terminación de contratos y licencias de uso de los sistemas de información 4.Aplicación de los Acuerdos de Niveles de Servicios (ANS) 6. Copias de seguridad alojadas en Drive	Preventivo	Correctivo	25	25	24	23	97	2	2	2	3	6	23	Moderado	Evitar	1. Listado de activos físicos de tecnologia 2. Listado de inventario intangible (Sistemas de información) 3. Controles de fechas de terminación de contratos y licencias de uso de los sistemas de información 4.Aplicación de los Acuerdos de Niveles de Servicios (ANS) 6. Copias de seguridad alojadas en Drive	Preventivo	Correctivo	GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	4. A través de la implementacion de la herramienta de mesa de ayuda se logra mantener un inventario de equipos y dispositivos actualizado, especificando características físicas software instalado. 5. En la matriz de proveedores se realizaran: Plan de Mantenimiento, Plan de Continuidad, RÓquisitos de seguridad y confidencialidad de cada proveedor en caso de presentarse alguna eventualidad y poder ser activado cualquiera de ellos. Durante el segundo Cuatrimestre del año no se ha presentado ninguna incidencia. **Evidencia:**	**22/09/2022**	**1. Los controles propuestos para bajar la valoración del riesgo residual con los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Alta, y con los mismos controles la valoración es moderada (riesgo residual).** **2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos,**
7	1. Desactualización de Licencias de aplicaciones FND. 2. No renovación de licencias en el momento indicado	Posibilidad de perdida de disponibilidad insuficiencias operativas de software	No tener un registro de los componentes que se utilizan en los procesos que utilizan sistemas de información	1. Resultados desactualizados y no en tiempo real. 2. sin consecutivos de los documentos. 3. Falta de herramienta semaforo para temas de vencimiento en correspondencia. 4. Posibles hallazgos 5. Llamados de atención 6. Riesgos materializados	TECNOLOGICO	4	5	20	45	Extrema	1. Bitacora de sistemas de información de la FND con sus respectivos tiempos de vigencias. 2. Programación de actividades de renovación con sistema de alarmas		Correctivo	22	21	23	21	87	0	0	1	5	5	15	Alta	Evitar	1. Bitacora de sistemas de información de la FND con sus respectivos tiempos de vigencias. 2. Programación de actividades de renovación con sistema de alarmas		Correctivo	GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	4. De acuerdo a la implementacion de la Norma ISO 27001 se elaboró la Matriz de sistemas GTE-PO-13-FT-01 de Información, donde se relacionan todos los datos relevantes del proveedor, entre los cuales están la fecha de inicio y terminacion del contrato. **Evidencia:** https://drive.google.com/drive/folders/1UYjE7fSdFILc9uxMdGSBHPvUTaSVR0JY	**22/09/2022**	**1. Los controles propuestos para bajar la valoración del riesgo residual con los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Extrema, y con los mismos controles la valoración es Alta(riesgo residual).** **2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos,**
8	1. Ausencia de Politica Corporativa de trabajo. 2. Desactualización de la Política de protección de datos. 3. Ausencia de antivirus propio. 4. Desconocimiento por parte de los usuarios de los lineamientos y compromisos de seguridad (Trabajo en Casa). 5.Desactualización de la política de seguridad de la informacion	Ataques Ciberneticos	No ejecutar el debido respaldo de toda la información y no contar con la protección de ésta.	1.Plagio de la información. 2. Perdida de la Informacion 3. Hurto informacion	TECNOLOGICO	4	5	20	45	Extrema	1) Constituir nuevas políticas de trabajo y políticas de seguridad digital (Incluyendo modalidad de trabajo en casa). 2) Control centralizado de equipos informáticos 3) Equipos protegidos a partir de Antivirus		Correctivo	24	24	23	22	93	0	0	1	5	5	15	Alta	Evitar	1) Constituir nuevas políticas de trabajo y políticas de seguridad digital (Incluyendo modalidad de trabajo en casa). 