MANUAL DE POLITICAS DE BASE DE DATOS DEL MINISTERIO DE LA DEFENSA NACIONAL

GUATEMALA | 2023

COMANDO DE INFORMATICA Y TECNOLOGIA

compañía DE SISTEMAS DEL BATALLON DEL TIC´S DEL CIT

2023

INDICE

[INDICE 1](#_Toc133612498)

[I. INTRODUCCION 4](#_Toc133612499)

[A. Propósito del Manual 4](#_Toc133612500)

[B. Alcances del Manual 5](#_Toc133612501)

[C. Definiciones 7](#_Toc133612502)

[1. Base de Datos: 7](#_Toc133612503)

[2. Políticas de Seguridad: 7](#_Toc133612504)

[3. Auditoría: 7](#_Toc133612505)

[4. Continuidad del Negocio: 7](#_Toc133612506)

[D. Acrónimos 7](#_Toc133612507)

[1. N/A (No Aplica): 7](#_Toc133612508)

[2. IT (Tecnología de la Información): 8](#_Toc133612509)

[3. SSO (Single Sign-On): 8](#_Toc133612510)

[4. GDPR (Reglamento General de Protección de Datos): 8](#_Toc133612511)

[5. DR (Recuperación ante Desastres): 8](#_Toc133612512)

[II. Política de backup: 8](#_Toc133612513)

[A. Objetivo 8](#_Toc133612514)

[B. Alcance 8](#_Toc133612515)

[C. Política de Backup 8](#_Toc133612516)

[D. Procedimiento de Backup 8](#_Toc133612517)

[III. Política de asignación de Permisos 9](#_Toc133612518)

[A. Propósito 9](#_Toc133612519)

[B. Alcance 9](#_Toc133612520)

[C. Política 9](#_Toc133612521)

[D. Procedimientos 9](#_Toc133612522)

[E. Cumplimiento 10](#_Toc133612523)

[IV. Política de seguridad de la base de datos para proteger información sensible 10](#_Toc133612524)

[A. Propósito 10](#_Toc133612525)

[B. Alcance 10](#_Toc133612526)

[C. Política 10](#_Toc133612527)

[1. Encriptación de datos: 10](#_Toc133612528)

[2. Uso de contraseñas seguras: 10](#_Toc133612529)

[3. Control de acceso: 11](#_Toc133612530)

[4. Monitoreo de la actividad: 11](#_Toc133612531)

[D. Procedimientos 11](#_Toc133612532)

[E. Cumplimiento 11](#_Toc133612533)

[V. Política de auditoría 11](#_Toc133612534)

[A. Propósito 11](#_Toc133612535)

[B. Alcance 11](#_Toc133612536)

[C. Política 12](#_Toc133612537)

[D. Procedimientos 12](#_Toc133612538)

[E. Cumplimiento 12](#_Toc133612539)

[VI. Política de actualizaciones 12](#_Toc133612540)

[A. Propósito 12](#_Toc133612541)

[B. Alcance 12](#_Toc133612542)

[C. Política 13](#_Toc133612543)

[D. Procedimientos 13](#_Toc133612544)

[E. Cumplimiento 13](#_Toc133612545)

[VII. Política de creación de usuarios 13](#_Toc133612546)

[A. Propósito 13](#_Toc133612547)

[B. Alcance 13](#_Toc133612548)

[C. Política 13](#_Toc133612549)

[D. Procedimientos 14](#_Toc133612550)

[E. Cumplimiento 14](#_Toc133612551)

[VIII. Política de revisión periódica de acceso de usuarios a la Base de Datos 14](#_Toc133612552)

[A. Propósito 14](#_Toc133612553)

[B. Alcance 14](#_Toc133612554)

[C. Política 14](#_Toc133612555)

[D. Procedimientos 15](#_Toc133612556)

[E. Cumplimiento 15](#_Toc133612557)

[IX. Política de eliminación de usuarios inactivos 15](#_Toc133612558)

[A. Propósito: 15](#_Toc133612559)

[B. Alcance: 15](#_Toc133612560)

[C. Política: 15](#_Toc133612561)

[D. Procedimientos: 16](#_Toc133612562)

[E. Cumplimiento: 16](#_Toc133612563)

[X. Política de contraseña segura 16](#_Toc133612564)

[A. Propósito 16](#_Toc133612565)

[B. Alcance 16](#_Toc133612566)

[C. Política 17](#_Toc133612567)

[D. Procedimientos 17](#_Toc133612568)

[E. Cumplimiento 17](#_Toc133612569)

[XI. Política de Responsabilidades del Administrador de Base de Datos 17](#_Toc133612570)

[A. Propósito: 17](#_Toc133612571)

[B. Alcance: 17](#_Toc133612572)

[C. Política: 17](#_Toc133612573)

[D. Procedimientos: 18](#_Toc133612574)

[E. Cumplimiento: 18](#_Toc133612575)

