REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA DEFENSA
EJÉRCITO BOLIVARIANO
COMANDO

EB-CGEB-DIR-18-24

DIRECTIVA

DÍA	MES	AÑO
22	02	2024

Nº SERIAL	REGISTRO
50 08	00000

NORMAS Y PROCEDIMIENTOS PARA EL USO DEL INTERNET, LA INTRANET, EL CORREO ELECTRÓNICO Y LAS CUENTAS DE ACCESO AL SISTEMA DE PERSONAL EN LAS UNIDADES Y DEPENDENCIAS DEL EJÉRCITO BOLIVARIANO.

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA DEFENSA
EJÉRCITO BOLIVARIANO
COMANDO

Caracas, 23 de febrero de 2024

DIRECTIVA EB–CGEB–DIR-18-24

ASUNTO: NORMAS Y PROCEDIMIENTOS PARA EL USO DEL INTERNET, LA INTRANET, EL CORREO ELECTRÓNICO Y LAS CUENTAS DE ACCESO AL SISTEMA DE PERSONAL EN LAS UNIDADES Y DEPENDENCIAS DEL EJÉRCITO BOLIVARIANO

BASE LEGAL:

- Constitución de la República Bolivariana de Venezuela, Gaceta Oficial N.° 5.908 del 19 de febrero de 2009.
- Ley Constitucional de la Fuerza Amada Nacional Bolivariana, según Gaceta Oficial N° 6.508 del 29ENE20.
- Ley Orgánica de Reforma de la Ley Orgánica de la Fuerza Armada Nacional Bolivariana, Gaceta Oficial Extraordinaria N.° 6.646 del 17 de septiembre de 2021.
- Ley Orgánica de Procedimientos Administrativos, Gaceta Oficial N° 2.818 del 01 de julio de 1981
- Ley Especial Contra los Delitos Informáticos, Gaceta Oficial N° 37.313 del 30 de octubre de 2001.

I. OBJETO

La presente Directiva tiene por objeto regular las normas y procedimientos a seguir para el uso de servicio de internet, la intranet, el correo electrónico zimbra y las cuentas de acceso al sistema de personal, así como mantener las medidas de seguridad necesarias en la administración, distribución y manejo de la información por estos medios.

II. SITUACIÓN

A. La Dirección de Tecnología de Información y las Comunicaciones del Ejército Bolivariano es el encargado de distribuir, regular el uso del internet y el ancho de banda consumido por las distintas direcciones de la Comandancia General del Ejército Bolivariano, y unidades externas al que

le presta el servicio. Así como almacenar y respaldar toda la información de la base de datos del personal militar, que es de interés personal o de la institución. A través de la página Web presta servicios de correo militar zimbra, e información de interés general para el personal militar y no militar.

B. El acceso al internet se rige por las reglamentaciones establecidas por la Comisión Nacional de Telecomunicaciones (CONATEL) y la Oficina Central de Estadística e Informática (OCEI). En el Ejército Bolivariano es a través del proveedor de servicio de internet, CANTV y a su vez un servidor instalado en la Dirección de Tecnología de Información y las Comunicaciones del Ejército Bolivariano, el cual controla y monitorea los accesos a las diferentes páginas Web o servicios de información, llevando un registro de los mismos y manteniendo la seguridad e integridad de la red interna del Ejército Bolivariano (intranet).

C. La Dirección de Tecnología de Información y las Comunicaciones del Ejército Bolivariano ha diseñado la página Web del Ejército Bolivariano, a través de la cual se proporciona información de carácter general de la organización al público interesado que accede esta página por Internet, la misma ofrece a aquellos usuarios que estén autorizados, la posibilidad de realizar consultas tales como: datos básicos del personal del Ejército Bolivariano, Planillas de Liquidación, Netos y Constancias de Trabajos, Sistema de Calificaciones del personal, etc.

D. Para el intercambio de información a través de la Red del Ejército Bolivariano, se utiliza el correo electrónico zimbra, el cual proporciona este servicio al personal militar y no militar orgánicos del Ejército Bolivariano que posean una cuenta y la clave de acceso correspondiente.

E. El auge, expansión y desarrollo que ha experimentado la tecnología de la informática ha traído consigo grandes beneficios para diversos campos de la actividad humana, pero así mismo ha provocado el surgimiento de "Tecnologías Adversas" entre las que se destacan:

1. Virus: es un programa con una serie de instrucciones programadas que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este mismo. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora. Un virus puede ingresar en una computadora a través del correo

electrónico, mensajería instantánea, redes sociales o dispositivos como pendrive, discos duros externos, discos compactos (DC) etc.