2) Control centralizado de equipos informáticos 3) Equipos protegidos a partir de Antivirus		Correctivo	GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	5. Se continua con la implementacion de políticas en el Directorio Activo. 6. Actualizacion de Antivirus automatico en todos los equipos. 7. La Gerencia de Tecnologia se encuentra trabajando en la implementacion de la norma ISO 27001. De acuerdo a ello se han actualizado y creado procedimientos, asi como tambien se han implementados nuevas herramientas tecnologicas. **Evidencia:** https://drive.google.com/drive/folders/1UYjE7fSdFILc9uxMdGSBHPvUTaSVR0JY	**22/09/2022**	**1. Los controles propuestos para bajar la valoración del riesgo residual con los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Extrema, y con los mismos controles la valoración es Alta(riesgo residual).** **2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos,**
9	1. Perdida de informacion. 2. Falta de mecanismos de control. 3.Suplantacion	Acceso a cuentas de correo FND	Manejar información restringida. Acceder a perfiles no autorizados.	1. Plagio de la informacion 2. Perdida de la Informacion 3. Hurto Informacion 4. Posibles hallazgos 5. Perdida de credibilidad 6. Pérdida de Recursos 7. Reprocesos 8. Materialización del riesgo 9. Llamado de atención por parte de la Alta Dirección	TECNOLOGICO	5	3	15	13	Extrema	1) Eliminacion de cuentas de correos electronicos. 2) Backups de cuentas de correos electronicos.		Correctivo	22	23	22	22	89	0	0	2	3	6	23	Moderado	Evitar	1) Eliminacion de cuentas de correos electronicos. 2) Backups de cuentas de correos electronicos.		Correctivo	GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	1. Se continúa con el proceso de inactivacion de cuentas de correos una vez se haya finalizado el vinculo laboral y se hace respaldo de la informacion.	**22/09/2022**	**1. No fueron efectivos los controles ya que el riesgo se materializó.** **2. Los controles son los mismos en el riego inherente y residual, y sin embargo no son efectivos.** **3. Revisar los controles e implementar un plan de choque con el fin de mitigar el riesgo materializado.**
10	1. Ausencia de inventario de equipos. 2. Ausencia de Bitácora de prestamo y asignación de equipos	Pérdida de equipos informáticos	No tener control sobre qué equipos de computo tienen los colaboradores de la FND	1. Plagio de la informacion 2. Perdida de la Informacion 3. Hurto Informacion 4. posibles hallazgos 5. perdida de recursos 6. Llamados de atención	TECNOLOGICO	2	4	8	24	Alta	1) Listado de activos físicos de tecnologia 2) Correos de asignación de equipos	PREVENTIVO		22	22	22	22	88	0	0	1	4	4	14	Alta	Evitar	1) Listado de activos físicos de tecnologia 2) Correos de asignación de equipos	PREVENTIVO		GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	4. Se continua con el control de equipos de computo por parte de la Gerencia de Tecnología. A través de la implementacion de la herramienta de mesa de ayuda se puede verificar el listado de equipos y a quien se ha realizado la asignación. 5. Implementacion del procedimiento GTE-PO	**22/09/2022**	**Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que e riesgo residual sigue siendo ALTO.**
11	1. Ausencia de mecanismos de monitoreo para brechas en la seguridad. 2. falta de controles	Brechas de seguridad informática	Pérdida de disponibilidad del activo de información	1. Pérdida de reputación 2. Glosas o Multas 3. mala imagen panel área 4. hallazgos entes de control 5. Perdida de credibilidad 6. Pérdida de Recursos 7. Reprocesos 8. Materialización del riesgo 9. Llamado de atención por parte de la Alta Dirección	TECNOLOGICO	2	4	8	24	Alta	Implementar políticas de seguridad de la información que aseguren la integridad de los sistemas de información de la FND	PREVENTIVO		5	15	20	20	64	0	0	1	4	4	14	Alta	evitar	Implementar políticas de seguridad de la información que aseguren la integridad de los sistemas de información de la FND	PREVENTIVO		GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	6. Actualizacion de la Politica de Seguridad de la Informacion de acuerdo a los lineamientos de la Norma ISO 27001, se espera aprobacion por parte de Comite de Gestion y Desempeño.	**22/09/2022**	**Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que e riesgo residual sigue siendo ALTO.**