[XII. Política de Responsabilidades del Administrador de Base de Datos 18](#_Toc133612576)

[A. Propósito: 18](#_Toc133612577)

[B. Alcance: 18](#_Toc133612578)

[C. Política: 18](#_Toc133612579)

[D. Procedimientos: 19](#_Toc133612580)

[E. Cumplimiento: 19](#_Toc133612581)

[XIII. Política de Procedimientos de Recuperación ante Desastres 19](#_Toc133612582)

[A. Propósito: 19](#_Toc133612583)

[B. Alcance: 20](#_Toc133612584)

[C. Política: 20](#_Toc133612585)

[D. Procedimientos: 20](#_Toc133612586)

[E. Cumplimiento: 21](#_Toc133612587)

[XIV. Resumen de las políticas del manual: 21](#_Toc133612588)

[XV. Importancia del cumplimiento de las políticas: 21](#_Toc133612589)

[XVI. Actualización y revisión del manual: 21](#_Toc133612590)

1. INTRODUCCION

La base de datos es uno de los activos más valiosos del Ministerio de la Defensa Nacional, ya que en ella se encuentra almacenada una gran cantidad de información crítica y sensible. Por esta razón, es fundamental contar con un conjunto de políticas y procedimientos que permitan proteger la integridad y confidencialidad de la información contenida en la base de datos.

El presente manual tiene como objetivo establecer las pautas para el uso seguro y efectivo de la base de datos del Ministerio de la Defensa Nacional. La implementación de estas políticas y procedimientos permitirá a la Institución proteger su información crítica y sensible, minimizar los riesgos asociados con el manejo de la información y garantizar la disponibilidad de la información en todo momento.

El manual se basa en las mejores prácticas y estándares de la industria, y está diseñado para ser una guía clara y fácil de entender para todos los usuarios que tengan acceso a la base de datos. Las políticas establecidas en este manual son esenciales para la gestión adecuada de la base de datos y deben ser seguidas por todos los usuarios.

En resumen, el presente manual es una herramienta clave para garantizar la seguridad y protección de la información crítica del Ministerio de la Defensa Nacional, y su implementación será de gran beneficio para la Institución en términos de gestión de la base de datos y prevención de riesgos de seguridad.

1. Propósito del Manual

El propósito de este manual es establecer las políticas y procedimientos necesarios para garantizar la seguridad y la integridad de la información almacenada en la base de datos del Ministerio de la Defensa Nacional. Este manual proporciona una guía detallada sobre cómo se deben gestionar los datos y se deben establecer las medidas necesarias para prevenir el acceso no autorizado a la información confidencial.

El objetivo principal de este manual es establecer una guía de buenas prácticas para la gestión de la base de datos. A través de la implementación de estas políticas y procedimientos, se busca asegurar la confidencialidad, integridad y disponibilidad de la información contenida en la base de datos, y establecer los mecanismos necesarios para prevenir y detectar cualquier incidente de seguridad que pueda poner en riesgo la información.

Entre los objetivos específicos del manual, podemos destacar los siguientes:

Definir y establecer una política de backup adecuada para garantizar la integridad de la información almacenada en la base de datos.

Establecer una política de asignación de permisos para asegurar que los usuarios tengan el acceso adecuado a la información que necesitan, sin comprometer la seguridad de esta.

Definir una política de seguridad de la base de datos para proteger la información sensible y crítica, y prevenir la divulgación no autorizada de la misma.

Establecer una política de auditoría para monitorear el uso de la base de datos, detectar posibles incidentes de seguridad y tomar medidas adecuadas para proteger la información.

Definir una política de actualizaciones para asegurar que la base de datos se mantenga actualizada y protegida contra posibles vulnerabilidades de seguridad.

Establecer una política de creación de usuarios para garantizar que solo los usuarios autorizados tengan acceso a la base de datos.

Definir una política de revisión periódica de acceso de usuarios a la base de datos para asegurarse de que los usuarios tengan el acceso adecuado a la información, y revocar los permisos innecesarios.

Establecer una política de contraseña segura para garantizar que las contraseñas utilizadas para acceder a la base de datos sean seguras y no comprometan la seguridad de la información.

En resumen, el manual tiene como objetivo establecer un conjunto de políticas y procedimientos que permitan proteger la información contenida en la base de datos, minimizar los riesgos asociados con el manejo de la información y garantizar su disponibilidad en todo momento. A través de la implementación de estas políticas, se busca proteger la información crítica y sensible del Ministerio de la Defensa Nacional, y garantizar su gestión adecuada y segura.

1. Alcances del Manual

Este manual se aplica a todos los usuarios que tienen acceso a la base de datos del Ministerio de la Defensa Nacional. Incluye las políticas y los procedimientos necesarios para la asignación de permisos, la seguridad de la base de datos, la auditoría, la actualización, la creación de usuarios, la revisión periódica del acceso de usuarios, la contraseña segura, la eliminación de usuarios inactivos, el cumplimiento normativo, la documentación y gestión del conocimiento y la continuidad del servicio o servicios prestados por el Comando de Informática y Tecnología.

