	PROCESO **ANALISIS Y MEJORA CONTINUA**	Código: FO-MC-MN-01
		Versión: 2
	MAPA DE RIESGOS DE LA DNBC	Vigente desde:

Identificación Riesgos y priorización de Causas

Nro	Proceso*	Objetivo del proceso	Nombre del Riesgo*	Descripción del Riesgo*	Tipo de Riesgo menú*	Cód Causa*	Causas*	Consecuencias*	PARTICIPANTES P1	P2	P3	P4	P5	P6	P7	Total	Priorización de Causas Prom
1	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	Seguridad Digital	1.1	Manejo inadecuado de la información.	Fuga, pérdida total o parcial de la información considerada como pública clasificada y pública reservada.							10	10	10
1	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	Seguridad Digital	1.2	Información física almacenada sin proteccion.	Pérdida total o parcial de la memoria institucional (registros que formen parte de la misionalidad de la DNBC).							6	6	6
1	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	Seguridad Digital	1.3	Desconocimiento de políticas de seguridad de la información.	Alta ocurrencia de incidentes de seguridad de la información.							5	5	5
1	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	Seguridad Digital	1.4	Deterioro de la información física almacenada en el archivo de gestión.	Demoras o interrupciones de las operaciones de los procesos de la DNBC.							5	5	5
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.1	Falta de planificación de la continuidad del negocio.	Demoras o interrupciones de las operaciones de los procesos de la DNBC.							5	5	5
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.2	Ausencia de redundancias para los sistemas de información.	Demoras o interrupciones de las operaciones de los procesos de la DNBC.							6	6	6
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.3	Capacidad de almacenamiento y procesamiento de la infraestructura tecnológica gestionada inadecuadamente.	Falla en la capacidad de respuesta de la infraestructura tecnológica.							6	6	6
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.4	Cambios en la infraestructura tecnológica sin controlar.	Indisponibilidad de los sistemas de información.							8	8	8
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.5	Falta de soporte por parte del Fabricante de los sistemas de información.	Información erróneamente procesada o entregada al usuario.							5	5	5
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.6	Falta de actualizaciones a los sistemas.	Demoras o interrupciones de las operaciones de los procesos por la indisponibilidad de los activos.							5	5	5
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.7	Infección por malware de los equipos de cómputo y servidores.	Fuga, pérdida total o parcial de la información.							6	6	6
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.8	Ausencia de copias de respaldo.	Pérdida total o parcial de la información almacenada.							6	6	6
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.9	Falta de mantenimiento al hardware que soporta los sistemas.	Daño en la infraestructura física tecnológica por polvo, corrosión, humedad.							6	6	6
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.10	Equipos de cómputo desatentidos y sin bloqueo de sesión.	Fuga, pérdida total o parcial de la información.							7	7	7

	PROCESO ANALISIS Y MEJORA CONTINUA	Código: FO-MC-MN-01
		Versión: 2
	MAPA DE RIESGOS DE LA DNBC	Vigente desde:

