FND Federación Nacional de Departamentos

GESTIÓN INTEGRAL ORGANIZACIONAL

FORMATO MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL

CÓDIGO: GOI-FR-07	
VERSIÓN: 2	
FECHA: 15/05/2021	

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: PROB. DE OCURR.	IMPACTO	NIVEL	VALORACIÓN	CONTROLES EXISTENTES: DESCRIPCIÓN	TIPO DE CONTROL: PREVENTIVO	CORRECTIVO	DO	AP	EF	EV	PUNTAJE (DO+AP+EF+EV)	PROB. DE OCURR.	IMPACTO	RIESGO RESIDUAL: PROB. DE OCURR.	IMPACTO	NIVEL	VALORACIÓN	OPCIONES DE MANEJO	PLAN DE MANEJO DEL RIESGO: CONTROL PROPUESTO O ACCIONES A TOMAR	TIPO DE CONTROL: PREVENTIVO	CORRECTIVO	RESPONSABLE: CARGO	DEPENDENCIA	CRONOGRAMA IMPLEMENTACIÓN ACCIONES: FECHA INICIO	FECHA TERMINO	INDICADOR PARA LA EVALUACIÓN DE ACCIONES IMPLEMENTADAS	SEGUIMIENTO ENERO -ABRIL - 2022	SEGUIMIENTO MAYO -AGOSTO - 2022	SEGUIMIENTO SEPTIEMBRE - DICIEMBRE - 2022	MONITOREO Y REVISIÓN OFICINA CONTROL INTERNO: FECHA	ACCIONES REALIZADAS
1	1. Desactualización de las aplicativos internos (sofos, sysman) 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.	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 esta.	1.Pérdida de autenticidad en la información que se maneja 2.Perder la continuidad en el buen funcionamiento de las áreas 3.Demora en la entrega de información a organismos de control 4.Pérdida de recursos 5. Pérdida de información financiera por inexistencia de copias de seguridad por parte de la Gerencia de Tecnología. 6. Posibles hallazgos 7. Malentendidos de riesgos. 8. Toma de decisiones erradas 9. Llamados de atención	TECNOLOGICO	5	5	25	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	1	1	Alta	evitar	1. Copias de seguridad alojadas en Drive 2. Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND	Preventivo		GERENTE DE TECNOLOGÍA	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 los sistemas de informacion AZ DIGITAL y SYSMAN de acuerdo a cláusulas contractuales de en los respectivos contratos. 2. Con la implementacion del Director de documentos electronicos de archivo AS DIGITAL se garantiza la trazabilidad de los documentos, integridad, confidencialidad y disponibilidad de la información. 3. Sistemas e aplicaciones: Transformacion Digital, Analisis de Datos. **Evidencia:** https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	1. Copias de seguridad de los sistemas de informacion AZ DIGITAL y SYSMAN de acuerdo a cláusulas contractuales de en los respectivos contratos. 2. Con la implementacion del Director de documentos electronicos de archivo AS DIGITAL se garantiza la trazabilidad de los documentos, integridad, confidencialidad y disponibilidad de la información.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**
2	1. Fallas en la autenticación de usuarios 2 Falta de mecanismos de control (USUARIOS, CONTRASEÑAS, ROLES) 3. Capacitación	Ausencia de controles en los sistemas de información	1. Manejar información restringida. 2. Acceder a perfiles no autorizados.	1. Manipulacion de las suertas. 2 . Perdida de informacion 3. Perdida de recursos 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	Alta	1. Claves unicas para trabajadores. 2. Manejo de información por areas o procesos. 3. Actualizaciones y cambios periodicos de las contraseñas.	Preventivo		20	25	25	25	95	2	0	1	3	3	Moderada	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 TECNOLOGÍA	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. Con la implementacion del Directorio Activo y el Procedimiento de Control de Acceso se definieron politicas para el uso de contraseñas seguras, periodicidad de tiempo para cambiarla (cada 60 dias). 2. El sistema de AZ DIGITAL está sincronizado con el directorio activo lo que permite ingresar con el mismo usuario y contraseña con lo que se ingresa al equipo de la FND y los usuarios son inactivados por directorio activo una vez terminen su vinculacion laboral 3. El acceso a la informacion en cada sistema de informacion esta definido por roles, permisos de usuarios **Evidencia:** https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	1. Con la implementacion del Directorio Activo y el Procedimiento de Control de Acceso se definieron politicas para el uso de contraseñas seguras, periodicidad de tiempo para cambiarla (cada 60 dias). 2. El sistema de AZ DIGITAL está sincronizado con el directorio activo lo que permite ingresar con el mismo usuario y contraseña con lo que se ingresa al equipo de la FND y los usuarios son inactivados por directorio activo una vez terminen su vinculacion laboral 3. El acceso a la informacion en cada sistema de informacion esta definido por roles, permisos de usuarios	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual se mantiene en moderado**
