FND Federación Nacional de Departamentos	GESTIÓN INTEGRAL ORGANIZACIONAL	Codigo: GIO-MR-03
	FORMATO MATRIZ DE RIESGOS GESTION DE SEGURIDAD DIGITAL	Versión: 01
		Fecha: 03/03/2020

FECHA DE ELABORACION:	30 de agosto de 2021
PROCESO	11. GESTIÓN TECNOLÓGICA
OBJETIVO DEL PROCESO	11. Gestionar de manera integral las tecnologías de la información y las comunicaciones - TIC en la FND, prestando todos los servicios alineados con las necesidades de la entidad y las partes interesadas, partiendo de los principios de eficiencia y calidad.
RESPONSABLE DEL PROCESO:	11. GERENTE DE TECNOLÓGIA

VALORES CALIFICACION PROBABILIDAD

DESCRIPTOR	DESCRIPCION	FRECUENCIA	NIVEL
RARO	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.	1
IMPROBABLE	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.	2
POSIBLE	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.	3
PROBABLE	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.	4
CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año	5

ALORES CALIFICACION IMPACT

ESCRIPTOR	DESCRIPCIÓN	NIVEL
INSIGNIFICA	Si el hecho llegara a presentarse, tendría consecuencias	1
MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.	2
MODERADO	Si el hecho llegara a presentarse, tendría medianas	3
MAYOR	Si el hecho llegara a presentarse, tendría altas consecuencias	4
CATASTRÓ	Si el hecho llegara a presentarse, tendría desastrosas	5

NOTA: Se priorizan aquellos riesgos que esten en zona de riesgo: moderado, importante e inaceptable y se plasman en el Mapa de Riesgos Residual.

MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS

PROBABILIDAD	IMPACTO: INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
RARO (1)	B	B	M	A	A
IMPROBABLE (2)	B	B	M	A	E
POSIBLE (3)	B	M	A	E	E
PROBABLE (4)	M	A	A	E	E
CASI SEGURO (5)	A	A	E	E	E

B: ZONA DE RIESGO BAJA: Asumir el riesgo.
M: ZONA DE RIESGO MODERADA: Asumir el riesgo, Reducir el riesgo.
A: ZONA DE RIESGO ALTA: Reducir el riesgo, Evitar, Compartir o Transferir.
E: ZONA DE RIESGO EXTREMA: Reducir el riesgo, Evitar, Compartir o Transferir.

DESCRIPCIÓN Y VALORACIÓN DE LAS CAUSAS Y LOS RIESGOS

	CAUSAS DESCRIPCIÓN DE LA CAUSA (Debido a.......)	RIESGO	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DESCRIPCIÓN DE LA CONSECUENCIA (Lo que genera.........)	CLASE DE RIESGO	EVALUACIÓN DEL RIESGO: PROBABILIDAD	IMPACTO	VALORACIÓN	ZONA DE RIESGO INHERENTE
1	1.Desactualizacion de los aplicativos internos (orfeo, sysman) 2.Ausencia de mecanismos de control tanto del operador como de la FND. 3. repositorio de la información	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 informacion que se maneja 2.Perder la continuidad en el buen funcionamiento de las areas. 3.Demora en la entrega de informacion a organizmos de control 4.Perdida de recursos 5. . Pérdida de información financiera por inexistencia de parametros de seguridad por parte de la Gerencia de Tecnología.	TECNOLOGICO	5	5	55	Extrema
2	1. Fallas en la autenticacion de usuarios 2.Falta de mecanismos de control (USUARIOS, CONTRASEÑAS, ROLES) 3,. Capacitación	Ausencia de controles en los sistemas de información	Manejar información restringida. 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	TECNOLOGICO	4	3	43	Alta
3	1. Hacking de la informacion privilegiada 2. Desconfiguracion de las plataformas con informacion 3. Falta de mecanismos controles 4. roles definidos	Manipulación, modificacion o alteracion sin autorizacion de la información registrada en los sistemas de la FND	Manejar información restringida. Acceder a perfiles no autorizados.	1.Perdida de informacion privada de la FND 2.Posibles sanciones por no reportar informacion a tiempo 3. Uso inadecuado de la información 4. Pérdida de credibilidad 5. Hallazgos de entes de control	TECNOLOGICO	4	4	44	Extrema
4	1. Desconocimiento normativo vigente sobre plataforma tecnologica y comunicaciones. 2.Incumplimiiento de los lineamientos en materia de la gestión plataformas tecnologica y comunicaciones. 3. falta de supervisión 4. Alta rotación de personal 5. Capacitación	Erronea gestión de la infraestructura tecnológica de la FND	Gestionar y los disitintos 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 conectvidad, 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	43	Alta
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	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 politica de la seguridad de la informacion 2.Actualiaciones del documento base de la politica de la seguridad de la informacion 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	44	Extrema