12	1. Exceso de permisos o privilegios por parte personal no autorizado 2. Mala segregación de funciones de administración	Acceso a información no autorizada	Pérdida de confidencialidad por divulgación no autorizada	1. Pérdida de reputación 2. pérdidas económicas 3. Glosas o Multas 4. hallazgos entes de control 5. Investigaciones disciplinarias 6. Pérdida de Recursos 7. Reprocesos 8. Materialización del riesgo 9. Llamado de atención por parte de la Alta Dirección	TECNOLOGICO	3	3	9	33	Alta	1.Actualizaciones 2.Cambios periodicos de contraseñas 3. Capacitar a los funcionarios para la solicitud de requerimientos	Preventivo		25	25	25	25	100	2	0	1	3	3	13	Moderado	evitar	1.Actualizaciones 2.Cambios periodicos de contraseñas 3. Capacitar a los funcionarios para la solicitud de requerimientos	Preventivo		GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLES SON EFECTIVOS .	5. Unificacion de contraseña de directorio activo con sistema de informacion AZDigital, cada vez que se solicita cambio de contraseña tambien se debe ingresar esa contraseña en este Sistema de Inormacion. 6. En el caso del Sistema de Información Syoman fue solicitada la implementacion de Contraseñas seguras y cada usuario tiene asignado el modulo de cambio de Contraseña donde una vez ingrese al sistema por primera vez debe cambiarla. 8. El acceso a la informacion, modulos, informes, colecciones (Az Digital) se realiza de acuerdo a la definicion de permisos de usuarios asignados por el usuario administrador.	**22/09/2022**	**1. No fueron efectivos los controles ya que el riesgo se materializó.** **2. Los controles son los mismos en el riego inherente y residual, y sin embargo no son efectivos.** **3. Revisar los controles e implementar un plan de choque con el fin de mitigar el riesgo materializado.**

13	1. Ausencia de revisión, verificacion, seguimiento, control 2.Duplicación de información en los sistemas de información	Información erróneа en sistemas de información	Pérdida de integridad por modificación no autorizada	1. Pérdida de reputación 2. pérdidas económicas 3. Glosas o Multas 4. hallazgo entes de control 5. Investigaciones disciplinarias 6. Pérdida de Recursos 7. Reprocesos 8. Materialización del riesgo 9. Llamado de atención por parte de la Alta Dirección	**TECNOLOGICO**	2	4		**8**	24	Alta	1.Acceso a funcionarios a sistemas de información mínimos necesarios. 2. Backups de información para poder restaurar datos en caso de materialización del riesgo	PREVENTIVO		**25**	**25**	**25**	**25**	**100**	2	0	1	4	4	14	Alta	evitar	1.Acceso a funcionarios a sistemas de información mínimos necesarios. 2. Backups de información para poder restaurar datos en caso de materialización del riesgo	Preventivo		GERENTE DE TECNOLÓGIA	SAF	1/1/2022	31/12/2022	ALTO	1. DURANTE ESTE PERIODO NO SE MATERIALIZARON RIESGOS. 2. SE HIZO EVALUACIÓN DE LOS RIESGOS , DONDE SE EVIDENCIO QUE LOS CONTROLERS SON EFECTIVOS .	**1.** Todos los sistemas de información cuenta con definicios de usuarios, roles y permisos de acuerdo a labor realizada en el proceso al que pertenecen. 2. Se da cumplimiento al respaldo de la informacion de acuerdo a lo establecido en los contratos de cada proveedor de Sistema de información.	**22/09/2022**	**1. No fueron efectivos los controles ya que el riesgo se materializó.** **2. Los controles son los mismos en el riego inherente y residual, y sin embargo no son efectivos,** **3. Revisar los controles e implementar un plan de choque con el fin de mitigar el riesgo materializado.**