3	1. Hacking de la información privilegiada 2. Ausencia de controles en los sistemas de información 3. Falta de mecanismos de control 4.Falta de roles definidos. 5. Ausencia de mecanismos de control	Manipulación, modificación o alteración no autorizada de la información registrada en los sistemas de la FND	1. Manejar información restringida. 2. Acceder a perfiles no autorizados.	1. Perdida de informacion 2. Perdida de recursos 3. Resultados defectuosos de reportar informacion a organismos de control y informacion 4. Pérdida de credibilidad 5. Hallazgos de entes de control.	TECNOLOGICO	4	4	16	Extrema	1.Actualizaciones 2. Cambios periodicos de contraseñas 3. Capacitar a los funcionarios para la solicitud de requerimientos	Preventivo		20	25	25	25	100	2	0	1	3	3	Alta	Evitar	1.Actualizaciones 2. Cambios periodicos de contraseñas 3. Capacitar a los funcionarios para la solicitud de requerimientos	Preventivo		GERENTE DE TECNOLOGÍA	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. Politicas implementadas en el directorio Activo y procedimiento de Control de Acceso: - Contraseñas Seguras (Mayusculas, minusculas, numeros, simbolo alfanumerico) - Solicitud de Cambio de contraseña: Cada 60 dias - Usuarios: NOMBRE.APELLIDO 2.Clausulas de confidencialidad de la información en los contratos de proveedores. 3. Definiciones de roles y permisos en los usuarios de los Sistemas de Informacion, como SYSMAN, AZ DIGITAL. **Evidencia:** https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	1. Politicas implementadas en el directorio Activo y procedimiento de Control de Acceso: - Contraseñas Seguras (Mayusculas, minusculas, numeros, simbolo alfanumerico) - Solicitud de Cambio de contraseña: Cada 60 dias - Usuarios: NOMBRE.APELLIDO 2.Clausulas de confidencialidad de la información en los contratos de proveedores. 3. Definiciones de roles y permisos en los usuarios de los Sistemas de Informacion, como SYSMAN, AZ DIGITAL.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**
4	1. Desconocimiento normativo vigente sobre plataforma tecnologica y comunicaciones. 2 Incumplimiento de las lineamientos en materia de la gestión plataforma tecnologica y comunicaciones. 2. Falta de mantenimiento 3. Alta rotación de personal 4. Capacitación	Fraude gestión de la infraestructura tecnológica de la FND	Gestionar y ha. distribuir procesos de infraestructura tecnológica de la FND y sus activos.	1. Fallas en la conectividad de los sistemas de información tanto internos como externos 2. Perdida de recursos (Internet, pagina Web, correo electronico sistemas de información) 3. perdida de recursos 4. Posibles sanciones de organismos de control, CGN, DIAN 5. Pérdida de credibilidad 6. Posibles hallazgos entes de control	TECNOLOGICO	4	3	12	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	1	3	3	Moderada	Evitar	1.Actualizacion y mantenimiento de las herramientas. 2.Mantenimiento de los activos de la FND y los proveedores.	Preventivo		GERENTE DE TECNOLOGÍA	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 Implementacion de la mesa de ayuda para reporte de requerimientos e incidentes. 2. Implementacion del procedimiento GTI-PO-01 Seguridad de los equipos - copia objetivo donde se definieron las medidas necesarias para evitar la perdida, daño, robo o el comprometer de los equipos y sistemas de informacion **Evidencia:** https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	1.Implementacion la mesa de ayuda para reporte de requerimientos e incidentes. 2. Implementacion del procedimiento GTI-PO-01 Seguridad de los equipos copia objetivo donde se definieron las medidas necesarias para evitar la perdida, daño, robo o el comprometer de los equipos y sistemas de informacion https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual se mantiene en moderado**