CONTROLES EXISTENTES

	DESCRIPCIÓN	TIPO DE CONTROL: PREVENTIVO	CORRECTIVO	DO	AP	EF	EV	PUNTAJE (DO+AP+EF+EV)	PROBABILIDAD	IMPACTO	NUEVA CALIFICACIÓN: PROBABILIDAD	IMPACTO	VALORACIÓN	ZONA DE RIESGO RESIDUAL	OPCIONES DE MANEJO
1	Ejecutar las copias de seguridad debidamente según el procedimiento.	Correctivo		25	25	25	25	100	0	0	1	4	14	Alta	evitar
2	Contar con el control adecuado de los usuarios y claves de los colaboradores de la FND	Preventivo		23	25	25	25	98	2	0	1	4	14	Alta	Reducir
3	Funcionarios con acceso a informacion exclusiva de su proceso.	PREVENTIVO		25	25	25	25	100	2	0	1	4	14	Alta	Evitar
4	Supervisión de los contratos con terceros que prestan los servicios de infraestructura tecnologica de los sistemas de información de la FND. Aplicación de los Acuerdos de Niveles de Servicios (ANS)	PREVENTIVO		20	20	20	20	80	2	0	2	4	24	Alta	Evitar
5	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	PREVENTIVO		24	24	24	24	96	2	0	2	4	24	Alta	Evitar

PLAN DE MANEJO DEL RIESGO

	CONTROL PROPUESTO O ACCIONES A TOMAR	TIPO DE CONTROL: PREVENTIVO	CORRECTIVO	RESPONSABLE: CARGO	DEPENDENCIA	CRONOGRAMA IMPLEMENTACIÓN ACCIONES: INICIA	TERMINA	INDICADOR PARA LA EVALUACIÓN DE ACCIONES IMPLEMENTADAS
1	1. Copias de seguridad alojadas en Drive 2. Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND	Preventivo	Correctivo	GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	100%
2	1.Claves unicas para trabajadores. Manejo de información por areas o procesos. 2.Actualizaciones y cambios periodicos de las contraseñas	Preventivo		GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	80%
3	1.Actualizaciones 2.Cambios periodicos de contraseñas 3. Capacitar a los funcionarios para la solicitud de requerimientos	Preventivo		GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	80%
4	1.Actualizacion y mantenimiento de las herramientas. 2.Mantenimiento de los activos de la FND y los proveedores.	Preventivo		GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	100%
5	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	5/1/2021	1/1/2022	50%