El presente manual de políticas para la base de datos establece una serie de directrices y procedimientos para asegurar la gestión segura y eficiente de la base de datos del Ministerio de la Defensa Nacional. Los alcances de este manual se refieren a la implementación de las políticas y procedimientos establecidos en el mismo, los cuales son aplicables a todas las personas que tengan acceso a la base de datos.

Entre los alcances específicos del manual, podemos destacar los siguientes:

Backup: la política de backup establecida en el manual es aplicable a todos los datos almacenados en la base de datos. El objetivo es asegurar la integridad de la información almacenada, mediante la realización de copias de seguridad periódicas.

Asignación de permisos: la política de asignación de permisos establecida en el manual es aplicable a todos los usuarios que tengan acceso a la base de datos. El objetivo es asegurar que los usuarios tengan el acceso adecuado a la información que necesitan, sin comprometer la seguridad de esta.

Seguridad de la base de datos: la política de seguridad de la base de datos establecida en el manual es aplicable a todas las bases de datos del Ministerio de la Defensa Nacional que contengan información sensible o crítica. El objetivo es prevenir la divulgación no autorizada de la información, y garantizar la protección de esta.

Auditoría: la política de auditoría establecida en el manual es aplicable a todas las bases de datos de la del Ministerio de la Defensa Nacional. El objetivo es monitorear el uso de la base de datos, detectar posibles incidentes de seguridad y tomar medidas adecuadas para proteger la información.

Actualizaciones: la política de actualizaciones establecida en el manual es aplicable a todas las bases de datos de la del Ministerio de la Defensa Nacional. El objetivo es asegurar que la base de datos se mantenga actualizada y protegida contra posibles vulnerabilidades de seguridad.

Creación de usuarios: la política de creación de usuarios establecida en el manual es aplicable a todas las personas que tengan la responsabilidad de crear y gestionar usuarios en la base de datos. El objetivo es garantizar que solo los usuarios autorizados tengan acceso a la base de datos.

Revisión periódica de acceso de usuarios a la base de datos: la política de revisión periódica de acceso de usuarios establecida en el manual es aplicable a todos los usuarios de la base de datos. El objetivo es asegurarse de que los usuarios tengan el acceso adecuado a la información, y revocar los permisos innecesarios.

Contraseña segura: la política de contraseña segura establecida en el manual es aplicable a todos los usuarios que tengan acceso a la base de datos. El objetivo es garantizar que las contraseñas utilizadas para acceder a la base de datos sean seguras y no comprometan la seguridad de la información.

En resumen, los alcances del manual se refieren a la implementación de las políticas y procedimientos establecidos en el mismo, los cuales son aplicables a todas las personas que tengan acceso a la base de datos. La implementación de estas políticas permitirá proteger la información crítica y sensible del Ministerio de la Defensa Nacional, minimizar los riesgos asociados con el manejo de la información y garantizar su disponibilidad en todo momento.

1. Definiciones

Se proporcionan definiciones para facilitar la comprensión de los términos técnicos utilizados en este manual.

1. Base de Datos:

Conjunto de datos organizados y relacionados que se almacenan en un sistema informático y que pueden ser accedidos y manipulados de manera eficiente.

1. Políticas de Seguridad:

Conjunto de reglas y directrices que se establecen con el fin de proteger la información y los activos de una organización.

1. Auditoría:

Proceso de evaluación sistemática y documentada de las actividades o de un sistema para determinar si se cumplen los objetivos y se satisfacen los requisitos establecidos.

1. Mantenimiento de los servicios:

Capacidad del datacenter para continuar operando en caso de interrupciones imprevistas en sus operaciones normales.

1. Acrónimos

Se proporcionan acrónimos para facilitar la comprensión de las abreviaturas utilizadas en este manual.

1. N/A (No Aplica):

Término utilizado para indicar que una política no es aplicable en una situación particular.

1. IT (Tecnología de la Información):

Conjunto de herramientas, tecnologías y recursos utilizados para procesar, almacenar y compartir información.

1. SSO (Single Sign-On):

Sistema que permite a un usuario autenticarse una sola vez para acceder a múltiples aplicaciones.

1. DR (Recuperación ante Desastres):

Proceso de planificación y preparación para garantizar que una organización pueda recuperarse rápidamente en caso de un desastre o una interrupción no planificada.

1. Política de backup:
2. Objetivo

El objetivo de esta política es garantizar la disponibilidad y la recuperación de datos en caso de desastres, mediante la implementación de un plan de backup y restauración de la base de datos.

1. Alcance

Esta política se aplicará a todos los usuarios y administradores de la Base de Datos.