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 tecnológica de los sistemas de información de la FND. Estado de normatividad Gobierno Digital	1.Posibles funciones por fallas manejo de la politica de la seguridad de la informacion 2. Posibles sanciones por incumplimiento a la normatividad vigente sobre la seguridad de la información 3.Perdida de credibilidad en la Seguridad Digital 4. Posibles hallazgos 5. Perdida de credibilidad 6. Perdida de Recursos 7. Reprocesos	TECNOLOGICO	4	5	20	Extrema	1.Ejecucion el 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	1	4	3	Alta	Evitar	1.Ejecucion el 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 TECNOLOGÍA	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, aprobada por Comite de Desempeño, al cargarla de la Feria del Director Ejecutivo. 2. Implementacion del procedimiento GTI-PO-01 Requisitos de Seguridad, en el que se define la administracion establecida por la TIC para identificar y controlar los requisitos de seguridad que deben tenerse en cuenta en los sistemas de informacion que se adquieren en la organización. 3. Elaboracion del Instructivo de Evaluacion y analisis de Riesgos por Activos. Procedimiento de Gestion y Administracion de Riesgos por Activos, Mdelo de Riesgos por Activos. (Falta aprobacion por parte de la Oficina de Planeacion) **Evidencia:** https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	1. Actualizacion de la politica de Seguridad de la informacion de acuerdo a los lineamientos de la norma ISO 27001, aprobada por Comite de Desempeño, al cargarla de la Feria del Director Ejecutivo. 2. Implementacion del procedimiento GTI-PO-01 Requisitos de Seguridad, en el que se define la administracion establecida por la TIC para identificar y controlar los requisitos de seguridad que deben tenerse en cuenta en los sistemas de informacion que se adquieren en la organización. 3. Aprobacion y publicacion del Instructivo de Evaluacion y analisis de Riesgos por Activos, Procedimiento de Gestion y Administracion de Riesgos por Activos, Mdelo de Riesgos por Activos	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**
6	1. Ausencia de personal calificado. 2.No cumplimiento en la gestión misional y administrativa. 3. Falta de controles a los elementos informáticos en el mantenimiento del sistema de informacion. 4.Ausencia de Documentación 5. Falta de recursos para la actualización de la tecnología en la FND 6. No reder adecuado capacitacion a los colaboradores	No disponibilidad de los sistemas tecnologicos y los de información	Tener medidas preventivas y reactivas de la FND y sistemas tecnologicos 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 almacenaje de los activos de la FND. 3. Reprocesos 4. Perdida de credibilidad 5. Utilización de los sistemas tecnologicos e informaticos obsoletos 6. Posibles hallazgos	TECNOLOGICO	4	5	12	Alta	1. Listado de activos fisicos de tecnologia 2. Listado de inventario tecnologico (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	25	25	24	25	97	2	2	1	5	3	Moderada	Evitar	1. Listado de activos fisicos de tecnologia 2. Listado de inventario tecnologico (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 TECNOLOGÍA	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. A futuro de la implementacion de la herramienta de mesa de ayuda se logra mantener un inventario de equipos y dispositivos actualizado, especificando características Fisicas software instalado. 2. En la matriz de proveedores ce realizaran. Plan de Mantenimiento, Plan de Contingencia, Requisitos 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. https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	1. A futuro de la implementacion de la herramienta de mesa de ayuda se logra mantener un inventario de equipos y dispositivos actualizado, especificando características Fisicas software instalado. 2. En la matriz de proveedores ce realizaran. Plan de Mantenimiento, Plan de Contingencia, Requisitos 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. https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual se mantiene en moderado**
7	1. Desactualización de Licencias de aplicaciones FND. 2. No renovación 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 consistencia de los documentos. 3. falta de herramienta cemaforo para temas de vencimiento de correspondencia. 4. Posibles hallazgos 5. Llamados de atención 6. Riesgos materializados.	TECNOLOGICO	4	5	20	Extrema	1. Bitacora de sistemas de informacion de la FND con sus respectivos tiempos de vencimiento. 2. Programacion de actividades de renovación con sistema de alarmas		Correctivo	22	21	23	21	87	0	0	1	5	5	Alta	Evitar	1. Bitacora de sistemas de informacion de la FND con sus respectivos tiempos de vencimiento. 2. Programacion de actividades de renovación con sistema de alarmas		Correctivo	GERENTE DE TECNOLOGÍA	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. De acuerdo a la implementacion de la Norma ISO 27001 se elaboró la bitácora de sistemas GTI-PO-13-FT-01 de informacion, donde se relacionan todos los activos de informacion con sus respectivas fechas de inicio y terminacion de licencias de uso. **Evidencia:** https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	1. De acuerdo a la implementacion de la Norma ISO 27001 se elaboró la bitácora de sistemas GTI-PO-13-FT-01 de informacion, donde se relacionan todos los activos de informacion con sus respectivas fechas de inicio y terminacion de licencias de uso.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**