	SEGUIMIENTO ENERO -ABRIL - GTE	SEGUIMIENTO MAYO -AGOSTO - GTE	MONITOREO Y REVISION OFICINA CONTROL INTERNO: SEGUIMIENTO Y MONITOREO
1	Se realizaron las copias de seguridad de los aplicativos: Sysman(Financiero), Orfeo, y cuentas de correo electronico de colaboradores salientes. Se alojan en el Drive del equipo de tecnología	1.Este riesgo no se ha materializado durante el cuatrimestre, sin embargo se continúan realizando las copias de seguridad de todos los aplicativos con los que se trabajan en la FND: Sysman(Financiero), Orfeo, y cuentas de correo electrónico de colaboradores salientes. Toda esta información se almacena en el Drive del equipo de tecnología. 2.Sysman se realiza backup diario, a Orfeo se le realiza backup semanal, y a las cuentas de correo electrónico cada vez que se vaya a eliminar un correo electrónico (Adjunto imagen que muestra la relación de las ultimas cuentas eliminadas). 3.GTE realiza la inactivación de las cuentas de correos electrónicos de los contratistas salientes que son informadas al área. Es importante indicar que si una cuenta está inactiva, no quiere decir que no aparecerá más en las cuentas de otros colaboradores, ya que, si en algún momento un usuario tuvo interacción con esa persona, podrá seguir viendo el historial de correos de esa persona. La restricción que se aplica es que el contratista saliente no podrá acceder o ingresar nunca más a su cuenta de correo electrónico. De igual manera se hace con el usuario de Sysman (si es que tiene) y el de Orfeo. 4.Por otro lado, se han realizado capacitaciones de SYSMAN en las siguientes fechas: □13 julio de 2021 capacitación stefanini sysman contabilidad y presupuesto □28 julio de 2021, modulo contratación sysman □30 agosto de 2021 capacitación modulo almacén □13 sept de 2021 capacitación stefanini sysman contabilidad y presupuesto	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital
2	Actualmente cada colaborador es el que administra y asigna sus contraseñas de los aplicativos de la FND. Sin embargo es necesario implementar políticas que aseguren el vencimiento y solicitud de cambios de contraseñas	Actualmente cada colaborador es el que administra y asigna sus contraseñas de los aplicativos de la FND. Sin embargo se han adelantado labores para este tema: 1) Se incluyó una sección de manejo contraseñas en la politica de seguridad de información (*8.4.1. Política de establecimiento, uso y protección de claves de acceso*), la cual está en proceso de revisión por parte de la empresa consultora de la certificación ISO 27001, con fines de ajustarla a los requerimientos de la norma anteriormente mencionada. Esto por recomendación de los mismos consultores quienes son expertos en seguridad de la información. 2) Se adquirió el Directorio Activo para la FND bajo el contrato FND.481.2021 - ADVANCED INFORMATION TECHNOLOGIES S.A.S. En este momento el equipo de tecnología se encuentra realizando la implementación y configuración del mismo en la FND. Una vez estén incluidos cada uno de los computadores al Directorio Activo, se iniciarán a implementar las politicas de seguridad identificadas, entre las cuales se encuentra el manejo de las contraseñas.	□Se puede evidenciar que los controles establecidos no son efectivos, ya que a pesar de estos el riesgo residual continua alto. □Evaluar los controles establecidos en cada uno de los riesgos teniendo en cuenta que se evidencia la poca efectividad de estos, ya que su ineficacia puede llevar a la materialización de estos.
3	1. Se actualizó el antivirus en los equipos de los colaboradores 2. Actualmente cada colaborador es el que administra y asigna sus contraseñas de los aplicativos de la FND. Sin embargo es necesario implementar políticas que aseguren el vencimiento y solicitud de cambios de contraseñas. 3. En la intranet se encuentra disponible el enlace para solicitud de requerimientos al equipo de tecnología	1. Se actualizó el antivirus en los equipos de los colaboradores, el cual tiene una vigencia de cubrimiento de 1 año, y que se actualiza de manera automatica cuando los equipos se conectan a internet. 2. Actualmente cada colaborador es el que administra y asigna sus contraseñas de los aplicativos de la FND. Sin embargo se incluyó una sección de manejo contraseñas en la politica de seguridad de información (8.4.1. Política de establecimiento, uso y protección de claves de acceso), la cual está en revisión; y se adquirió el Directorio Activo para la FND bajo el contrato FND.481.2021 - ADVANCED INFORMATION TECHNOLOGIES S.A.S. en el que se va a implementar las politicas de seguridad, entre las cuales se encuentra el manejo de las contraseñas. 3. En la intranet se encuentra disponible el enlace para solicitud de requerimientos al equipo de tecnología. Se anexa imagen de la hoja de calculo en la que se reciben dichas solicitudes.	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital Se puede evidenciar que los controles establecidos no son efectivos, ya que a pesar de estos el riesgo residual continua alto.
4	1. Revisión periodica del correcto funcionamiento de los equipos de la FND. 2. Se mantienen los aplicativos disponibles para los colaboradores actualizados.	1. Revisión periodica del correcto funcionamiento de los equipos de la FND. Esto se controla basado en las solicitudes o requerimientos que hacen los colaboradores a través de correo electronico o por medio del canal dispuesto en la intranet 2. Se mantienen los aplicativos disponibles para los colaboradores actualizados.	□Se puede evidenciar que los controles establecidos no son efectivos, ya que a pesar de estos el riesgo residual continua alto. □Evaluar los controles establecidos en cada uno de los riesgos teniendo en cuenta que se evidencia la poca efectividad de estos, ya que su ineficacia puede llevar a la materialización de estos.
5	1. Seguimiento al plan de acción definido para la implementación de la política de gobierno digital. 2. Presentación del PETI al comité de Gestión y Desempeño	Se cuenta con una proyección de documento de PETI, el cual debe actualizarse para estar articulado con el Plan Estrategico FND 2021-2025 "1. PETI FND.docx" Tanto el 15 de julio de 2021, cómo el 20 de agosto de 2021 se ha solicitado el Plan Estrategico a la oficina de Planeación de la FND, sin tener respuesta positiva. Esto retrasa la construcción de esta tarea teniendo en cuenta que es la base para poder construir el Plan.	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital Se puede evidenciar que los controles establecidos no son efectivos, ya que a pesar de estos el riesgo residual continua alto □Oficiar a la Oficina de planeación, para que explique los motivos de la no entrega del plan estratégico para articular el PETI, para el cumplimiento de los objetivos del área de tecnología.