Identificación Riesgos y priorización de Causas

Nro	Proceso*	Objetivo del proceso	Nombre del Riesgo*	Descripción del Riesgo*	Tipo de Riesgo menú*	Cód Causa*	Causas*	Consecuencias*	PARTICIPANTES P1	P2	P3	P4	P5	P6	P7	Total	Priorización de Causas Prom
2	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.11	Puertos USB de los equipos de cómputo habilitados para uso.	Fuga, pérdida total o parcial de la información.							7	7	7
3	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confindencialidad de la información por acceso a la red no autorizado.	Afectación de la confindencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	Seguridad Digital	3.1	Falla en los controles de acceso lógico.	Fuga de la información digital transferida por la red de la DNBC.							9	9	9
3	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confindencialidad de la información por acceso a la red no autorizado.	Afectación de la confindencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	Seguridad Digital	3.2	Puntos de red habilitados y sin uso.	Acceso a la información y servicios compartidos en red no autorizado.							5	5	5
3	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confindencialidad de la información por acceso a la red no autorizado.	Afectación de la confindencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	Seguridad Digital	3.3	Uso inadecuado a la información de autenticación secreta (usuario y contraseña).	Fuga de la información digital almacenada y procesada por la infraestructura tecnológica de la entidad.							6	6	6
3	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confindencialidad de la información por acceso a la red no autorizado.	Afectación de la confindencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	Seguridad Digital	3.4	Conexión de equipos de cómputo personales a la red de la DNBC.	Exposición de la plataforma tecnológica a una infección por malware.							5	5	5
4	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	Seguridad Digital	4.1	Políticas de seguridad de la información sin definir.	Alto nivel de ocurrencia de incidentes de seguridad de la información.							6	6	6
4	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	Seguridad Digital	4.2	Falta de revisión y actualización de las políticas general y específicas de seguridad de la información.	Incumplimiento de los requisitos legales y/o contractuales.							6	6	6
4	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	Seguridad Digital	4.3	Falta de comunicación de las políticas general y específicas de seguridad de la información a los Servidores Públicos y Contratistas.	Pérdida de la cultura organizacional en materia de seguridad de la información.							9	9	9
4	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	Seguridad Digital	4.4	Inasistencia de los Servidores Públicos y Contratistas a las jornadas de sensibilización en seguridad de la información.	Alto nivel de ocurrencia de incidentes de seguridad de la información.							6	6	6
5	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad del conocimiento con el que cuentan algunos funcionarios o contratistas del proceso.	Afectación de las operaciones normales de la DNBC debido a la ausencia del personal considerado como crítico para el proceso,y los cuales no cuentan con transferencia de conocimiento ni respaldo, en caso de situaciones administrativas.	Seguridad Digital	5.1	Poca capacidad de contratación de la DNBC.	Incumplimiento de los compromisos y gestión inadecuada del proceso.							6	6	6
5	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad del conocimiento con el que cuentan algunos funcionarios o contratistas del proceso.	Afectación de las operaciones normales de la DNBC debido a la ausencia del personal considerado como crítico para el proceso,y los cuales no cuentan con transferencia de conocimiento ni respaldo, en caso de situaciones administrativas.	Seguridad Digital	5.2	Perfiles de profesionales dificiles de encontrar.	Pérdida de la imagen y reputación de la DNBC.							5	5	5
5	Gestión de Tecnologia Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad del conocimiento con el que cuentan algunos funcionarios o contratistas del proceso.	Afectación de las operaciones normales de la DNBC debido a la ausencia del personal considerado como crítico para el proceso,y los cuales no cuentan con transferencia de conocimiento ni respaldo, en caso de situaciones administrativas.	Seguridad Digital	5.3	Falta de transferencia de conocimiento entre las personales del mismo proceso o área.	Demoras o interrupciones de las operaciones de los procesos por falta del personal capacitado.							9	9	9
																0	
																0	
																0	

	PROCESO ANALISIS Y MEJORA CONTINUA	Código:
		Versión:
	MAPA DE RIESGOS DE LA DNBC	Vigente desde:

				¿Qué puede suceder...?			¿Qué me genera la materialización de esa situación?	¿Qué me genera la materialización de esa situación?				Tenga en cuenta: El riesgo de Corrupción "No se acepta"							Autoevaluación	Seguimiento		¿Qué paso despues de aplicar controles? Riesgo residual		
Nro*	Proceso	Objetivo	Nombre del Riesgo	Descripción del Riesgo	Tipo de Riesgo	Cód. Causa *	Causas (>=7)*	Consecuencias *	Probabilidad	Impacto	Evaluación del Riesgo	Tratamiento*	Nombre y descripción del Control*	Responsable*	Otros responsables que participan en su ejecución*	Periodicidad *	Proposito *	Indicador*	Evidencia*	Fecha / Descripción del resultado obtenido	Fecha / Descripción del seguimiento	Contingencia	Probabilidad	Impacto	Evaluación del Riesgo
1	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	Seguridad Digital	1.1	Manejo inadecuado de la información.	Fuga, pérdida total o parcial de la información considerada como pública clasificada y pública reservada.	Probable	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: 8.1.1 Inventario de activos 8.1.2 Propiedad de los activos 8.2.1 Clasificación de la información 8.2.2 Etiquetado de la información 8.2.3 Manejo de activos Procedimiento gestión de activos: Generar procedimientos para la gestión y manejo adecuado de la información física y digital en la DNBC.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información Gestión Documental	Diario	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	- Procedimiento de gestión de activos de información. - Instructivo de gestión de activos de información.			Uso de la información digitalizada.	Probable	Mayor	Extremo
1	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	Seguridad Digital	1.1	Información física almacenada sin protección.	Pérdida total o parcial de la memoria institucional (registros que formen parte de la misionalidad de la DNBC).	Probable	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: 18.1.3 Protección de registros Adecuar en cada dependencia archivadores para el almacenamiento y archivo adecuado de la información física, por medio de los cuales se pueda controlar su acceso y proteger.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información Gestión Documental	Diario	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	información manejada por el proceso que se encuentre almacenada en archivadores que restrinjan su acceso.			Uso de la información digitalizada.	Probable	Mayor	Extremo
1	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	Seguridad Digital	1.1	Manejo inadecuado de la información.	Fuga, pérdida total o parcial de la información considerada como pública clasificada y pública reservada.	Probable	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: 8.1.3 Uso aceptable de los activos Establecer, implementar y comunicar políticas de seguridad de la información enfocadas a la protección de la información, su clasificación, etiquetado y manejo adecuado.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información Gestión Documental	Diario	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	Manual de políticas especificas de seguridad y privacidad de la información.			Uso de la información digitalizada.	Probable	Mayor	Extremo
2	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.4	Cambios en la infraestructura tecnológica sin controlar.	Indisponibilidad de los sistemas de información.	Posible	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.12.1.2 Establecer e implementar un procedimiento de gestión de cambios en la infraestructura tecnológica a fin de controlar su ejecución.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información	Mensual	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	- Procedimiento de gestión de cambios. - Formato de gestión de cambios.			Uso de copias de seguridad o respaldo de la información.	Posible	Mayor	Extremo
2	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.4	Cambios en la infraestructura tecnológica sin controlar.	Indisponibilidad de los sistemas de información.	Posible	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.12.3.1 Establecer un esquema de respaldo para la información almacenada y procesada en los sistemas de información.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información	Diario	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	- Política de copias de respaldo. - Logs de ejecución de copias de respaldo.			Uso de copias de seguridad o respaldo de la información.	Posible	Mayor	Extremo
2	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.4	Cambios en la infraestructura tecnológica sin controlar.	Indisponibilidad de los sistemas de información.	Posible	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.11.2.4 Diseñar e implementar un plan de mantenimiento preventivo anual para la infraestructura tecnológica física.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información	Anual	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	-Plan de mantenimiento preventivo anual. - Hoja de vida de los equipos.			Uso de copias de seguridad o respaldo de la información.	Posible	Mayor	Extremo
2	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.4	Cambios en la infraestructura tecnológica sin controlar.	Indisponibilidad de los sistemas de información.	Posible	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.12.6.1 Realizar periódicamente un análisis de vulnerabilidades técnicas a los sistemas de información que se usen en la DNBC, para evaluar su exposición ante estas vulnerabilidades. Posteriormente, diseñar el plan de remediación a dichas vulnerabilidades identificadas e implementarlo.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información	Anual	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	-Plan de pruebas de vulnerabilidades. -Plan de remediación.			Uso de copias de seguridad o respaldo de la información.	Posible	Mayor	Extremo