2. Caballo de Troya: Es un programa malicioso o malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo que al ejecutarlo le brinda a un atacante acceso remoto y control total al equipo infectado, de forma encubierta sin que el usuario se percate de ello, con la finalidad de robar información o alterar el funcionamiento de la computadora.
3. Gusanos: Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador con la finalidad de colapsar las computadoras y las redes informáticas, impidiendo así el trabajo a los usuarios. El principal objetivo de los gusanos es propagarse y afectar al mayor número de dispositivos posible. Para ello, crean copias de sí mismos en el ordenador afectado, que distribuyen posteriormente a través de diferentes medios, como el correo electrónico, programas P2P entre otros.
4. Bomba lógica o cronológica: Es un código malicioso que se inserta secretamente en una red informática, un sistema operativo o una aplicación de software. Permanece inerte hasta que se produce una condición específica. Cuando esta condición se cumple, la bomba lógica se activa y devasta el sistema dañando datos, borrando archivos o limpiando discos duros. Las bombas lógicas son difíciles de detectar antes de que se active, y puede programarse para que cause el máximo daño y para que se active mucho tiempo después de haber sido "infiltrada" en la computadora o servidor.
5. Adware: También conocido como software de publicidad, muestra anuncios basados en visitas o búsquedas. Además, reduce la capacidad de cómputo del equipo.
6. Spybot: Es un tipo de virus informático espía que recopila información de un dispositivo para transmitirlo a una entidad externa sin el consentimiento del usuario, posiblemente para extorsionarlo.
7. Malware: Altera el funcionamiento normal del equipo al destruir o corromper el sistema operativo o programas. Puede propagarse mediante códigos por correo electrónico.
8. Ransomware: Secuestra la información del equipo mediante cifrado para que el usuario no pueda acceder a ella y de este modo solicitarle un rescate económico. De lo contrario, la información podría destruirse o publicarse en internet.

9. Botnets: Es una red de equipos o de código informático que desarrolla o ejecuta malware. Los atacantes infectan un grupo de equipos con software malicioso conocido como robots o Bots, capaz de recibir órdenes desde su controlador. Los equipos conectados en una Botnet forman una red que proporciona al controlador acceso a una capacidad de procesamiento sustancial. Dicha capacidad puede emplearse para coordinar ataques de denegación de servicios DDoS, enviar correo basura spam, robar datos y crear anuncios falsos en su navegador.
10. Hoax: Son mensajes cuyo contenido no es cierto y que incentivan a los usuarios a que los reenvíen a sus contactos. El objetivo de estos falsos virus es que se sobrecargue el flujo de información mediante correo electrónico y las redes.
11. Hijackers: Son programas que secuestran navegadores de internet, modificando y ralentizando su funcionamiento, ataca a los navegadores Internet Explorer, Edge, Firefox, Google Chrome, Opera, etc.
12. Phishing: Este ataque es de los más comunes y frecuentes. Trata de ofrecer contenidos falsos de forma visual a través de un correo electrónico para que el usuario haga clic e instale un código malicioso en el ordenador.
13. Virus de macro: son códigos escritos para que bajo ciertas condiciones, vinculando sus acciones a modelos de documentos y a otros archivos de modo que cuando una aplicación carga el archivo y ejecuta las instrucciones contenida.
14. Aplicaciones maliciosas o Apps: Cuando instalamos una app en nuestro dispositivo móvil, esta nos pide concederle una serie de permisos. A veces, estos permisos no tienen relación con la funcionalidad de la aplicación o descargamos una aplicación poco fiable que acaba por infectar nuestro dispositivo, tomar control y robar la información que tenemos almacenada en él como contactos, credenciales, imágenes, vídeos, etc.

    Todas las "Tecnologías Adversas" antes descritas son esparcidas principalmente por el uso de unidades de disquetes, memorias USB (pendrives), discos compactos (CD) contaminadas o el llamado "software pirata" y por el internet especialmente a través del correo electrónico bajo la forma de mensajes encubiertos, de aquí la importancia de no "ABRIR" mensajes de dudosa procedencia y la utilización de mensajes en grupos, ya que esto facilita la propagación de estos programas dañinos. Las páginas Web de descargas de películas ilegales, juegos de computadoras y programas son una fuente

de programas maliciosos, que infectan las computadoras alterando su funcionamiento.

F. FORMAS DE IMPEDIR LOS ATAQUES DE TECNOLOGÍA ADVERSAS

1. Instale un programa antivirus de marca reconocida: Con la instalación de un programa de calidad y fiable se detendrá las infecciones a su computadora, además de actualizar constantemente para adaptarse a los virus más recientes.
2. Actualice el sistema operativo con frecuencia: Estas amenazas aprovechan constantemente nuevas vulnerabilidades en el código fuente de los sistemas operativos. Los desarrolladores actualizan el código a través de paquetes o actualizaciones para combatir estas amenazas. Es esencial que actualice con regularidad para aprovechar estas mejoras y aumentar los niveles de seguridad.
3. No descargue nada desconocido o en lo que no confíe: No utilice programas de dudosa reputación (pirateados). Por lo que se hace mayor énfasis en los programas gratuitos. Utilice solo los mejores programas y antivirus de empresas de marca reconocida.

