DIRECCIÓN GENERAL
DE SANIDAD MILITAR

PLAN DE CONTINUIDAD DEL NEGOCIO

2025

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Diciembre 2024	Versión Inicial. Elaboración por primera vez del documento. NOTA PROASIG - PROPLAES: Este Plan fue aprobado en sesión de Comité de Gestión y Desempeño Institucional, del que hacen parte el Director General de Sanidad Militar, los Subdirectores de Salud, Técnico y de Gestión, y Administrativo y Financiero de la DIGSA, los Directores de Sanidad del Ejército y Armada Nacional, Jefatura Salud de la Fuerza Aérea y los Coordinadores de Grupo de Planeación Estratégica, Asuntos Legales y Seguimiento y Evaluación de la DIGSA; y documentado mediante Acta N° 0124014880202 , de fecha -30 de diciembre de 2024

CONTROL DE APROBACIÓN

Aprobó:	Comité de Gestión y Desempeño Institucional Acta No. 0124014880202 de 30 de diciembre de 2024
Revisó:	TC. Jorge Darwin Guevara Guerrero Coordinador Grupo Sistema Integral de Tecnologías de la Información y Comunicación DIGSA PD. Ángela María Tofiño Saavedra Coordinadora Grupo Asuntos Legales DIGSA PD. Alexandra Martínez Vargas Coordinadora Grupo de Planeación Estratégica DIGSA Representante de la Alta Dirección TASD. Yamile López Gestor de Calidad de Grupo Sistema Integral de Tecnologías de la Información y Comunicación DIGSA
Elaboró	PD. Roberto Rodríguez Perdomo Gestor Seguridad de la Información del Grupo Sistema Integral de Información – Tecnologías de la Información y las Comunicaciones DIGSA

Contenido

1. Presentación 5
2. Objetivo 5
3. Alcance 5
4. Definiciones 6
5. Políticas 7
6. Estrategias de Recuperación 10
7. Identificar Activos o Sistemas Críticos de Ti 13
8. Identificación de Procesos Críticos 14
9. Roles y Responsabilidades 15
10. Actividades del Plan de Continuidad del Negocio 16
11. Identificación De Amenazas 16
12. Bibliografía 18

LISTA TABLAS

Tabla 1. Posibles Eventos y Estrategias de Recuperación 9
Tabla 2. Posibles pruebas de recuperación de TI 12
Tabla 3. Identificación de Activos Críticos 13
Tabla 4. Identificación de Procesos Críticos 14
Tabla 5. Matriz de Roles y Responsabilidades 15
Tabla 6. Actividades del Plan para la Vigencia 2025 16

LISTA ILUSTRACIONES

Ilustración 1. Diagrama de dependencia. 14
Ilustración 2. Fuentes de Amenazas 18

1. Presentación

La Gestión de la Continuidad del Negocio (GCN) es un proceso estratégico que garantiza la capacidad de una organización para continuar operando en caso de incidentes o interrupciones disruptivas. Su objetivo principal es minimizar el impacto de estos eventos y restaurar las operaciones críticas en el menor tiempo posible. Ante la creciente necesidad de asegurar la continuidad de los servicios y la protección de la información, la DIGSA ha implementado un plan de GCN desde el 1 de junio de 2021. Este plan, alineado con la política de gobierno digital, la dimensión 3 del MIPG, el plan de desarrollo y las políticas de seguridad informática institucionales, busca asegurar la continuidad de los procesos críticos de la organización.

El plan de GCN de la DIGSA identifica los procesos críticos, evalúa los posibles riesgos y define las acciones necesarias para garantizar su continuidad. Al integrar los requisitos de la GCN con otros aspectos como seguridad de la información, operaciones, personal y logística, se asegura una respuesta integral ante cualquier eventualidad.

Beneficios de la GCN para la DIGSA:

- Minimización de riesgos: Identificación y mitigación de amenazas que puedan afectar las operaciones.
- Protección de activos: Salvaguarda de la información y los sistemas críticos.
- Continuidad de los servicios: Mantenimiento de la prestación de servicios a los usuarios.
- Cumplimiento normativo: Adhesión a los requisitos legales y regulatorios.
- Mejora de la reputación: Demostración de un compromiso con la resiliencia organizacional.
- Al implementar la GCN, la DIGSA demuestra su compromiso con la protección de los intereses de sus usuarios y garantiza la continuidad de sus operaciones, incluso en situaciones adversas.

