GESTIÓN INTEGRAL ORGANIZACIONAL

FORMATO MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL

N°	CAUSAS DESCRIPCIÓN DE LA CAUSA (Debide a.....)	RIESGO	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS DESCRIPCIÓN DE LA CONSECUENCIA (Lo que genera.....)	CLASE DE RIESGO	RIESGO INHERENTE					CONTROLES EXISTENTES							RIESGO RESIDUAL					PLAN DE MANEJO DEL RIESGO						SEGUNDO CUATRIMESTRE (mayo- agosto)		MONITOREO Y REVISION OFICINA CONTROL INTERNO	
						PROBABILIDAD	IMPACTO	NIVEL	VALOR	VALORACIÓN	DESCRIPCION	TIPO DE CONTROL	DO	AP	EF	EV	PUNTAJE (DO+AP+EF+EV)	PROBABILIDAD	IMPACTO	NIVEL	VALOR	VALORACIÓN	CONTROL PROPUESTO O ACCIONES A TOMAR	TIPO DE CONTROL	RESPONSABLE		CRONOGRAMA IMPLEMENTACION ACCIONES		SEGUIMIENTO	EVIDENCIAS Y/O SOPORTES	FECHA	ACCIONES REALIZADAS
																									CARGO	DEPENDENCIA	INICIA	TERMINA				
2	1.Debilidad en la aplicación del procedimiento de Control de Acceso. 2. Desconocimiento de las responsabilidades de los colaboradores frente a roles asiganados a sus usuarios en los diferentes Sistemas de Información.	1. Acceso a información no autorizada.	Todos los colaboradores de la FND, se les asigena a solicitud del líder del proceso un usuario con roles y permisos de acuerdo a las responsabilidades que cumplen dentro del area. Sin embargo, por desconocimiento se pude presentar prestamos de usuarios entre colaboradores.	1.Manipulacion de información no autorizada. 2. Perdida de información 3. Perdida de credibilidad de la Entidad. 4. Posibles materialización de riesgos.	OPERATIVOS	2	3	6	23	Moderada	1. Elaboración del Procedimiento de Control de Acceso. 2. Implementación del Procedimiento de Control de Acceso	Preventivo	25	25	25	25	100	1	2	2	12	Baja	1. Concientizar a los colaboradores FND de la responsabilidad que tienen en el manejo de usuarios asignados en los diferentes Sistemas de Información. 2. Dar a conocer a los colaboradores que los Sistemas de Información de la FND, cuentan con modulo de auditorias donde se puede evidenciar la trazabilidad de las actividades o registros realizados por cada usuario. 3. Solicitud de creacion de usuarios con roles y permisos a través de mesa de ayuda.	Preventivo	Coordinación de Tecnología	Jefatura Administrativa	1/1/2023	1/12/2023	1. Se realizó el envió de pieza de sensibilización a los colaboradores en temas asociados a los roles y responsabilidades de los usuarios, asi mismo se enviaron piezas relacionadas a seguridad de la información asociadas a la norma ISO IEC 27001. 2. Se dio gestión a Tickets generados en Mesa de ayuda sobre creación de usuarios con roles y permisos en los Diferentes Sistemas de Información.	https://drive.google.com/drive/folders/1naf6QBJoa2bF9ev6aJ2Rwy7gKfdCNrA/R?hcpv=dwnm8	22/09/2023	De conformidad con el monitoreo a la matriz de seguridad digital: Se pueden detallar el desarrollo de actividades por parte del proceso de acuerdo con las evidencias soportes; sin embargo: 1.No se evidencia diligenciamiento en la columna idricador: 2. No es claro como se valoran los constroles para lograr que el riesgo residual pase de moderado a bajo. 3. Revisar el riesgo y los controles conforme a la actualización de la Política de Administración del Riesgo aprobada en el Comite Institucional de Gestión y Desempeño del 31 de Julio de 2023.
2	1. Falta de elaboración del Procedimiento Requisitos de Seguridad . 2. Falta de aplicabilidad del Procedimiento Requisitos de Seguridad . 2. Falta de Verificacion de Requisitos de Seguridad en los servicios con los diferentes proveedores.	1. Posible incidencia de Hacking en la entidad.	La Entidad no time definido la forma de controlar los requisitos de seguridad que deben tenerse en cuenta en los sistemas de información que se adquieran en la organización.	1. Manipulación de información no autorizada. 2. Perdida de información. 3. Perdida de credibilidad de la Entidad.	DE TECNOLOGÍA	3		12	34	Extrema	1. Reglas de Seguridad en Firewall. 2. Dispositivos de Seguridad en el Rack de comunicaciones.	Preventivo	25	25	25	25	100	2	2	**4**	**22**	Baja	1. Implementacion del Protocolo IPV6 en la Entidad. 2. Aprobación de la Politica de Seguridad y Privacidad de la Información . 