1. Política de Backup

Para garantizar la disponibilidad de la Base de Datos en caso de interrupciones del servicio o fallos en el hardware, se llevará a cabo diariamente un backup de nivel cero (0), lo que implica una copia completa de la Base de Datos.

1. Procedimiento de Backup

El procedimiento de backup se llevará a cabo de la siguiente manera:

Se realizará diariamente un backup completo de la Base de Datos.

Se almacenará la copia de seguridad en un lugar seguro y fuera de línea.

Se verificará la integridad de la copia de seguridad regularmente para garantizar su disponibilidad y recuperación en caso de desastres.

1. Procedimiento de Restauración

En caso de ser necesario, se llevará a cabo el procedimiento de restauración de la siguiente manera:

Se identificará la última copia de seguridad disponible.

Se verificará la integridad de la copia de seguridad antes de iniciar la recuperación de los datos.

Se llevará a cabo la restauración de los datos en el servidor correspondiente.

Se comprobará la integridad de los datos restaurados para garantizar su disponibilidad y correcta recuperación.

Con esta política de backup, se busca garantizar la disponibilidad y recuperación de los datos en caso de desastres, protegiendo la información almacenada en la Base de Datos y evitando posibles pérdidas de información crítica para la institución.

1. Política de asignación de Permisos
2. Propósito

El propósito de esta política es garantizar la integridad y la confidencialidad de los datos almacenados en la base de datos del Ministerio de la Defensa Nacional, mediante la asignación de permisos adecuados y limitados, según la necesidad específica y exclusiva del usuario.

1. Alcance

Esta política se aplica a todos los usuarios de la base de datos del Ministerio de la Defensa Nacional, incluyendo el personal interno y externo que tenga acceso a la Base de Datos.

1. Política

La asignación de permisos se realizará de manera adecuada y limitada, según la necesidad específica y exclusiva del usuario, sin otorgar permisos que el usuario no necesite según su número de plaza y numero de catálogo. Esto garantizará que los usuarios solo tengan acceso a la información necesaria para realizar sus tareas y evitará la exposición innecesaria de información confidencial.

Los permisos otorgados a nivel de aplicación respaldarán la asignación de permisos de la Base de Datos. Se asegurará que los permisos asignados estén en línea con las políticas y procedimientos establecidos por el Ministerio de la Defensa Nacional y con las regulaciones y normativas aplicables.

1. Procedimientos

Se establecerán procedimientos específicos para la asignación de permisos, que incluirán la identificación de las necesidades específicas de los usuarios, la asignación de permisos de manera adecuada y limitada, y la revisión periódica de los permisos asignados para garantizar que sigan siendo necesarios y apropiados.

Además, se llevará a cabo una revisión periódica de los permisos de los usuarios, a fin de garantizar que solo tengan acceso a la información necesaria para realizar sus tareas y que se cumpla con las políticas y procedimientos establecidos por el Ministerio de la Defensa Nacional.

1. Cumplimiento

El incumplimiento de esta política puede dar lugar a la exposición innecesaria de información confidencial y a posibles riesgos y amenazas para la seguridad de la información. Todos los miembros del Ministerio de la Defensa Nacional tienen la responsabilidad de cumplir con esta política y los procedimientos establecidos en ella.

1. Política de seguridad de la base de datos para proteger información sensible
2. Propósito

El propósito de esta política es garantizar la seguridad y la privacidad de la información sensible almacenada en la Base de Datos del Ministerio de la Defensa Nacional, mediante la implementación de medidas de seguridad de la Base de Datos.

1. Alcance

Esta política se aplica a todos los usuarios de la Base de Datos del Ministerio de la Defensa Nacional, incluyendo el personal interno y externo que tenga acceso a la Base de Datos.

1. Política

Se implementarán medidas de seguridad de la Base de Datos para proteger la información sensible almacenada de accesos no autorizados. Estas medidas incluirán, entre otras:

1. Uso de contraseñas seguras:

Se establecerán políticas específicas para el uso de contraseñas seguras por parte de los usuarios de la Base de Datos, a fin de garantizar que se utilicen contraseñas seguras y robustas para evitar el acceso no autorizado.

1. Control de acceso:

Se establecerán procedimientos específicos para el control de acceso a la Base de Datos, a fin de garantizar que solo los usuarios autorizados tengan acceso a la información sensible almacenada.

1. Monitoreo de la actividad:

Se llevará a cabo un monitoreo constante de la actividad en la Base de Datos, a fin de identificar posibles accesos no autorizados y tomar medidas para evitarlos.

1. Procedimientos

Se establecerán procedimientos específicos para la implementación de medidas de seguridad de la Base de Datos, que incluirán la encriptación de datos, el uso de contraseñas seguras, el control de acceso y el monitoreo de la actividad. Estos procedimientos se implementarán de manera constante y se revisarán periódicamente para garantizar su eficacia.