2. Objetivo

Garantizar la continuidad del negocio asegurando que los procesos críticos de la Dirección General de Sanidad Militar, no se vean interrumpidos por Amenazas, desastres o incidentes. A través de la identificación de riesgos y la protección de los activos de la información, la minimización del tiempo de inactividad y la continuidad de las operaciones. Esta práctica, complementada por las buenas medidas de seguridad y privacidad de la información.

3. Alcance

El Plan de Continuidad de Negocio en Tecnologías de la Información definido en este documento está asociado al proceso de Gestión Tecnológica, para el restablecimiento de los sistemas de información e infraestructura tecnológica que soportan los procesos misionales, dependencias y grupos que conforman la estructura organizacional de la entidad.

Alcance:

- Identificación de activos críticos: Determinar las aplicaciones, sistemas y datos esenciales para las operaciones.
- Definición de tiempos de recuperación: Establecer plazos máximos para restaurar los servicios y evitar pérdidas significativas.
- Desarrollo de procedimientos: Crear guías detalladas para responder a diferentes tipos de incidentes y recuperar los sistemas afectados.

- Capacitación del personal: Asegurar que el personal clave conozca y pueda ejecutar el plan en caso de emergencia.
- Pruebas y mantenimiento: Implementar un programa regular de pruebas y actualizaciones para garantizar la efectividad del plan.

Beneficios:

- Minimización de pérdidas: Reducción de las consecuencias financieras y de reputación asociadas a interrupciones del servicio.
- Mayor resiliencia: Aumento de la capacidad de la organización para enfrentar eventos disruptivos.
- Cumplimiento normativo: Adhesión a los estándares de seguridad y continuidad del negocio.

4. Definiciones

Activación:	Acto de declarar que los acuerdos de la entidad para la continuidad de negocio deben llevarse a la práctica con el fin de continuar la entrega de productos o servicios clave.
Activos de información:	Es aquel elemento de información que tiene valor para la Dirección General de Sanidad Militar-DIGSA, el cual recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida o soportada por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, talento humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.
Amenaza:	Evento que puede desencadenar un incidente produciendo daños materiales o inmateriales a la Entidad.
Análisis de impacto al negocio:	Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas.
Confidencialidad:	Garantía en que se acceda a la información de la compañía únicamente por los usuarios autorizados, por lo tanto, no deberá estar disponible ni será revelada a individuos, procesos u organizaciones sin la respectiva autorización. El conocimiento o divulgación de la información sin autorización impacta negativamente a la Dirección General de Sanidad Militar-DIGSA.
Continuidad del negocio:	Capacidad de la Entidad para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.
Desastre:	Problema o evento no planificado, cuya consecuencia es la interrupción de los procesos de negocio durante un período de tiempo, superior a lo que la Entidad puede soportar sin sufrir perjuicios considerables para el negocio.
Disponibilidad:	La información manejada en la compañía deberá estar disponible, en el momento y forma que se requiera, dejando un registro del suministro de la misma y realizando el seguimiento pertinente del uso que se da a dicha información.
Estrategia de recuperación:	Secuencia de actividades con el fin de brindar continuidad de la operación de los procesos en una contingencia de impacto menor o mayor.
Evento:	Ocurrencia o cambio de un conjunto particular de circunstancias.

Impacto:	Es la consecuencia de la materialización de una amenaza sobre un activo.
Incidente:	Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar una interrupción o una reducción en la calidad de ese servicio.
Integridad:	Exactitud y completitud de la información, esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.
Propietario del activo de información:	Grupo de trabajo, Oficina, Dirección o Delegatura, que tiene como responsabilidad velar por la protección del activo de información. Tiene responsabilidad de controlar la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.
Riesgo:	Estimación del grado de exposición de un activo a que una amenaza se materialice sobre él, causando daños a la Entidad.
Trabajo Remoto:	Desempeño de un trabajo de manera regular en un lugar diferente del centro de trabajo habitual, generalmente empleando medios informáticos.
Vulnerabilidad:	Debilidad o falta de control asociada a un proceso o recurso que puede ser explotada provocando un daño sobre dicho proceso.