III. DISPOSICIONES

A. DISPOSICIÓN DE CARÁCTER GENERAL:

1. Cada unidad o dependencia del Ejército Bolivariano que tenga acceso al servicio de internet a través de la Dirección de Tecnología de Información y las Comunicaciones del Ejército Bolivariano, tendrá la responsabilidad de velar porque su personal orgánico realice el correcto uso del mismo, así como del intercambio de información a través de la intranet y del correo electrónico zimbra del Ejército Bolivariano, para tal fin se realizará un monitoreo de estos medios y se notificará por escrito a la unidad o dependencia que presente de alguna manera uso indebido de ellos.
2. Cada unidad o dependencia del Ejército Bolivariano será responsable por llevar un registro de las cuentas asignadas a cada uno de sus usuarios orgánicos, así como de realizar el control de entrega y recepción de dichas cuentas cuando su personal sea transferido.
3. Se conformará un comité (multidisciplinario) para determinar el criterio, contenido y enfoque del diseño de la página Web del Ejército Bolivariano y el cual estará integrado por la Dirección de Inteligencia,

la Dirección de Tecnología de Información y las Comunicaciones del Ejército Bolivariano y la Oficina de Gestión Comunicacional.

4. Está prohibido el envío de mensajes por correo electrónico zimbra, cualquiera que sea la índole del mensaje, restringiéndose su uso exclusivamente para temas de trabajo o en asuntos relativos al servicio.
5. El envío de información CLASIFICADA será únicamente por el correo militar zimbra, quedando prohibido el uso de correos electrónicos de otros proveedores para el envío de información.
6. Está prohibido el envío o divulgación de información CLASIFICADA por cualquier medio, tal como lo establece el artículo 550 del Código Orgánico de Justicia Militar, Sección IX, sobre los delitos contra la Seguridad de la Fuerza Armada Nacional, que textualmente dice:
   "Los que revelen órdenes, consignas, documentos o noticias privadas o secretas de las Fuerzas Armadas, serán penados con prisión de cuatro a diez años. Si el hecho hubiere impedido que una operación de guerra produjere las ventajas que debía producir u ocasionare la pérdida o destrucción de fortalezas, naves, aeronaves, cuarteles u otros elementos o pertrechos de guerra, o causado cualquier otro grave daño, la pena podrá ser aumentada hasta en una tercera parte."
7. Está prohibido el acceso a páginas no autorizadas a través del servidor proxy de la Dirección de Tecnología de Información y las Comunicaciones del Ejército Bolivariano, tales como páginas de apuestas, pornografía, etc, así como la modificación de las propiedades del navegador Internet Explorer, Edge, Firefox, Google Chrome entre otros con aplicaciones o plugins, para evadir las restricciones de seguridad del servidor proxy, y acceder a páginas de alto consumo de ancho de banda de internet, como Neflix, YouTube, Tiktok, Redes Sociales etc.
8. Está prohibido el cambio de equipos de computación de los puntos de red asignados y deberá estar asignado por dirección MAC de la tarjeta de red y activar la seguridad de puerto en los switches.
9. Cada usuario militar o no militar, tendrá la responsabilidad directa por el acceso, uso y manejo del internet desde su sitio de trabajo y a través del equipo de computación asignado, siendo responsable por las páginas Web visitadas, del tipo de información consultada, del intercambio de información realizada por la intranet del Ejército Bolivariano, de la información recibida y enviada a través del correo electrónico zimbra u otros correos electrónicos públicos.

10. Los usuarios que tenga asignada una cuenta para el acceso a la base de datos del Ejército Bolivariano, serán responsables directos por el uso debido o indebido de ella, o por el mal manejo de la misma por descuido o negligencia.
11. Serán responsables por la clave personal utilizada para acceder a los diferentes sistemas informáticos, ya que la misma es única e intransferible.
12. Serán responsables por el cambio periódico de su clave de acceso al sistema de base de datos y del correo militar zimbra.