Además, se llevará a cabo una evaluación periódica de la seguridad de la Base de Datos, a fin de identificar posibles áreas de mejora y tomar medidas para mejorar la seguridad y la privacidad de la información almacenada.

1. Cumplimiento

El incumplimiento de esta política puede dar lugar a la exposición de información sensible y a posibles riesgos y amenazas para la seguridad de la información. Todos los miembros del Ministerio de la Defensa Nacional tienen la responsabilidad de cumplir con esta política y los procedimientos establecidos en ella.

1. Política de auditoría
2. Propósito

El propósito de esta política es garantizar la seguridad y la privacidad de la información almacenada en la Base de Datos del Ministerio de la Defensa Nacional, mediante el establecimiento de un proceso de monitoreo y auditoría de la base de datos.

1. Alcance

Esta política se aplica a todos los usuarios de la Base de Datos del Ministerio de la Defensa Nacional, incluyendo el personal interno y externo que tenga acceso a la Base de Datos.

1. Política

Se establecerá un proceso de monitoreo y auditoría de la Base de Datos para detectar y prevenir actividades maliciosas y garantizar el cumplimiento de las políticas de seguridad establecidas. Cada tabla de la Base de Datos contará con su respectiva auditoría y deberá tener activos los “triggers” (disparadores) correspondientes a la acción de “insert”, “update”, “delete” (ingreso, actualización, eliminación) de la información.

El monitoreo y la auditoría se llevarán a cabo de manera constante y se registrarán los resultados de cada auditoría. Además, se establecerán procedimientos específicos para la revisión y el análisis de los registros de auditoría, a fin de identificar posibles actividades maliciosas o violaciones de las políticas de seguridad.

1. Procedimientos

Se establecerán procedimientos específicos para el monitoreo y la auditoría de la Base de Datos, que incluirán la implementación de “triggers” en cada tabla de la Base de Datos, la revisión y el análisis periódico de los registros de auditoría, y la toma de medidas para prevenir y detectar actividades maliciosas.

Además, se llevará a cabo una evaluación periódica del proceso de monitoreo y auditoría de la Base de Datos, a fin de identificar posibles áreas de mejora y tomar medidas para mejorar la eficacia del proceso.

1. Cumplimiento

El incumplimiento de esta política puede dar lugar a posibles actividades maliciosas y violaciones de las políticas de seguridad. Todos los miembros del Ministerio de la Defensa Nacional tienen la responsabilidad de cumplir con esta política y los procedimientos establecidos en ella.

1. Política de actualizaciones
2. Propósito

El propósito de esta política es garantizar la seguridad y la privacidad de la información almacenada en la Base de Datos del Ministerio de la Defensa Nacional, mediante la implementación de medidas para mantener la Base de Datos actualizada y protegida contra vulnerabilidades conocidas.

1. Alcance

Esta política se aplica a todos los usuarios de la Base de Datos del Ministerio de la Defensa Nacional, incluyendo el personal interno y externo que tenga acceso a la Base de Datos.

1. Política

Se mantendrá la Base de Datos actualizada y se aplicarán parches y actualizaciones de seguridad para corregir vulnerabilidades conocidas y minimizar el riesgo de ataques.

Las actualizaciones se llevarán a cabo de manera constante y se establecerá un proceso para identificar y aplicar las actualizaciones necesarias de manera oportuna. Además, se establecerán procedimientos específicos para la implementación de actualizaciones, a fin de minimizar el impacto en la disponibilidad y el rendimiento de la Base de Datos.

1. Procedimientos

Se establecerán procedimientos específicos para la identificación y aplicación de parches y actualizaciones de seguridad para la Base de Datos, que incluirán la evaluación de la importancia y el impacto de cada actualización, la planificación de la implementación y la revisión y el análisis posterior a la implementación.

Además, se llevará a cabo una evaluación periódica del proceso de actualizaciones, a fin de identificar posibles áreas de mejora y tomar medidas para mejorar la eficacia del proceso.

1. Cumplimiento

El incumplimiento de esta política puede dar lugar a la exposición innecesaria de información confidencial y a posibles riesgos y amenazas para la seguridad de la información. Todos los miembros del Ministerio de la Defensa Nacional tienen la responsabilidad de cumplir con esta política y los procedimientos establecidos en ella.

1. Política de creación de usuarios
2. Propósito

El propósito de esta política es garantizar la seguridad y la privacidad de la información almacenada en la Base de Datos del Ministerio de la Defensa Nacional, mediante el establecimiento de procedimientos para la creación y gestión de usuarios en la Base de Datos.

1. Alcance

Esta política se aplica a todos los usuarios de la Base de Datos del Ministerio de la Defensa Nacional, incluyendo el personal interno y externo que tenga acceso a la Base de Datos.