5. Políticas

5.1	El propósito de este plan es activar la ejecución de la recuperación de la operación de TI de Dirección General de Sanidad Militar - DIGSA, en el evento o situación que se interrumpan sus actividades normales y fallen los requerimientos mínimos de operación de los sistemas de información e infraestructura tecnológica.
5.2	La Dirección General de Sanidad Militar - DIGSA tiene como responsabilidad evaluar la necesidad y requerimientos que debe tener preparados para responder ante un evento de interrupción con el propósito de asegurar la disponibilidad de los sistemas de información, la infraestructura e integridad de los datos. Por lo tanto, es importante establecer 3 objetivos específicos.
5.3	Definir los roles y las responsabilidades a los funcionarios del Grupo de Recursos Informáticos en la aplicación del Plan de Continuidad del Negocio, estrategia de recuperación tecnológica y responsables de los activos de información de otras dependencias.
5.4	Asegurar que los procedimientos de recuperación de la infraestructura tecnológica de la Entidad, establecida dentro estrategia de recuperación sean ejecutados frente a un evento de interrupción.
5.5	Establecer procedimientos de recuperación viables en términos de costo-beneficio que permita restablecer la disponibilidad de la información para la Entidad.
5.6	Los roles y responsabilidades que puede asignar la Entidad en caso que suceda un evento de interrupción con afectación significativa a la disponibilidad de la infraestructura tecnológica de Dirección General de Sanidad Militar - DIGSA, con el fin de actuar y tomar decisiones teniendo en cuenta el grado de afectación.
5.7	Líder principal de la estrategia de recuperación de TI: Directivo de Dirección General de Sanidad Militar - DIGSA o quien haga sus veces, con capacidad para la toma de decisiones.

5.8	Líder Alterno de la Estrategia de recuperación: Directivo de la Dirección General de Sanidad Militar-DIGSA o quien haga sus veces, con capacidad para la toma de decisiones ante situaciones críticas con conocimiento general de los sistemas de información e infraestructura tecnológica de la Entidad. Apoyará al Líder principal en la toma de decisiones. • Realizará las mismas tareas del líder principal, en caso de estar ausente este.
5.9	Equipo de Recuperación Tecnológica: Este equipo deberá estar conformado por funcionarios del grupo de Tecnologías de la Información con conocimientos en gestión tecnológica o que dirijan procesos de gestión tecnológica. De igual forma, pueden ser funcionarios de otras dependencias con las capacidades y conocimientos en aspectos de tecnología, quienes bajo la coordinación y orientación del Líder principal de Recuperación Tecnológica, deberán evaluar los daños causados por cualquier tipo de siniestro para ejecutar la recuperación de la infraestructura, el hardware, software y las telecomunicaciones necesarias para garantizar la operación de los procesos en las dependencias de la Dirección General de Sanidad Militar-DIGSA. • Evaluar la disponibilidad de la infraestructura de procesamiento de información. • Coordinar el restablecimiento de la infraestructura tecnológica necesaria para la operación en continuidad de los procedimientos críticos. • Verificar la disponibilidad de la infraestructura de comunicaciones necesaria para la recuperación de las aplicaciones en el centro de operación en contingencia y el centro de cómputo alterno. • Verificar la disponibilidad de requerimientos de Hardware y Software necesarios para el centro de cómputo alterno. • Coordinar y ejecutar las labores de restauración de hardware, sistema operativo, aplicaciones, y bases de datos que soportan los procedimientos críticos de la Entidad. • Comunicar y explicar a todos los usuarios internos las limitaciones con las cuales tendrán que desempeñar sus funciones según sea el caso. • Coordinar las actividades necesarias para la creación y configuración de usuarios en el sistema operativo y/o aplicación. • Coordinar la correcta operación del Hardware y Software de comunicaciones requeridas por las aplicaciones críticas. • Soportar a los equipos en continuidad en cualquier requerimiento de Hardware o Software, comunicando al Líder de Continuidad la necesidad de contratación o compra, para su debido trámite. • Realizar la restauración de la última copia disponible de la información, sistemas operativos, bases de datos y aplicaciones de la Dirección General de Sanidad Militar-DIGSA, en caso de presentarse un evento de interrupción significativo que afecte la integridad y disponibilidad de la información y sea necesaria la restauración en instalaciones de procesamiento diferentes con las que cuenta la Entidad. Comité de seguridad de la información: responsable de dar soporte a los equipos de continuidad de todas las áreas, en la definición, implementación, pruebas y

	actualización de la Dirección General de Sanidad Militar-DIGSA, para los procesos o áreas que estén bajo su responsabilidad. Dar soporte a los Líderes de Procedimiento, en la identificación y actualización del nivel de riesgo de Seguridad de la Información. • Monitorear la efectividad de los controles de seguridad física y lógica de las instalaciones de procesamiento de información, el acceso, respaldo de la información. • Verificar la funcionalidad y efectividad de los controles en las fases de planeación, alerta, transición, recuperación y vuelta a la normalidad con el fin de que se salvaguarde la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad. • Coordinar las pruebas que permitan evaluar los controles de seguridad de la información, luego de la activación de las estrategias de recuperación. Teniendo en cuenta los posibles riesgos de continuidad del negocio que se pueden presentar a nivel de infraestructura tecnológica, en la siguiente descripción, se detallan las posibles estrategias enfocadas a la recuperación de la Entidad que podrán ser evaluadas, implementadas y aprobadas por la Alta Dirección, según la situación contingente que se pueda presentar.