2	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Seguridad Digital	2.4	Cambios en la infraestructura tecnológica sin controlar.	Indisponibilidad de los sistemas de información.	Posible	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.12.6.1 Actualizar el versionamiento o instalación de parches de los sistemas de información usados en la DNBC.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información	Anual	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	-Formato de gestión de cambios aplicado.			Uso de copias de seguridad o respaldo de la información.	Posible	Mayor	Extremo
3	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad de la información por acceso a la red no autorizado.	Afectación de la confidencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	Seguridad Digital	3.1	Falla en los controles de acceso lógico.	Fuga de la información digital transferida por la red de la DNBC.	Probable	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.13.1.1 Controles de redes Establecer las responsabilidades y procedimientos para la gestión de equipos de redes, por parte del Líder o Gestor del proceso Gestión de Tecnología Informática.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información	Anual	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	Configuraciones realizadas en los dispositivos de red.			Desconexión de equipos conectados a la red comprometida.	Probable	Mayor	Extremo
3	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad de la información por acceso a la red no autorizado.	Afectación de la confidencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	Seguridad Digital	3.1	Falla en los controles de acceso lógico.	Fuga de la información digital transferida por la red de la DNBC.	Probable	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.13.1.1 Controles de redes Aplicar restricciones para la conexión de los sistemas y equipos de cómputo a la red de la DNBC, como por ejemplo validación por medio del domino o MAC, Configuración de NAP (Network Access Protection) herramienta de Windows o configuración en el DHCP de listas blancas.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información	Bimestral	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	Configuraciones realizadas en los dispositivos de red.			Desconexión de equipos conectados a la red comprometida.	Probable	Mayor	Extremo
3	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad de la información por acceso a la red no autorizado.	Afectación de la confidencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	Seguridad Digital	3.1	Falla en los controles de acceso lógico.	Fuga de la información digital transferida por la red de la DNBC.	Probable	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: 13.1.2 Seguridad de los servicios de red Restringir la navegación en la red por medio de protocolos no seguros y en los cuales no sea posible el cifrado de la información.	Gestión de Tecnología Informática	Encargado de Seguridad de la Información	Diario	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	Configuraciones realizadas en los dispositivos de red.			Desconexión de equipos conectados a la red comprometida.	Probable	Mayor	Extremo
4	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	Seguridad Digital	4.3	Falta de comunicación de las políticas general y específicas de seguridad de la información a los Servidores Públicos y Contratistas.	Pérdida de la cultura organizacional en materia de seguridad de la información.	Casi Seguro	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.5.1.1 Políticas para la seguridad de la información Establecer e implementar un conjunto de políticas específicas de seguridad de la información y comunicarlas a las partes interesadas de la DNBC.	Dirección General	Gestión de Tecnología Informática Encargado de Seguridad de la Información	Diario	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	Registro de revisión peroódica de las políticas de seguridad de la información.			Uso de copias de seguridad o respaldo de la información.	Casi Seguro	Catastrófico	Extremo
4	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	Seguridad Digital	4.3	Falta de comunicación de las políticas general y específicas de seguridad de la información a los Servidores Públicos y Contratistas.	Pérdida de la cultura organizacional en materia de seguridad de la información.	Casi Seguro	Catastrófico	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información Definir e implementar actividades de formación y sensibilización en seguridad de la información dentro de los programas de capacitación de la DNBC.	Gestión del Talento Humano	Encargado de Seguridad de la Información	Anual	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	Programa de capacitación Listas de asistencia			Uso de copias de seguridad o respaldo de la información.	Casi Seguro	Catastrófico	Extremo
5	Gestión de Tecnología Informática	Propender y mantener la sostenibilidad de la infraestructura tecnológica y de los sistemas de información, con el fin de contribuir al normal desarrollo de las actividades de los procesos de la DNBC, a traves de la ejecución del Plan Estrategico de TI.	Afectación de la disponibilidad del conocimiento con el que cuentan algunos funcionarios o contratistas del proceso.	Afectación de los operaciones normales de la DNBC debido a la ausencia del personal considerado como crítico para el proceso,y los cuales no cuentan con transferencia de conocimiento ni respaldo, en caso de situaciones administrativas.	Seguridad Digital	5.3	Falta de transferencia de conocimiento entre las personales del mismo proceso o área.	Demoras o interrupciones de las operaciones de los procesos por falta del personal capacitado.	Posible	Mayor	Extremo	Reducir	Control aplicable del Anexo A, NTC-ISO-IEC 27001: A.7.1.2 Términos y condiciones del empleo Incluir dentro de los términos del empleo: la responsabilidad de elaborar la documentación relacionada al desarrollo de las actividades y tareas en el proceso o en defecto capacitar a personal del área de manera integral.	Gestión del Talento Humano	Encargado de Seguridad de la Información	Anual	Prevenir	Porcentaje de cumplimiento del plan de tratamiento de riesgos de seguridad de la información.	Política de seguridad de los recursos humanos			Usar personal suplente para el desarrollo de las tareas críticas.	Posible	Mayor	Extremo