1. Política

Se establecerán procedimientos para la creación y gestión de usuarios en la Base de Datos, a fin de garantizar que solo los usuarios autorizados tengan acceso a la información almacenada. Se establecerá una política clara de acceso a la Base de Datos, limitando el acceso a usuarios autorizados y configurando roles y permisos para controlar el acceso.

Los procedimientos para la creación y gestión de usuarios incluirán la verificación de la necesidad de acceso a la Base de Datos, la asignación de roles y permisos específicos según las necesidades del usuario y la eliminación de usuarios que ya no necesiten acceso a la Base de Datos.

Todos los usuarios que soliciten acceso a la base de datos del Ministerio de la Defensa Nacional deberán tener número de catalogo para poder ser identificados, en caso de no tener numero de catálogo, no se les darán permisos ni acceso a la misma.

1. Procedimientos

Se establecerán procedimientos específicos para la creación y gestión de usuarios en la Base de Datos, que incluirán la verificación de la necesidad de acceso, la asignación de roles y permisos específicos y la eliminación de usuarios que ya no necesiten acceso.

Además, se llevará a cabo una evaluación periódica de los usuarios con acceso a la Base de Datos, a fin de identificar posibles usuarios no autorizados y tomar medidas para limitar su acceso.

1. Cumplimiento

El incumplimiento de esta política puede dar lugar a la exposición innecesaria de información confidencial y a posibles riesgos y amenazas para la seguridad de la información. Todos los miembros del Ministerio de la Defensa Nacional tienen la responsabilidad de cumplir con esta política y los procedimientos establecidos en ella.

1. Política de GESTION de usuarios CON PERMISOS EN La Base de Datos
2. Propósito

El propósito de esta política es garantizar la seguridad y la privacidad de la información almacenada en la Base de Datos del Ministerio de la Defensa Nacional, mediante el establecimiento de un proceso de revisión periódica del acceso de los usuarios.

1. Alcance

Esta política se aplica a todos los usuarios de la Base de Datos del Ministerio de la Defensa Nacional, incluyendo el personal interno y externo que tenga acceso a la Base de Datos.

1. Política

Se ha establecido un proceso de revisión periódica del acceso de los usuarios, con el fin de garantizar la seguridad y la privacidad de la información almacenada en la Base de Datos. Aquellos usuarios que no utilicen sus credenciales en un periodo de cuarenta (40) días o más serán deshabilitados. Estos usuarios deberán solicitar los permisos correspondientes por el conducto respectivo si desean volver a tener acceso a la Base de Datos.

Además, aquellos miembros del personal que causen baja, sean suspendidos de empleo por cualquier motivo, asciendan de tropa a Espta. o cualquier otro motivo por el que dejen su puesto, serán deshabilitados. En caso de que necesiten volver a tener acceso a la Base de Datos, deberán solicitar los permisos correspondientes por el conducto respectivo.

1. Procedimientos

Se establecerá un procedimiento específico para la identificación de usuarios inactivos y la eliminación de los mismos, así como para la gestión de las solicitudes de permisos correspondientes.

1. Cumplimiento

El incumplimiento de esta política puede dar lugar a la exposición innecesaria de información confidencial y a posibles riesgos y amenazas para la seguridad de la información. Todos los miembros del Ministerio de la Defensa Nacional tienen la responsabilidad de cumplir con esta política y los procedimientos establecidos en ella.

1. Política de eliminación de usuarios inactivos
2. Propósito:

Establecer un conjunto de directrices y procedimientos para garantizar la seguridad y la privacidad de la información almacenada en nuestra Base de Datos, a través de la eliminación de los usuarios inactivos.

1. Alcance:

Esta política se aplicará a todos los usuarios de la Base de Datos del Ministerio de la Defensa Nacional.

1. Política:

El responsable de la Base de Datos llevará a cabo una eliminación periódica de los usuarios inactivos para garantizar la integridad y confidencialidad de los datos almacenados en la Base de Datos. Un usuario se considera inactivo si no ha utilizado sus credenciales de acceso a la Base de Datos por un periodo de cuarenta (40) días o más, que han causado baja, han sido suspendidos de empleo, han ascendido de tropa a Espta o por cualquier otro motivo por el que hayan dejado su puesto, esto se detalla con mayor detenimiento en la “Política de gestión de usuarios con permisos en la base de datos”.

Además, se llevará un registro detallado de todas las cuentas de usuario eliminadas, incluyendo la fecha y hora de la eliminación, el usuario que llevó a cabo la eliminación y cualquier otra información relevante.

Antes de llevar a cabo la eliminación de las cuentas de usuario inactivas, se llevará a cabo una copia de seguridad completa de los usuarios de la Base de Datos. Dicha copia se mantendrá durante un periodo de treinta (30) días a partir de la fecha de eliminación.

En caso de que se requiera la recuperación de alguna cuenta de usuario eliminada, se deberá solicitar por el conducto respectivo y únicamente se reestablecerá el usuario con sus respectivos permisos por orden de la Jefatura del Estado Mayor del Ministerio de la Defensa Nacional u Orden Administrativa firmada por el Comandante de Batallón de TIC´s.