Tabla 1. Posibles Eventos y Estrategias de Recuperación

Evento	Descripción	Estrategia
Desastre, pérdida total de sitio	Este evento integra todos los eventos que causen daños a los funcionarios, a la infraestructura física de la sede principal y a la infraestructura tecnológica de la Entidad.	- Recuperación de proceso tecnológico que soporta la operación de negocio. - Traslado de la operación tecnológica, bajo los procedimientos de un Plan de Recuperación de Desastres.
		- Recuperación de procesos mediante la ejecución de ER - Estrategias de Recuperación y estrategias de continuidad, bajo el escenario de afectación de sitio (traslado a sitio de terceros, teletrabajo o activación de Centro Alterno de Operaciones).

Evento	Descripción	Estrategia
Daño de infraestructura tecnológica	Afectación parcial o total de la infraestructura tecnológica disponible en el Centro de Datos.	- Recuperación de proceso tecnológico que soporta la operación de negocio. - Traslado de la operación tecnológica, bajo los procedimientos de un Plan de Recuperación de Desastres.
Falla de proveedores críticos	Incumplimiento de los servicios contratados, afectando la operación.	- Los supervisores del contrato deberán validar la respuesta de los proveedores críticos de sus procesos, establecer cláusulas de continuidad y contingencia, establecer ANS (acuerdos de nivel de servicio) para operación normal y en contingencia; realizar seguimiento a los ANS establecidos.

Fuente: Elaboración propia SISAM

6. Estrategias de Recuperación

6.1	Las estrategias de recuperación que se describen a continuación se presentan como un referente para la Entidad, con el fin de ser evaluadas por parte de la Alta Dirección de la Entidad aquella que se ajuste a las necesidades actuales y futuras de la Dirección General de Sanidad Militar-DIGSA, con relación a la continuidad de carácter tecnológico de la Entidad en caso de presentarse un evento de interrupción mayor.
6.2	Restauración de la infraestructura tecnológica en un nuevo centro de datos.
6.3	Consiste en que luego de la evaluación de los daños, en caso de que la afectación sea muy significativa y no se cuente con instalaciones de procesamiento de información, se requiera restaurar la infraestructura en un nuevo centro de datos. Para poder activar la estrategia de recuperación es necesaria previamente realizar las siguientes actividades: • Tener actualizado el inventario de hardware, software de la Entidad, principalmente el de dispositivos de red e infraestructura tecnológica con el fin de solicitar al proveedor de los equipos o prestador de los servicios equipos con características similares. • Realizar la contratación de acuerdo a las políticas definidas por la Dirección General de Sanidad Militar-DIGSA. • Restaurar con una copia de respaldo de las bases de datos, aplicaciones, sistemas operativos e información con el fin de restablecerlas en el nuevo centro de datos. • Establecer la topología de la red del nuevo Centro de Datos. • Verificar la disponibilidad de las aplicaciones e información en el nuevo Centro de Datos.