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 actualizacion de la tecnologia 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 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 informaión obsoletos 6. Posibles hallazgos	TECNOLOGICO	4	3	43	Alta	Ejecutar las copias de seguridad debidamente según el procedimiento. Contar con el adecuado inventario de los activos de la FND	PREVENTIVO		25	25	24	23	97	2	0	2	4	24	Alta	1. Listado de activos fisicos de tecnología 2. Listado de inventario intangible (Sistemas de información) 3. Controles de fechas de terminación de contratos	1. Listado de activos fisicos de tecnología 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) 5. Copias de seguridad alojadas en Drive	Preventivo	Correctivo	GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	100%	El equipo de tecnología tiene en el Drive los listados de los activos e intangibles con los que cuenta la FND.	1. Se mantiene actualizado un listado con todos los activos con el que el área cuenta. Este fue cotejado con la Coordinación Administrativa durante el cuatrimestre, ejercicio en el cual se evidencio un control de existencia de los mismos. 2 y 3) Se cuenta con un listado sencillo y de control de todos los sistemas de información que tiene la FND, en el cual se establecen las fechas de inicio y fin de cada uno de los contratos. Esto permite al equipo GTE a estar atentos a posibles futuros vencimiento de los licenciamientos de los mismos, y así iniciar las labores de continuidad del negocio con tiempo oportuno. Para controlar estas actividades, GTE creó un sistema de alertas por medio del calendario de Google, en donde se da aviso al equipo del vencimiento de un sistema de información con mínimo 1 mes de anterioridad. 4) Durante el cuatrimestre no ha sido requerido activar los ANS con ningun prestador de servicios tecnologicos de la FND 5) Se vienen realizando las copias de seguridad de todos los aplicativos con los que se trabajan en la FND: Sysman(Financiero), Orfeo, y cuentas de correo electronico de colaboradores salientes. Toda esta informacion se alojan en el Drive del equipo de tecnología. Sysman se realiza backup diario, a Orfeo se le realiza backup semanal, y a las cuentas de correo electronica cada vez que se vaya a eliminar un correo electronico (Adjunto imagen que muesta la relación de las ultimas cuentas eliminadas).	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital
7	1. Desactualizacion de Licencias de aplicaciones FND. 2. No renovaciòn de licencias en el momento indicado	Insuficiencias operativas de software	No tener un registro de los componentes que se utilizan en los procesos que utilizan sistemas de informacion	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.	TECNOLOGICO	4	5	45	Extrema	Bitacora de revision y lista de chequeo en intalacion y vigencias de software en la FND	PREVENTIVO		22	21	23	21	87	0	0	1	4	14	Alta	Evitar	1. Bitacora de sistemas de información de la FND con sus respectivos tiempos de vigencias. 2. Programaciòn de actividades de renovaciòn con sistema de alarmas		Correctivo	GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	100%	El equipo de tecnología tiene en el Drive el listado de los sistemas de información con los que cuenta la FND, con su respectivo contrato, y fechas de vencimientos de vigencias.	Se cuenta con un listado sencillo y de control de todos los sistemas de información que tiene la FND, en el cual se establecen las fechas de inicio y fin de cada uno de los contratos. Esto permite al equipo GTE a estar atentos a posibles futuros vencimiento de los licenciamientos de los mismos, y así iniciar las labores de continuidad del negocio con tiempo oportuno. Para controlar estas actividades, GTE creó un sistema de alertas por medio del calendario de Google, en donde se da aviso al equipo del vencimiento de un sistema de información con mínimo 1 mes de anterioridad.	