1. Procedimientos:

El responsable de la Base de Datos llevará a cabo un proceso de identificación de los usuarios inactivos. Además, se realizará una revisión periódica de los usuarios que han causado baja, han sido suspendidos de empleo, han ascendido de tropa a Espta o por cualquier otro motivo por el que hayan dejado su puesto, para asegurarse de que sean deshabilitados.

Una vez identificados los usuarios inactivos, el responsable de la Base de Datos procederá a la eliminación de estos.

1. Cumplimiento:

Todos los usuarios de la Base de Datos del Ministerio de la Defensa Nacional están obligados a cumplir con esta política de eliminación de usuarios inactivos. El incumplimiento de esta política puede dar lugar a medidas disciplinarias, como la revocación de los privilegios de acceso a la Base de Datos.

1. Política de contraseña segura
2. Propósito

El propósito de esta política es garantizar la seguridad y la privacidad de la información almacenada en la Base de Datos del Ministerio de la Defensa Nacional, mediante la implementación de una política de contraseñas seguras.

1. Alcance

Esta política se aplica a todos los usuarios de la Base de Datos del Ministerio de la Defensa Nacional, incluyendo el personal interno y externo que tenga acceso a la Base de Datos.

1. Política

Se implementará una política de contraseñas robustas, compuestas por doce (12) o más caracteres, que debe incluir obligatoriamente una (01) letra mayúscula, una (01) letra minúscula, un (01) número y un (01) carácter especial como mínimo.

1. Procedimientos

Se establecerá un procedimiento específico para la implementación y gestión de la política de contraseñas seguras, que incluirá la verificación de la complejidad de las contraseñas.

Las solicitudes de restablecimiento de contraseñas se deberán realizar por el conducto respectivo y únicamente se reestablecerá la contraseña por orden de la Jefatura del Estado Mayor del Ministerio de la Defensa Nacional u Orden Administrativa firmada por el Comandante de Batallón de TIC´s.

1. Cumplimiento

El incumplimiento de esta política puede dar lugar a la exposición innecesaria de información confidencial y a posibles riesgos y amenazas para la seguridad de la información. Todos los miembros del Ministerio de la Defensa Nacional tienen la responsabilidad de cumplir con esta política y los procedimientos establecidos en ella.

1. Política de Responsabilidades del Administrador de Base de Datos
2. Propósito:

El propósito de esta política es establecer las responsabilidades del Administrador de Base de Datos para garantizar la disponibilidad, integridad, confidencialidad y seguridad de la información almacenada en la Base de Datos.

1. Alcance:

Esta política es aplicable a todos los Administradores de Base de Datos que trabajan con la información almacenada en la Base de Datos del Ministerio de la Defensa Nacional.

1. Política:

El Administrador de Base de Datos es responsable de garantizar la disponibilidad, integridad, confidencialidad y seguridad de la información almacenada en la Base de Datos. Las responsabilidades principales del Administrador de Base de Datos incluyen la configuración, instalación y mantenimiento de la Base de Datos, definición de políticas y procedimientos de seguridad y acceso, gestión y monitoreo de los recursos de la Base de Datos, planificación y ejecución de estrategias de backup y restauración, administración de usuarios y permisos, monitoreo y optimización del rendimiento de la Base de Datos, resolución de problemas y mantenimiento de la disponibilidad del sistema.

1. Procedimientos:

El Administrador de Base de Datos debe mantenerse en contacto y colaboración para garantizar la correcta gestión de la Base de Datos. Las responsabilidades específicas del Administrador de Base de Datos en este ámbito son la comunicación con todo el personal responsable e involucrado en la administración de los servicios proporcionados por el Comando de Informática y Tecnología.

Esta acción no reemplaza las obligaciones administrativas requeridas por los procesos, ya que es responsabilidad del Administrador de la Base de Datos solicitar la documentación necesaria para cada diligencia y el solicitante será responsable de su gestión.

El Administrador de Base de Datos deberá asegurarse de que se cumplan los procedimientos establecidos y dar parte de cualquier desviación o problema encontrado.

1. Cumplimiento:

El incumplimiento de esta política puede comprometer la disponibilidad, integridad, confidencialidad y seguridad de la información almacenada en la Base de Datos. Los Administradores de Base de Datos que incumplen esta política pueden ser sujetos a acciones disciplinarias.

1. Política de Procedimientos de Recuperación ante Desastres
2. Propósito:

Establecer los procedimientos necesarios para garantizar la recuperación de la Base de Datos en caso de un desastre natural o humano, minimizando la pérdida de información y garantizando la continuidad del servicio.

1. Alcance:

Esta política se aplica a todos los todos los usuarios del Ministerio de la Defensa Nacional que tengan acceso a la Base de Datos.