	• Verificar la conexión entre el Centro de Datos Principal y el Centro Alterno de Procesamiento de Datos. • Monitorear y verificar la funcionalidad y eficacia de los controles de seguridad lógica de la infraestructura del Centro Principal de Procesamiento de Datos, dando continuidad a los controles que salvaguarden la seguridad de la información. • Realizar pruebas de conexión desde la sede alterna destinada por la Entidad que le permitan simular eventos de interrupción, evaluando tiempos de restauración y recuperación de los procesos críticos de la Entidad. • Verificar la disponibilidad de las aplicaciones y la información restaurada. • Validar que los funcionarios que se encuentran en el Centro Alterno de Operaciones (CAO) o en el sitio de recuperación operativa designada, puedan acceder normalmente a la información y las aplicaciones definidas en los elementos mínimos de recuperación de cada uno de los procedimientos. • Monitorear y verificar la disponibilidad de las aplicaciones, unidades de red, repositorios de información que requieran los procesos críticos de la Entidad. Replicación de la Información en un Centro Alterno de Datos (CAD): Esta estrategia de interrupción puede activarse en el evento en el que el Centro de Datos Principal, presente una afectación mayor que no permita la conexión a los servidores y por ende genere indisponibilidad de las aplicaciones y la información que está alojada en el Centro de Datos de la Entidad, redireccionando el tráfico de datos al Centro Alterno de Datos (CAD). Para activar la estrategia de recuperación es necesaria tener en cuenta las siguientes actividades: • Realizar el cambio de línea host, re- direccionando el tráfico de datos del Centro de Datos Principal al Centro Alterno de Datos (CAD). • Monitorear y verificar la funcionalidad y eficacia de los controles de seguridad lógica de la infraestructura del Centro Alterno de Datos (CAD), dando continuidad a los controles que salvaguarden la seguridad de la información. • Realizar pruebas de conectividad desde la sede de la Procuraduría Principal, los Puntos de Atención (Procuradurías Regionales) y/o el Centro Alterno de Operaciones (CAO), validando que en caso de contingencia se pueda dar continuidad a los servicios prestados por la Dirección General de Sanidad Militar-DIGSA.
6.4	Aprovisionamiento de los servicios en la nube (CLOUD): Consiste en realizar la replicación en línea o definir la periodicidad de ejecución de las copias de respaldo remotamente a los servidores virtuales alojados en la nube de las aplicaciones, bases de datos de las aplicaciones e información crítica. Para poder activar la estrategia de recuperación es necesaria previamente realizar las siguientes actividades: • Realizar la evaluación de los recursos tecnológicos necesarios a nivel de almacenamiento, gestión de la capacidad futura de procesamiento, controles de seguridad física y lógica, niveles de escalamiento, niveles de disponibilidad de la infraestructura, redundancia de la infraestructura en servidores virtuales alojados en una nube privada y demás condiciones que la Dirección General de Sanidad Militar-DIGSA, considere necesarios. • Solicitar el presupuesto para la siguiente vigencia con el fin de iniciar el proceso de contratación del servicio de CLOUD para la replicación de la data almacenada en el Centro de Datos Principal de la Entidad.

	• Realizar la gestión contractual con el proveedor de acuerdo con las políticas de la Entidad.
6.5	Las pruebas se deberán realizar de acuerdo con el cronograma de ejecución de pruebas a la estrategia de recuperación tecnológica y el alcance de los escenarios de recuperación establecida por la Entidad. Estos serán los posibles a probar: • Pérdida de un canal de telecomunicaciones de la Entidad. • Interrupción en el suministro eléctrico. • Interrupción del aire acondicionado central en el DATACENTER. • Desastre natural con destrucción parcial o total de las instalaciones de la sede principal.
6.6	A continuación, se identifican los tipos de pruebas que pueden ser aplicados por Entidad.

Tabla 2. Posibles pruebas de recuperación de TI

Tipo de Prueba	Descripción	Frecuencia sugerida de ejecución
Escritorio	Estas pruebas son realizadas por la Grupo de Recursos Informáticos donde se revisan las estrategias de recuperación simulando un escenario a seguir. Aquí básicamente se realizan pruebas tales como el árbol de llamadas con el fin de verificar que los funcionarios que hacen parte de la activación del plan tienen claro su rol y a quienes comunicar.	Según se requiera
Componente / Modular	Prueba de validación de un elemento específico del plan, en forma aislada. Ejemplo: árboles de llamadas, información del directorio de continuidad, recuperación de un aplicativo específico, activación de canales alternos de comunicación, entre otros.	Según se requiera
Respaldo	Se valida de forma colectiva la disponibilidad de las aplicaciones y/o sistemas de información, estas pruebas se pueden realizar de forma independiente por proceso.	Periódicamente
Simulaciones	Integra varios tipos de procedimientos críticos/o áreas dentro de la organización, bajo un escenario “artificial”. Por ejemplo, áreas como: evacuación, comunicación, procesos, TI, proveedores, entre otras. Puede o no ejecutarse en el ambiente alterno.	Al menos cada dos años
Funcional / actividades críticas	Prueba en el ambiente alterno establecido, de una o más actividades críticas, por un periodo preestablecido de tiempo. Lo anterior, sin generar impacto en la operación normal.	Al menos una vez al año

Fuente: Elaboración propia SISAM

7. Identificar Activos o Sistemas Críticos de Ti

Los sistemas de tecnologías de información pueden ser muy complejos debido a la gran cantidad de interdependencias que pueden tener en elementos de software y de hardware. En esta actividad se trata de analizar los diferentes sistemas de TI con el fin de determinar las funciones o servicios críticos que se desprenden de ellos y también se busca identificar elementos críticos requeridos para realizar estas funciones o prestar estos servicios.