8	1. Ausencia de Política Corporativa de trat	Ataques Ciberneticos	No ejecutar el debido respaldo de toda la información y no contar con la protección de ésta.	Plagio de la infomracion Perdida de la Imformacion Hurto Informacion	TECNOLOGICO	4	5	45	Extrema	Monitoreo y seguimiento a los proveedores tecnologicos de la FND. Sistema de antivirus vigente en equipos FND	PREVENTIVO		24	24	23	22	93	0	0	2	4	24	Alta	Evitar	1) Constituir nuevas politicas de trabajo y politicas de seguridad digital (incluyendo modalidad de trabajo en casa). 2) Control centralizado de equipos informàticos 3) Equipos protegidos a partir de Antivirus		Correctivo	GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	100%	Se está adelantando estudios para la implementación de un Directorio Activo que permita realizar control y aplicación de políticas de seguridad información de manera centralizada y a todos los equipos de la FND	1) Se efectuó segunda versión de política de Seguridad de la Información, la cual cumple con los requisitos del MinTic, no está aprobada debido a que se encuentra en REVISIÓN por parte de la empresa consultora de la certificación ISO 27001, con fines de ajustarla a los requerimientos de la norma anteriormente mencionada. Esto por recomendación de los mismos consultores quienes son expertos en seguridad de la información. Sin embargo, existen controles asociados a la politica que se encuentran implementados, cómo son la utilización de las contraseñas en los sistemas de la FND, control de acceso a información de Google Drive, Segmentación de la red de la FND, Circuito Cerrado de Televisión (camaras web), control del acceso a los rack de comunicaciones. Ademas se realizó el diagnostico del estado actual de la FND en relación con la implementación de la ISO 27001. (Se adjunta resultado) 2) Se adquirió el Directorio Activo para la FND bajo el contrato FND.481.2021 - ADVANCED INFORMATION TECHNOLOGIES S.A.S. En este momento el equipo de tecnología se encuentra realizando la implementación y configuración del mismo en la FND. Una vez estén incluidos cada uno de los computadores al Directorio Activo, se iniciarán a implementar las politicas de seguridad identificadas, entre las cuales se encuentra el manejo de las contraseñas, control de accesos, bloqueo de puertos, cifrado de datos, y otras. 3) Se actualizó el antivirus en los equipos de los colaboradores, el cual tiene una vigencia de cubrimiento de 1 año, y que se actualiza de manera automatica cuando los equipos se conectan a internet.	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital .
9	1. Perdida de informacion.	Acceso a cuentas de correo FND	Manejar información restringida. Acceder a perfiles no autorizados.	Plagio de la infomracion Perdida de la Imformacion Hurto Informacion	TECNOLOGICO	4	4	44	Extrema	Seguimiento a bitacora contractual - usuarios	PREVENTIVO		22	23	22	22	89	0	0	3	4	34	Extrema	Evitar	1) Eliminacion de cuentas de correos electronicos. 2) Backups de cuentas de correos electronicos.		Correctivo	GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	100%	Se está adelantando estudios para la implementación de un Directorio Activo que permita realizar control y aplicación de políticas de seguridad información de manera centralizada y a todos los equipos de la FND	GTE realiza la inactivación de las cuentas de correos electronicos de los contratistas salientes que son informadas al área. Es importante indicar que si una cuenta está inactiva, no quiere decir que no aparecerá más en las cuentas de otros colaboradores, ya que si en algún momento un usuario tuvo iteracción con esa persona, podrá seguir viendo el historial de correos de esa persona. La restricción que se aplica, es que el contratista saliente no podrá acceder o ingresar nunca mas a su cuenta de correo electronico. De igual manera se hace con el usuario de Sysman (si es que tiene) y el de Orfeo. Se realiza backup a las cuentas de correo electronica cada vez que se vaya a eliminar un correo electronico (Adjunto imagen que muesta la relación de las ultimas cuentas eliminadas).	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital Se puede evidenciar que los controles establecidos no son efectivos, ya que a pesar de estos el riesgo residual continua alto.