El futuro es de todos · Mininterior · DNBC Bomberos Colombia	**PROCESO** **ANALISIS Y MEJORA CONTINUA**	Código: FO-MC-MN-01
		Versión: 2
	MAPA DE RIESGOS DE LA DNBC	Vigente desde:

CRITERIOS PARA CALIFICAR LA PROBABILIDAD

Nivel	Descriptor	Descripción	Frecuencia
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez al año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de 1 vez al año

					Nivel identificado por participante									
Nro	**Nombre de Riesgo**	**Descripción Riesgo**	**Cód Causa**	**Causas**	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**Total**	**Prom**	**Descriptor**
1	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	1.1	Manejo inadecuado de la información.	4							4	4	Probable
2	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	2.4	Cambios en la infraestructura tecnológica sin controlar.	3							3	3	Posible
3	Afectación de la confindencialidad de la información por acceso a la red no autorizado.	Afectación de la confindencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	3.1	Falla en los controles de acceso lógico.	4							4	4	Probable
4	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	4.3	Falta de comunicación de las políticas general y específicas de seguridad de la información a los Servidores Públicos y Contratistas.	5							5	5	Casi Seguro
5	Afectación de la disponibilidad del conocimiento con el que cuentan algunos funcionarios o contratistas del proceso.	Afectación de las operaciones normales de la DNBC debido a la ausencia del personal considerado como crítico para el proceso,y los cuales no cuentan con transferencia de conocimiento ni respaldo, en caso de situaciones administrativas.	5.3	Falta de transferencia de conocimiento entre las personales del mismo proceso o área.	3							3	3	Posible
												0		
												0		

CRITERIOS PARA CALIFICAR LA PROBABILIDAD

Nivel	Descriptor	Descripción	Frecuencia
1	Rara vez	El evento puede ocurrir sólo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez al año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de 1 vez al año

			Nivel identificado por participante									
Nro	Nombre de Riesgo	Descripción Riesgo	P1	P2	P3	P4	P5	P6	P7	Total	Prom	Descriptor
1	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	4							4	4	Probable
2	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	3							3	3	Posible
3	Afectación de la confindencialidad de la información por acceso a la red no autorizado.	Afectación de la confindencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	4							4	4	Probable
4	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	5							5	5	Casi Seguro
5	Afectación de la disponibilidad del conocimiento con el que cuentan algunos funcionarios o contratistas del proceso.	Afectación de las operaciones normales de la DNBC debido a la ausencia del personal considerado como crítico para el proceso,y los cuales no cuentan con transferencia de conocimiento ni respaldo, en caso de situaciones administrativas.	3							3	3	Posible

	PROCESO ANALISIS Y MEJORA CONTINUA	Código: FO-MC-MN-01 Versión: 2
	MAPA DE RIESGOS DE LA DNBC	Vigente desde:

CRITERIOS PARA CALIFICAR EL IMPACTO DEL RIESGO

				Impacto Cuantitativo*				Impacto Cualitativo*							
#*	Riesgo	Código Causa	Consecuencias	1. Afectación presupuestal de la entidad?	2. Afectación en la cobertura del servicio?	3. Genera pago de indemnizaciones a terceros?	4. Genera sanciones con pagos representativos?	5. Puede ocasionar interrupción de las operaciones de la entidad?	6. Puede generar que un ente de control o ente regulador tome medidas?	7. Puede generar para la información de la entidad?	8. Puede tener efectos sobre los Objetivos Institucionales?	9. Puede tener efectos para la imagen institucional?	10. Ocasiona lesiones físicas o pérdida de vidas humanas?	Total	Impacto
1	Afectación de la confidencialidad, integridad y disponibilidad de la información física.	1.1	Fuga, pérdida total o parcial de la información considerada como pública clasificada y pública reservada.	Superior o igual a 20% del presupuesto	Superior o igual a 10% de la cobertura	Superior o igual a 20% del presupuesto	Superior o igual a 20% del presupuesto	2 días o más	Imposición de sanciones	Perdida total de la información critica de la entidad	Incumplimiento de los objetivos institucionales y las metas de gobierno	Afecta la imagen institucional a nivel local por retrasos en la prestación del servicio	No genera lesiones ni perdida de vidas humanas	10	**Catastrófico**
2	Afectación de la disponibilidad de la información almacenada y procesada en la infraestructura tecnológica.	2.4	Indisponibilidad de los sistemas de información,	Superior o igual a 5% del presupuesto	Superior o igual a 5% de la cobertura	Superior o igual a 5% del presupuesto	Superior o igual a 5% del presupuesto	2 días o más	Hallazgos administrativos	Perdida total de la información critica de la entidad	Incumplimiento de los objetivos institucionales y las metas de gobierno	Afecta la imagen institucional a nivel local por retrasos en la prestación del servicio	No genera lesiones ni perdida de vidas humanas	10	**Catastrófico**
3	Afectación de la confindencialidad de la información por acceso a la red no autorizado.	3.1	Fuga de la información digital transferida por la red de la DNBC.	Superior o igual a 1% del presupuesto	Superior o igual a 0,5% de la cobertura	Superior o igual a 0,5% de la cobertura	Superior o igual a 0,5% de la cobertura	2 días o más	Investigación penal, fiscal o disciplinaria	Perdida total de la información critica de la entidad	Incumplimiento de los objetivos institucionales y las metas de gobierno	Afecta la imagen institucional a nivel local por retrasos en la prestación del servicio	No genera lesiones ni perdida de vidas humanas	10	**Catastrófico**
4	Afectación de la confidencialidad, integridad y disponibilidad de la información causada por las personas.	4.3	Pérdida de la cultura organizacional en materia de seguridad de la información.	Superior o igual a 20% del presupuesto	Superior o igual a 10% de la cobertura	Superior o igual a 20% del presupuesto	Superior o igual a 20% del presupuesto	1 día o más	Investigación penal, fiscal o disciplinaria	Perdida total de la información critica de la entidad	Incumplimiento de los objetivos institucionales y las metas de gobierno	Afecta la imagen institucional a nivel local por retrasos en la prestación del servicio	No genera lesiones ni perdida de vidas humanas	10	**Catastrófico**
5	Afectación de la disponibilidad del conocimiento con el que cuentan algunos funcionarios o contratistas del proceso.	5.3	Demoras o interrupciones de las operaciones de los procesos por falta del personal capacitado.	Superior o igual a 0,5% del presupuesto	Superior o igual a 0,5% de la cobertura	Superior o igual a 0,5% del presupuesto	Superior o igual a 0,5% del presupuesto	1 día o más	Hallazgos administrativos	Inconsistencias en la información de algun proceso	Incumplimiento de los objetivos institucionales y las metas de gobierno	Afecta la imagen institucional a nivel local por retrasos en la prestación del servicio	No genera lesiones ni perdida de vidas humanas	10	**Catastrófico**