La tabla siguiente muestra los niveles de criticidad, que contempla un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema.

Tabla 3. Identificación de Activos Críticos

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
Aplicaciones	Sistema de Control de flujo de documentos, Correo electrónico	B	3	Contenedor de aplicaciones
Web	Sitio web Entidad	A	1	Capa de presentación
Base de Datos	SQL nómina	A	1	Contenedor de aplicaciones en SQL
Seguridad de Información	Firewall, CORE, File Server, Web server, Switch Core.	A	1	Servicio de firewall de la Entidad
Sistemas de Almacenamiento	NAS (Network, Área, Storage)	A	3	Capacidad de almacenamiento en la NAS
Comunicaciones	Acceso Local a Internet, LAN server, Red WAN, Red LAN	C	4	Comunicación de Internet del usuario local
Cuartos de Máquinas	Centro de Datos	A	1	Servicio de Centro de datos de la Entidad
Proveedores de Aplicaciones y/ o comunicaciones	Interno/externo	B	2	Desarrollo Interno o contratado por externos. Canales de Comunicaciones
Recurso Humano	Internos/externos	C	3	Profesionales encargados de administrar las infraestructuras de la Entidad.

Fuente: Elaboración propia SISAM

8. Identificación de Procesos Críticos

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla.

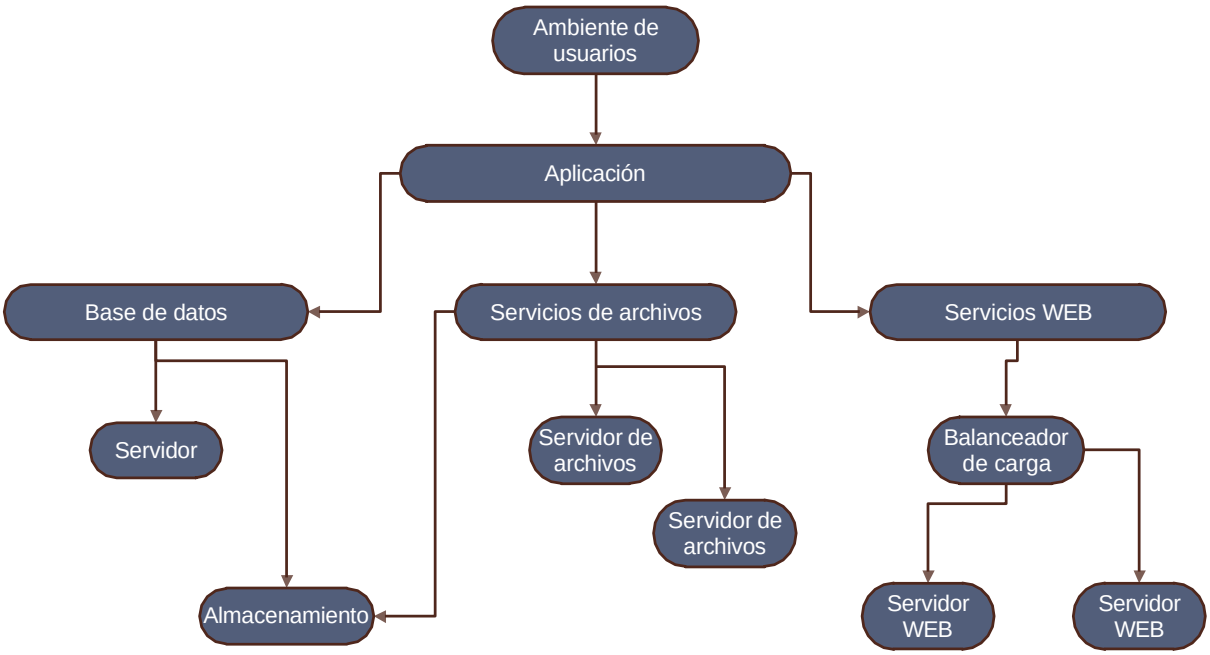
Tabla 4. Identificación de Procesos Críticos

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse.
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

Fuente: Elaboración propia SISAM

Una vez identificados los procesos críticos del negocio, se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios. Como complemento de esta actividad (identificación de activos) se realiza, el diagrama de dependencia que nos indican la conformación y criticidad de ciertos elementos de un sistema, tal como se muestra en la Figura No.1.

Ilustración 1. Diagrama de dependencia.