10	1. Ausencia de inventario de equipos. 2. Ausencia de Bitàcora de prestamo y asignaciòn de equipos	Pèrdida de equipos informàticos	No tener control sobre què equipos de computo tienen los colaboradores de la FND	Plagio de la infomracion Perdida de la Imformacion Hurto Informacion	TECNOLOGICO	2	4	24	Alta	Seguimiento a bitacora de prestamos de equipos	PREVENTIVO		22	22	22	22	88	0	0	2	3	23	Moderada	Evitar	1) Listado de activos fisicos de tecnología 2) Correos de asignaciòn de equipos	PREVENTIVO		GERENTE DE TECNOLÓGIA	SAF	5/4/2021	31/12/2021	100%	Se está adelantando estudios para la implementación de un Directorio Activo que permita realizar control y aplicación de políticas de seguridad información de manera centralizada y a todos los equipos de la FND	Los equipos informaticos que fueron entregados a los colaboradores, todos tienen asignado un responsable (personal de planta), quién será responsable de responder por los mismos. En cuanto a los equipos de escritorio, que son los que se encuentran en las instalaciones de la FND, no puedes ser sacados de los edificios sin una autorizaciín escrita a la administración de los mismos, controlando así la no sustracción, perdida o robo de los mismos. En cuanto a los computadores portátiles, no es posible conocer la ubicación geografica exacta de cada computador, así que siempre estarán asignados a un subdirector, y él por vía correo electronico será la persona que nos indiqué a quién, ya sea persona de planta o contratista, se le hará entrega del portátil. Esta informaciòn es actualizada en la matriz del área GTE con fines de saber el usuario final de cada equipo.	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital .
11	Ausencia de mecanismos de monitoreo para brechas en la seguridad	Brechas de seguridad informática	Pérdida de disponibilidad del activo de información	Pérdida de reputación pérdidas económicas Glosas o Multas hallazgos entes de control	TECNOLOGICO	2	4	24	Alta	Monitoreo manual de correcto funcionamiento de los sistemas de información	PREVENTIVO		5	19	20	20	64	0	0	1	4	14	Alta	evitar	Implementar politicas de seguridad de la información que aseguren la integridad de los sistemas de información de la FND	PREVENTIVO		GERENTE DE TECNOLÓGIA	SAF	1/9/2021	31/12/2021	50%	No estaba identificado el riesgo	1) Se efectuó segunda versión de política de Seguridad de la Información, la cual cumple con los requisitos del MinTic, no está aprobada debido a que se encuentra en REVISIÓN por parte de la empresa consultora de la certificación ISO 27001, con fines de ajustarla a los requerimientos de la norma anteriormente mencionada. Esto por recomendación de los mismos consultores quienes son expertos en seguridad de lAdemas se realizó el diagnostico del estado actual de la FND en relación con la implementación de la ISO 27001. (Se adjunta resultado)a información. Sin embargo, existen controles asociados a la politica que se encuentran implementados, cómo son la utilización de las contraseñas en los sistemas de la FND, control de acceso a información de Google Drive, Segmentación de la red de la FND, Circuito Cerrado de Televisión (camaras web), control del acceso a los rack de comunicaciones. Ademas se realizó el diagnostico del estado actual de la FND en relación con la implementación de la ISO 27001. (Se adjunta resultado)	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital .
12	Exceso de permisos o privilegios por parte personal no autorizado Mala segregación de funciones de administración	Acceso a información no autorizada	Pérdida de confidencialidad por divulgación no autorizada	Pérdida de reputación pérdidas económicas Glosas o Multas hallazgos entes de control Investigaciones disciplinarias	TECNOLOGICO	3	3	33	Alta	Funcionarios con acceso a informacion exclusiva de su proceso.	PREVENTIVO		25	25	25	25	100	2	0	1	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	1/9/2021	31/12/2021	50%	No estaba identificado el riesgo	Actualmente cada colaborador es el que administra y asigna sus contraseñas de los aplicativos de la FND. Sin embargo se han adelantado labores para este tema: 1) Se incluyó una sección de manejo contraseñas en la politica de seguridad de información (*8.4.1. Politica de establecimiento, uso y protección de claves de acceso*), la cual está enproceso de revisión por parte de la empresa consultora de la certificación ISO 27001, con fines de ajustarla a los requerimientos de la norma anteriormente mencionada. Esto por recomendación de los mismos consultores quienes son expertos en seguridad de la información. 2) Se adquirió el Directorio Activo para la FND bajo el contrato FND.481.2021 - ADVANCED INFORMATION TECHNOLOGIES S.A.S. En este momento el equipo de tecnología se encuentra realizando la implementación y configuración del mismo en la FND. Una vez estén incluidos cada uno de los computadores al Directorio Activo, se iniciarán a implementar las politicas de seguridad identificadas, entre las cuales se encuentra el manejo de las contraseñas.	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital

13	Ausencia de revisión, verificacion, seguimiento, control Duplicación de información en los sistemas de información	Información errónea en sistemas de información	Pérdida de integridad por modificación no autorizada	Pérdida de reputación Glosas o Multas hallazgos entes de control Investigaciones disciplinarias	**TECNOLOGICO**	**2**	**3**	23	**Moderada**	Funcionarios con acceso a informacion exclusiva de su proceso.	PREVENTIVO		**25**	**25**	**25**	**25**	**100**	2	0	**1**	**4**	14	**Alta**	evitar	1.Acceso a funcionarios a sistemas de informaciòn minimos necesarios. 2. Backups de informaciòn para poder restaurar datos en caso de materialización del riesgo	PREVENTIVO		GERENTE DE TECNOLÓGIA	SAF	1/6/2021	31/12/2021	**100%**	No estaba identificado el riesgo	No se ha materializado el riesgo 1. Las unicas personas que tienen acceso a los sistemas financieros y de gestión documental, son las personas de planta que son solicitadas a GTE por parte de un jefe de área. De resto, a nadie más se le habilita el acceso a los mismos. Se adjunta imagen de solicitudes. 2. Se mantienen los backups de la información de los mismos con el fin de tener un plan de mitigaci{on de la información, en caso de una alteración de la misma.	La Gerencia de tecnología GTE, debe continuar implementando mecanismo de control para evitar que se materialicen los riesgos de seguridad digital