8	1. Ausencia de Política 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 las lineamientos y compromisos de seguridad (Trabajo en Casa). 5.Desactualización de la politica de seguridad de la informacion	Ataques Cibernéticos	No ejecutar el debido respaldo de toda la información y no contar con la protección de esta.	1.Plagio de la informacion. 2. Perdida de la informacion 3. Hurto informacion	TECNOLOGICO	4	5	20	Extrema	1) Constituir nuevas politicas de trabajo y politicas 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	Alta	Evitar	1) Constituir nuevas politicas de trabajo y politicas 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 TECNOLOGÍA	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 continua con la implementacion de politicas en el Directorio Activo. 2. Actualizacion de Antivirus automatico en todos los equipos. 3. 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 implementado nuevas herramientas tecnologicas. **Evidencia** https://drive.google.com/drive/folders/1U7QJ9J7fbdEcJ4waAKDS8kPuKsTvdrV-k3V	1. Se continua con la implementacion de politicas en el Directorio Activo. 2. Actualizacion de Antivirus automatico en todos los equipos. 3. 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 implementado nuevas herramientas tecnologicas.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**
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. Perdida de credibilidad 5. Posibles hallazgos 6. Perdida de credibilidad 7. Perdida de Recursos 8. Reprocesos 9. Malentendidos del riesgo 10. Llamados de atención por parte de la dirección	TECNOLOGICO	5	3	15	Extrema	1) Eliminacion de cuentas de correos electronicos. 2) Backups de cuentas de correos electronicos.		Correctivo	22	23	22	22	89	0	0	1	3	3	Moderada	Evitar	1) Eliminacion de cuentas de correos electronicos. 2) Backups de cuentas de correos electronicos.		Correctivo	GERENTE DE TECNOLOGÍA	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 continua con el proceso de inactivacion de cuentas de correos una vez haya finalizado el vinculo laboral y se hace respaldo de la informacion	1. Se implementó la sincronización de las cuentas de correos con el directorio activo con el fin de inactivar usuarios una vez se haya finalizado el vínculo laboral. Se realizo respaldo de la información.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**
10	1. Ausencia de inventario de equipos. 2. Ausencia de Bitácora de préstamos y asignación de equipos	Pérdida de equipos informáticos	No tener control sobre que 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	4	3	8	Alta	1) Listado de activos fisicos de tecnologia 2) Correos de asignación de equipos	PREVENTIVO		22	22	22	22	88	0	0	1	3	3	Alta	Evitar	1) Listado de activos fisicos de tecnologia 2) Correos de asignación de equipos	PREVENTIVO		GERENTE DE TECNOLOGÍA	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 continua con el control de equipos de computo por parte de la Gerencia de Tecnologia. A través de la implementacion de la herramienta de mesa de ayuda se puede verificar el listado de equipos y a quien se ha entregado la asignacion. 2. Implementacion del procedimiento GTI-PO-09 administracion de activos TI, Mantenimiento y Licenciamiento.	1. Se continua con el control de equipos de computo por parte de la Gerencia de Tecnologia. A través de la implementacion de la herramienta de mesa de ayuda se puede verificar el listado de equipos y a quien se ha entregado la asignacion.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**