Fuente: Elaboración propia SISAM

9. Roles y Responsabilidades

Tabla 5. Matriz de Roles y Responsabilidades

MATRIZ DE ROLES Y RESPONSABILIDADES					
ITEM	ROLES Y/O TAREAS ASIGNADAS	RESPONSABLE DE CADA AREA DE TRABAJO EN SISAM			
		ÁREA DE OPERACIONES TIC	ÁREA DE GOBIERNO TIC	ÁREA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	ÁREA GESTIÓN DE SISTEMAS DE INFORMACIÓN, APLICACIONES Y BASE DE DATOS
1	INFRAESTRUCTURA	PD YEISON YARA GUEVARA TASD.GUSTAVO TORRES FORERO TASD.CRISTIAN RODRÍGUEZ DELGADO			
2	TELECOMUNICACIONES				
3	SEGURIDAD INFORMÁTICA				
4	PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP)				
5	OFICIAL SEGURIDAD INFORMATICA			PD. ROBERTO RODRÍGUEZ PERDOMO	
6	INNOVACION, GESTIÓN, SEGUIMIENTO Y MEJORA CONTINUA		SS. JULIAN ANDRES AGUEDELO PD. JULIO SALGADO TASD. YAMILE LÓPEZ TASD. MARYORI TATIANA LEIVA UBILLUS AASD. LINDA RODRÍGUEZ VÁSQUEZ. PS. INGRID MARTINEZ GUEVARA PS. KAREN MAESTRE		
7	MESA DE SERVICIO				
8	GOBIERNO DIGITAL				
9	CATALOGO DE SERVICIOS				
10	INVENTARIO				
11	CONTROL DE ACCESO				
12	SAP (mantenimiento SAP)				
13	GESTIÓN MESA DE SERVICIO				
14	ZENDESK (Enfermeras profesionales-apoyo funcional con los proveedores).				
15	GESTIÓN BASE DE DATOS				TC. JORGE GUEVARA YARA PD. ROZ MARY ORIGUA HUERTO PD. JUAN ORLANDO RAMOS PS. NESTOR GOMEZ GOMEZ PS. WILSON PEREZ
16	GESTIÓN DE APLICACIONES				
17	GESTIÓN DE SISTEMAS DE INFORMACIÓN				
18					
19					
20					

Fuente: Elaboración propia SISAM

10. Actividades del Plan de Continuidad del Negocio

En la Dirección General de Sanidad Militar se definen las actividades a desarrollar con el objetivo de minimizar el impacto de cualquier interrupción de los servicios, alojando servicios en la nube y garantizando la continuidad del negocio.

Tabla 6. Actividades del Plan para la Vigencia 2025

					Fecha Programada	
ESTRATEGIA / EJE	Gestión	Actividades	Producto	Responsable	Fecha Inicial	Fecha Final
Alojar Servicios en la Nube	Implementar en la DIGSA la alta disponibilidad de servicios en la Nube	Realizar pruebas de continuidad de los servicios críticos alojados en la Nube	Alcanzar alta disponibilidad en el servicio	Área Seguridad de la Información-AREIN	05/03/2025	31/12/2025
Contingencias y Medidas de Seguridad	Implementar políticas de control de acceso	Autenticación del doble factor en los usuarios de la DIGSA	Alcanzar un alto Porcentaje de usuarios que utilicen el doble factor de autenticación.	Área Seguridad de la Información-AREIN	05/03/2025	31/12/2025
Monitoreo de Redes y Sistemas	Realizar monitoreo en tiempo real de redes y sistemas	Detectar a través de un software actividades sospechosas	Mitigar las vulnerabilidades y alertas de seguridad detectadas.	Área Seguridad de la Información-AREIN	05/03/2025	31/12/2025
Educación y Capacitación	Capacitar al personal de la DIGSA	Dictar charlas relacionadas con las buenas prácticas de las medidas de ciberseguridad	Capacitar al 100% del personal en ciberseguridad.	Área Seguridad de la Información-AREIN	05/03/2025	31/12/2025

Fuente: Elaboración propia SISAM

11. Identificación De Amenazas

Las amenazas pueden ser el resultado de actos deliberados o mal intencionados que afectan los activos de los procesos. Las organizaciones enfrentan numerosas amenazas comunes tales como el potencial de falla de un servidor o la pérdida del fluido eléctrico; pero también enfrentan otras amenazas que son específicas para esta entidad o son únicas consideradas desde el punto de vista de su impacto potencial.

Para la identificación de las amenazas a las que pueden enfrentarse los activos de TI se realizarán entrevistas con expertos de DIGSA, quienes suministrarán información sobre cuáles son las amenazas con mayor impacto

desde la perspectiva de continuidad del servicio o servicios de TI, las que podrían llegar a afectar la continuidad de las operaciones de TI, y, por consiguiente, podrían causar una pérdida financiera o afectación de la imagen de la compañía.