#*	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.
1	Mayor	Moderado	Mayor	Mayor	Mayor	Mayor	Catastrófico	Mayor	Menor	Insignificante
2	Moderado	Menor	Menor	Menor	Mayor	Menor	Catastrófico	Mayor	Menor	Insignificante
3	Menor	Insignificante	Insignificante	Insignificante	Mayor	Moderado	Catastrófico	Mayor	Menor	Insignificante
4	Mayor	Moderado	Mayor	Mayor	Moderado	Moderado	Catastrófico	Mayor	Menor	Insignificante
5	Insignificante	Insignificante	Insignificante	Insignificante	Moderado	Menor	Menor	Mayor	Menor	Insignificante

#*	Catastrófico	Mayor	Moderado	Menor	Insignificante	Catastrófico	Mayor	Moderado	Menor	Insignificante	IMPACTO*
1	1	6	1	1	1	Catastrófico	Mayor	Moderado	Menor	Insignificante	Catastrófico
2	1	2	1	5	1	Catastrófico	Mayor	Moderado	Menor	Insignificante	Catastrófico
3	1	2	1	2	4	Catastrófico	Mayor	Moderado	Menor	Insignificante	Catastrófico
4	1	4	3	1	1	Catastrófico	Mayor	Moderado	Menor	Insignificante	Catastrófico
5	0	1	1	3	5		Mayor	Moderado	Menor	Insignificante	Mayor

CRITERIOS PARA CALIFICAR EL IMPACTO														
#	Riesgo	Consecuencias	¿Afecta al grupo de funcionarios del proceso?	¿Afecta el cumplimiento de las metas y objetivos de la dependencia?	¿Genera pérdida de confianza de la entidad, afectando su reputación?	¿Generan pérdida de recursos a la entidad?	¿Afecta la generación de productos o la prestación de servicios?	¿Da lugar al detrimento de calidad de vida de la comunidad por la pérdida de bienes o servicios o los recursos públicos?	¿Genera pérdida de la confidencialidad, disponibilidad e integridad de la información de la entidad?	¿Da lugar a procesos sancionatorios, disciplinarios y/o fiscales?	¿Genera pérdida de credibilidad del sector?	¿Ocasiona lesiones físicas o pérdida de vidas humanas?	Total	Impacto
1	Afectación de la confidencialidad, integridad y disponibilidad de la información física manejada por los procesos de la DNBC.	Fuga, pérdida total o parcial de la información considerada como pública clasificada y pública reservada.	Si	Si	Si	Si	Si	No	Si	Si	Si	No	8	Mayor
2	Afectación de la disponibilidad de la información almacenada y procesada en los sistemas de información, servidores, bases de datos de la DNBC, debido a una falla tecnológica.	Indisponibilidad de los sistemas de información,	Si	Si	Si	Si	Si	No	Si	Si	Si	No	8	Mayor
3	Afectación de la confindencialidad de la información de la DNBC provocada por un acceso no autorizado a la red de la DNBC y a los servicios de procesamiento y almacenamiento de información.	Fuga de la información digital transferida por la red de la DNBC.	Si	Si	Si	Si	Si	No	Si	Si	Si	No	8	Mayor
4	Afectación de la confidencialidad, integridad y disponibilidad de la información de la DNBC, debido a un incumplimiento de las políticas de seguridad de la información por parte de los Servidores Públicos, Contratistas y todo aquel con acceso a la información de la DNBC.	Pérdida de la cultura organizacional en materia de seguridad de la información.	Si	Si	Si	Si	Si	No	Si	Si	Si	No	8	Mayor
5	Afectación de las operaciones normales de la DNBC debido a la ausencia del personal considerado como crítico para el proceso,y los cuales no cuentan con transferencia de conocimiento ni respaldo, en caso de situaciones administrativas.	Demoras o interrupciones de las operaciones de los procesos por falta del personal capacitado.	Si	Si	Si	No	Si	No	Si	Si	Si	No	7	Mayor