B. DISPOSICIONES DE CARÁCTER PARTICULAR:

1. SEGUNDO COMANDANTE Y JEFE DE ESTADO MAYOR GENERAL DEL EJÉRCITO BOLIVARIANO.
   Informará a las Direcciones y Dependencias integrantes del Estado Mayor General, de lo dispuesto en la presente Directiva a fin de dar fiel cumplimiento a las disposiciones en ella contempladas.
2. GRANDES COMANDOS Y UNIDADES SUPERIORES.
   Informará a las Unidades Subordinadas y Dependencias Adscritas, lo dispuesto en la presente Directiva a fin de dar fiel cumplimiento a las disposiciones en ella contempladas.
3. INSPECTORÍA GENERAL.
   Incluirá en sus guías de verificación las comprobaciones necesarias para asegurar el cumplimiento de la presente Directiva.
4. DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN Y LAS COMUNICACIONES.
   a. Será el Administrador de los diferentes servicios informáticos, tales como el servidor que proporciona la conexión a internet, intranet y del correo electrónico zimbra del Ejército Bolivariano, llevando para tal fin un registro de los usuarios existentes, del nivel de acceso permitido y de las cuentas asignadas.
   b. Ejercerá el control de los accesos al internet, intranet y del correo electrónico zimbra, realizando el monitoreo correspondiente e informando a las Unidades y Dependencias del Ejército Bolivariano que presenten uso indebido de estos servicios informáticos.
   c. Mantendrá actualizada la página Web del Ejército Bolivariano y realizará las modificaciones necesarias, según las recomendaciones que al respecto realice el comité nombrado para tal fin.

IV. VIGENCIA:

La presente directiva entrará en vigencia a partir de la fecha de su distribución derogando lo dispuesto en la directiva N° EJ-AGEJ-DIR-08-01 de fecha 12NOV01 "Normas y Procedimientos para el uso del Internet, la Intranet, el Correo electrónico y las Cuentas de Acceso al Sistema de Personal en las Unidades y Dependencias del Ejército Bolivariano".

Cúmplase

JOSE ANTONIO MURGA BAPTISTA
Mayor General
Comandante General del Ejército Bolivariano

Elaborado

RAFAEL ÁNGEL SUÁREZ RODRÍGUEZ
General de División
Director de Tecnología de Información y las Comunicaciones

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA DEFENSA
EJÉRCITO BOLIVARIANO
COMANDO

DIRECTIVA EB-CGEB-DIR-18-24

NORMAS Y PROCEDIMIENTOS PARA EL USO DEL INTERNET, LA INTRANET, EL CORREO ELECTRÓNICO Y LAS CUENTAS DE ACCESO AL SISTEMA DE PERSONAL EN LAS UNIDADES Y DEPENDENCIAS DEL EJÉRCITO BOLIVARIANO.

DISTRIBUCIÓN:

Original.....	Ayudantía General del Ejército Bolivariano
Copia N° 01.....	Segundo Comando y Jefatura de Estado Mayor General del Ejército Bolivariano
Copia N° 02.....	Inspectoría General del Ejército Bolivariano
Copia N° 03.....	Jefatura del Estado Mayor General del Ejército Bolivariano
Copia N° 04.....	Dirección de Personal del Ejército Bolivariano
Copia N° 05.....	Dirección de Inteligencia del Ejército Bolivariano
Copia N° 06.....	Dirección de Apresto Operacional del Ejército Bolivariano
Copia N° 07.....	Dirección de Planificación y Presupuesto del Ejército Bolivariano
Copia N° 08.....	Dirección de Planificación Estratégica del Ejército Bolivariano
Copia N° 09.....	Dirección de Desarrollo Nacional del Ejército Bolivariano
Copia N° 10.....	Dirección de Investigación, Innovación y Desarrollo del Ejército Bolivariano
Copia N° 11.....	Dirección de Tecnología de Información y las Comunicaciones del Ejército Bolivariano
Copia N° 12.....	Dirección de Adquisiciones del Ejército Bolivariano
Copia N° 13.....	Dirección de Fuerza de Complemento del Ejército Bolivariano
Copia N° 14.....	Dirección de Régimen Especial de Seguridad del Ejército
Copia N° 15.....	Dirección de Educación del Ejército Bolivariano
Copia N° 16.....	Oficina de Gestión Administrativa del Ejército Bolivariano
Copia N° 17.....	Oficina de Gestión Comunicacional del Ejército Bolivariano
Copia N° 18.....	Junta Permanente de Evaluación del Ejército Bolivariano
Copia N° 19.....	6to. Cuerpo de Ingenieros del Ejército Bolivariano
Copia N° 20.....	Comando Logístico del Ejército Bolivariano

Copia N° 21..... Cuartel General del Ejército Bolivariano

Copia N° 22..... Consultoría Jurídica del Ejército Bolivariano

Es copia auténtica.

LEONARDO ANTONIO TRUJILLO CORDERO
General de División
Ayudante General del Ejército Bolivariano

LATC/mpl
2 FEB 14