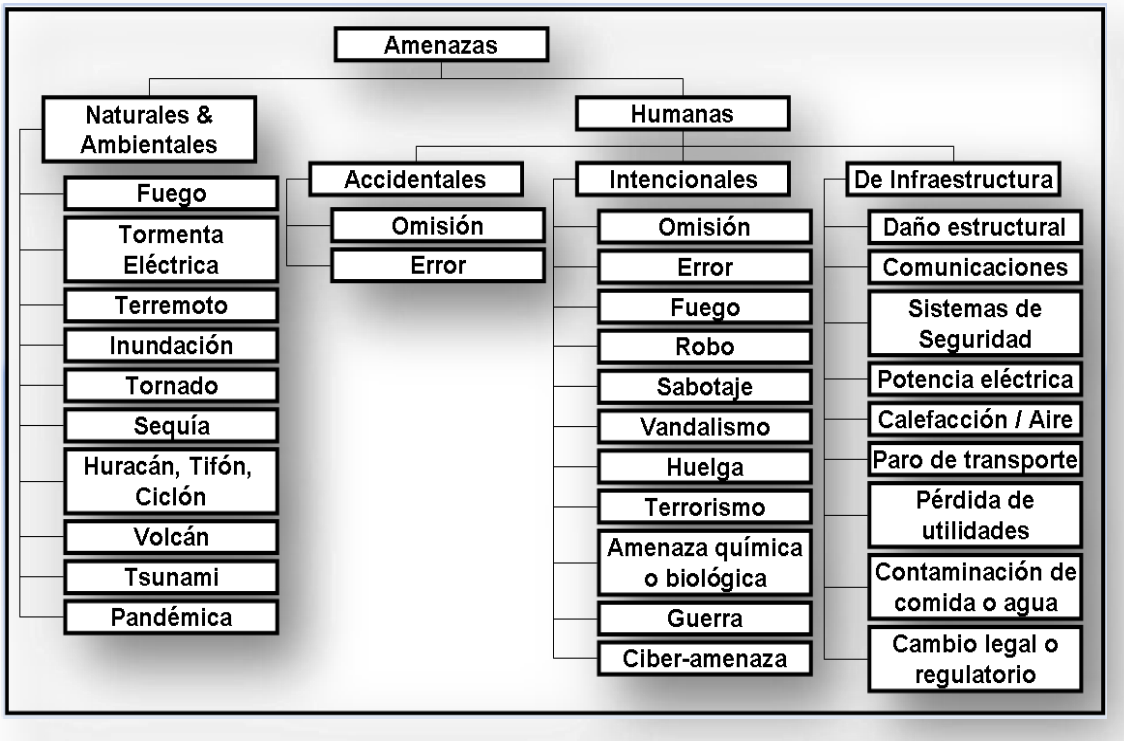
Una vez identificadas las amenazas, y con el propósito de complementar y de validar la lista de amenazas encontradas, se realiza una verificación contra algunas de las fuentes de amenazas especificadas en Figura No. 2. Fuentes de amenazas., agrupándolas para el análisis de riesgo como amenazas de tipo natural, intencionales (humanas) o accidentales.

En esta actividad se establece el conjunto de vulnerabilidades que posee cada activo crítico de TI, que, en caso de ser explotadas por una o varias amenazas, afectarían la continuidad de las operaciones.

Las vulnerabilidades, por su parte, son debilidades o ausencia de controles que un activo perteneciente a un proceso pueda tener. Algunas vulnerabilidades consideradas dentro de esta metodología son:

- Ausencia de políticas.
- Configuraciones no seguras
- Errores de configuración.
- Errores de mantenimiento.
- Errores del administrador.
- Errores en código.
- Exposición a materiales peligrosos.
- Fallas de usuarios.
- Manuales de uso no documentados.
- Medidas de protección de acceso inadecuadas.
- Medidas de protección física inadecuadas.
- Procesos o procedimientos no documentados.
- Usuario desinformado.
- Tecnología inadecuada.
- Debilidad o inexistencia de controles.
- Condiciones de locales inadecuadas o no seguras.

Ilustración 2. Fuentes de Amenazas



Fuente: Elaboración propia SISAM

12. Bibliografía

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES (2018). Manual de Gobierno Digital. Bogotá

MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIONES, Fortalecimiento de la Gestión TI en el Estado, https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

ISO/IEC/27001(2013). Sistema de Gestión de Seguridad de la Información. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, Bogotá D.C.