3. Socialización de la Politica de Seguridad y Privacidad de la Información 4. Segmentación de redes para controlar el acceso a invitados y colaboradores de FND	Preventivo	Coordinación de Tecnología	Jefatura Administrativa	1/1/2023	1/12/2023	1. Se realizó envió de piezas de socialización y sensibilización de la politica de seguridad y privacidad de la información, asi mismo se envió una pieza indicando la ubicación especifica de la politica de seguridad y privacidad de la información para que pueda ser consultada cuando sea requerida por los colaboradores de la FND. 2. Se realizó actualizacion de la Politica de Seguridad y privacidad de la información incluyendo la Politica de Seguridad Digital. Esta actualización fué aprobada en Comite de Desempeño y Desarrollo Institucional realizado el 31 de Iulio de 2023. El acta reposa en la	https://drive.google.com/drive/folders/1MvKEIuyeKULA7ayvKGKrxHB67BBeSO?usp=sharing	22/09/2023	De conformidad con el monitoreo a la matriz de seguridad digital: Se pueden detallar el desarrollo de actividades por parte del proceso de acuerdo con las evidencias soportes; sin embargo: 1.No se evidencia diligenciamiento en la columna idricador: 2. No es claro como se valoran los constroles para lograr que el riesgo residual pase de
3	1. Debilidad en la realizacion del respaldo de información de la FND	1. Perdida de información. 2. Reprocesos al interior de la entidad.	Riesgo de perdida de información si no se establecen los controles de seguimiento y verificación de que la información que se maneja en el Drive dispuesto para el almacenamiento de la información no se le hace el respaldo adecuado	1. Perdida de la informacón. 2. Posible materialización de hallazgos parentes de Control. 3. Afectación reputacional de la entidad.	OPERATIVOS	2	2	4	22	Baja	1. Realización de respaldo de información almacenada en el Drive de la entidad.	Preventivo	25	25	25	25		1	2	**2**	**12**	Baja	1. El Profesional de Soporte debe notificar a la Coordinadora de Tecnologia que fue realizado el respaldo del Drive y adjuntar evidencia.	Preventivo	Coordinación de Tecnología	Jefatura Administrativa	1/1/2023	1/12/2023	1. Se realizó el respaldo en este periodo en el Drive de la FND	https://drive.google.com/drive/folders/1mJFzrasJ1f8j_wDb6L0ZbbbJr3GuK3Qp?usp=drive_link	22/09/2023	De conformidad con el monitoreo a la matriz de seguridad digital: Se pueden detallar el desarrollo de actividades por parte del proceso de acuerdo con las evidencias soportes; sin embargo: 1.No se evidencia diligenciamiento en la columna idricador: 2. No es claro como se valoran los constroles para lograr que el riesgo residual pase de
4	1. Indisponibilidad en los Sistemas de Información contratados con terceros	1. Perdida de disponibilidad de la información.	Los Sistemas de Información de la FND son sumistrados a través de contratación con terceros, si no se realiza estricta verificacion en los acuerdos de disponibilidad de servicios se corre riesgos de disponibilidad de información	1. Indisponibilidad de la información. 2. Posible materialización de hallazgos parentes de Control. 3. Afectación reputacional de la entidad.	DE TECNOLOGÍA	2	3	**6**	23	Moderada	1. Los ANS hacen parte integral de los contratos de la Coordinación de Tecnologia. 2. Seguimiento al cumplimiento de envio de copias de seguridad de informacion con los diferentes proveedores	Preventivo	25	25	25	25	100	1	2	**2**	**12**	Baja	1. Se implementa el Procedimiento de Plan de Continuidad. 2. Actualización e implementación del Formato Registro de Copias de Seguridad	Preventivo	Coordinación de Tecnología	Jefatura Administrativa	1/1/2023	1/12/2023	1. Se realiza el seguimiento de los registros de las copias de seguridad enviadas por los proveedores de los sistemas de información (Syxman - AZ Digital) 2. La Coordinación de Tecnologia se encuentra trabajando en la contrucción del BIA (Bussiness Impact Analysis) primera fase de la creación del Plan de Continuidad	https://drive.google.com/drive/folders/2c_ycaDCkcm5MMbkqWFkfrgoqwKzDJ?usp=drive_link	22/09/2023	De conformidad con el monitoreo a la matriz de seguridad digital: Se pueden detallar el desarrollo de actividades por parte del proceso de acuerdo con las evidencias soportes; sin embargo: 1.No se evidencia diligenciamiento en la columna idricador:

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 , donde se evidencia la implementación de los controles aplicables y son gestionados por el área SST de GRH.