11	1. Ausencia de mecanismos de monitoreo para brechas de la seguridad. 2. falta de controles	Brechas de seguridad informática	Pérdida de disponibilidad del activo de informacion	1. Perdida de reputación 2. Glosas o Multas 3. Perdida de confiabilidad area 4. Hallazgos entes de control 5. Perdida de credibilidad 6. Perdida de Recursos 7. Reprocesos 8. Malentendidos del riesgo 9. Llamados de atención por parte de la dira Dirección	TECNOLOGICO	4	3	8	Alta	Implementar politicas de seguridad de la información que aseguren la integridad de los sistemas de informacion de la FND	PREVENTIVO		5	19	20	20	64	0	0	1	3	3	Alta	evitar	Implementar politicas de seguridad de la información que aseguren la integridad de los sistemas de informacion de la FND	PREVENTIVO		GERENTE DE TECNOLOGÍA	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, en espera aprobacion por parte de Comite de Gerencia y Desempeño.	1. Actualizacion de la Politica de Seguridad de la informacion de acuerdo a los lineamientos de la Norma ISO 27001, aprobada por el Comite de Gerencia y Desempeño. A la espera de la firma del Director Ejecutivo para su publicacion.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**
12	1. Excesos de permisos a 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. Perdida de reputación 2. Glosas o Multas 3. Perdida de credibilidad 4. Hallazgos entes de control 5. Investigaciones disciplinarias 6. Perdida de Recursos 7. Reprocesos 8. Malentendidos del riesgo 9. Llamados de atención por parte de la dira Dirección	TECNOLOGICO	4	3	9	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	Moderada	evitar	1.Actualizaciones 2. Cambios periodicos de contraseñas 3. Capacitar a los funcionarios para la solicitud de requerimientos	Preventivo		GERENTE DE TECNOLOGÍA	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. Unificacion de contraseña de directorio activo con sistema de informacion AZDIgital, cada vez que se solicite cambio de contraseña tambien se debe ingresar una contraseña en este Sistema de Insercion. 2. En la caso del Sistema de Informacion Syoman fue solicitada la implementacion de contraseña de directorio activo, se encuentra programado el modulo de contraseña de Contraseña donde una vez ingrese al sistema por primera vez debe cambiarla. 3. 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.	1. Unificacion de contraseña de directorio activo con sistema de informacion AZDIgital, cada vez que se solicite cambio de contraseña tambien se debe ingresar una contraseña en este Sistema de Insercion. 2. En la caso del Sistema de Informacion Syoman fue solicitada la implementacion de contraseña de directorio activo, se encuentra programado el modulo de contraseña de Contraseña donde una vez ingrese al sistema por primera vez debe cambiarla. 3. 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.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual se mantiene en moderado**
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	1. Perdida de reputación 2. Glosas o Multas 3. Perdida de credibilidad 4. Hallazgos entes de control 5. Investigaciones disciplinarias 6. Perdida de Recursos 7. Reprocesos 8. Malentendidos del riesgo 9. Llamados de atención por parte de la dira Dirección	TECNOLOGICO	4	3	9	Alta	1.Accesos a funcionarios a sistemas de información minimos necesarios. 2. Backups de información para poder restaurar datos en caso de materialización del riesgo	PREVENTIVO		25	25	25	25	100	2	0	1	3	3	Alta	Evitar	1.Accesos a funcionarios a sistemas de información minimos necesarios. 2. Backups de información para poder restaurar datos en caso de materialización del riesgo	PREVENTIVO		GERENTE DE TECNOLOGÍA	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. Todos los sistemas de informacion cuentan con definicion de usuarios, roles, permisos de acuerdo a labor realizada en el proceso al que pertenecen. 2. Se da cumplimiento al requisito de la informacion de acuerdo a lo establecido en los contratos de cada proveedor de Sistemas de Informacion.	1. Todos los sistemas de informacion cuentan con definicion de usuarios, roles, permisos de acuerdo a labor realizada en el proceso al que pertenecen. 2. Se da cumplimiento al requisito de la informacion de acuerdo a lo establecido en los contratos de cada proveedor de Sistemas de Informacion.	22/12/2022	**Revisar los contratos existentes, medidas, contratarlas y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.**

Nota: Todos los riesgos asociados con salud y seguridad en el trabajo (Identificación de peligros y evaluación de los riesgos), para cada proceso se encuentran establecidos en la FORMATO MATRIZ IDENTIFICACIÓN DE PELIGROS, EVALUACIÓN Y CONTROL DE LOS RIESGOS GHH-PO-06-FT-01, donde se evidencia la implementación de los controles aplicables y son gestionados por el área SST de GHH.