1. Política:

Se establecerán procedimientos de recuperación ante desastres para garantizar la disponibilidad y continuidad de los servicios de la Base de Datos en caso de un desastre natural o humano.

Se realizarán copias de seguridad de la Base de Datos de manera periódica y se almacenarán en un lugar seguro, estas se encontrarán en un servidor destinado para el almacenamiento de los respaldos el cual permanecerá fuera de línea.

Se definirán los roles y responsabilidades del equipo encargado de la recuperación ante desastres, incluyendo la designación de un líder del equipo y la identificación de las personas clave que serán necesarias para la recuperación.

Se definirán los procedimientos para la recuperación de la Base de Datos, incluyendo la identificación de los recursos necesarios y los plazos para la recuperación.

Se llevarán a cabo pruebas regulares para verificar la efectividad de los procedimientos de recuperación ante desastres.

Se definirán los procedimientos de comunicación en caso de un desastre, incluyendo la notificación al equipo encargado de la recuperación y a los usuarios afectados.

Se garantizará la protección y privacidad de la información durante la recuperación de la Base de Datos.

1. Procedimientos:

Identificación de los riesgos y amenazas que puedan afectar la Base de Datos.

Definición de los roles y responsabilidades del equipo encargado de la recuperación ante desastres.

Definición de los procedimientos de copias de seguridad y almacenamiento de la información.

Definición de los procedimientos para la recuperación de la Base de Datos, incluyendo la identificación de los recursos necesarios y los plazos para la recuperación.

Realización de pruebas regulares para verificar la efectividad de los procedimientos de recuperación ante desastres.

Definición de los procedimientos de comunicación en caso de un desastre.

Garantizar la protección y privacidad de la información durante la recuperación de la Base de Datos.

Esta información se encuentra en el Plan de recuperación ante desastres de la Compañía de Sistemas del Batallón de TIC´s.

1. Cumplimiento:

El incumplimiento de esta política puede dar lugar a la pérdida de información y/o la interrupción del servicio, lo que podría tener un impacto negativo en el Ministerio de la Defensa Nacional. Todos los usuarios que incumplan esta política serán sujeto de sanción según las medidas disciplinarias y/o legales según lo establecido por el Ministerio de la Defensa Nacional.

1. Resumen de las políticas del manual:

Este manual establece una serie de políticas y procedimientos para garantizar la seguridad y la privacidad de la información almacenada en la Base de Datos del Ministerio de la Defensa Nacional. Las políticas incluyen la política de backup, la política de asignación de permisos, la política de seguridad de la base de datos, la política de auditoría, la política de actualizaciones, la política de creación de usuarios, política de gestión de usuarios con permisos en la base de datos, la política de contraseña segura, la política de eliminación de usuarios inactivos, la política de cumplimiento normativo, la política de documentación y gestión del conocimiento, y la política de continuidad del negocio.

1. Importancia del cumplimiento de las políticas:

El cumplimiento de las políticas establecidas en este manual es fundamental para garantizar la seguridad y la privacidad de la información almacenada en la Base de Datos del Ministerio de la Defensa Nacional. El incumplimiento de estas políticas puede dar lugar a la pérdida de información confidencial, la exposición a posibles riesgos y amenazas, y la violación de las normativas y regulaciones aplicables. Es responsabilidad de todos los miembros del Ministerio de la Defensa Nacional cumplir con estas políticas y procedimientos.

1. Actualización y revisión del manual:

Este manual será revisado y actualizado de manera periódica, a fin de garantizar que se reflejen los cambios en la organización, las normativas y regulaciones aplicables, y las mejores prácticas en cuanto a la seguridad de la información. Es responsabilidad del Pelotón de Base de Datos la Compañía de Sistemas del Batallón de TIC´S del Comando de Informática y Tecnología llevar a cabo la revisión y actualización periódica del manual, y de todos los miembros del Ministerio de la Defensa Nacional mantenerse al día con las políticas y procedimientos establecidos en el mismo.

|  |
| --- |
| ELABORO  Comandante del Pelotón de Base de Datos  de la Compañía de Sistemas  del Batallón de TIC´S  del comando de Informática y Tecnología  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  TTE. TTMM.  CHRISTIAN ROBERTO MUÑOZ VELASQUEZ |
|  |
| REVISO  Comandante de la Compañía de Sistemas  del Batallón de TIC´S  del comando de Informática y Tecnología  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  CAPITAN 2DO.  INFANTERIA WILDER GILBERTO CUM RAMIREZ |
|  |
| AUTORIZO  Comandante del Batallón de TIC´S  del comando de Informática y Tecnología  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  CORONEL INFANTERIA  HEBER BOORETH MOYA RODRIGUEZ |
|  |
| VISTO BUENO  Comandante del Comando de Informática y Tecnología  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  CORONEL INFANTERIA  RONALD EDUARDO MORALES PEREZ |