



**FUERZA AÉREA
DIRECCIÓN DE SISTEMAS DE
INFORMACIÓN Y COMUNICACIONES**

REGULACIÓN GENERAL

FA-EZ-2014-011-O

ASUNTO: PARA LA UTILIZACIÓN DEL CORREO ELECTRÓNICO INSTITUCIONAL ZIMBRA.

Referencias:

- a. Ley orgánica de Transparencia y acceso a la información pública (LOTAIP).
- b. Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos.
- c. Reglamento de la Ley del Sistema Nacional de Archivos.
- d. Reglamento para la elaboración, manejo, custodia, difusión y seguridad de la información militar clasificada RT3-IV 2010.
- e. Orden General Ministerial Nro. 090 del 08 de Mayo del 2013 donde se publicó la Directiva referente al Uso de Correo Electrónico.
- f. Directiva Nro. 2013-01 referente al uso del Correo Electrónico Institucional de Fuerzas Armadas.
- g. Mensaje Militar Nro. 13-DTIC-d-257 del 17 de mayo del 2013 donde el señor Jefe del Comando Conjunto dispone la implementación del correo en Fuerzas Armadas.
- h. Norma Técnica de Gestión de Procesos de la Secretaria de Administración Pública del Ecuador.

A. ANTECEDENTES

1. En base al proyecto de "Mejorar la capacidad operativa y estratégica del Sistema de Mando y Control de las operaciones militares" y oficio donde se definen los estándares tecnológicos para las Fuerzas Armadas, el COTIFA (Comité de Telecomunicaciones e Informática de Fuerzas Armadas) en reunión del 19 de Julio de 2011 determina que la plataforma de correo electrónico para las Fuerzas Armadas será "Zimbra".
2. Para implementar esta solución, el Comando Conjunto de Fuerzas Armadas por medio de la Ejecución del Contrato N° 2011-a-012 para Implementar una Solución de Correo Electrónico Militar para las Fuerzas Armadas, ha provisto de nuevos servidores en las diferentes Fuerzas por medio de los cuales se brinda el servicio de correo electrónico "Zimbra".
3. Las Fuerzas Armadas por medio de la Ejecución del Contrato N° 2011-a-012 para Implementar una Solución de Correo Electrónico Militar para las Fuerzas Armadas,

han provisto de nuevos servidores instalados en las diferentes Fuerzas por medio de los cuales se brinda el servicio de correo electrónico "Zimbra".

4. La suite de colaboración "Zimbra", es una solución de programas informáticos colaborativos para la gestión de correos, agenda y mensajería instantánea entre otros que se pueden agregar como componentes.
5. La implementación de esta herramienta ha sido realizada en el Ministerio de Defensa Nacional, Fuerza Aérea Ecuatoriana y Comando Conjunto de las Fuerzas Armadas por lo que se convierte en un estándar institucional.
6. La suite de colaboración "Zimbra", ha sido probada y utilizada, tanto dentro de la institución como fuera de ella, con resultados muy satisfactorios, además se ha validado su nivel de seguridad con centros de análisis de vulnerabilidades propios y de terceros como la empresa ADHOC.
7. En la actualidad la demanda de información exige que el intercambio de datos entre dependencias se realice de manera ágil y segura para lo cual se debe utilizar eficientemente la herramienta de correo electrónico.

B. PROPÓSITOS

1. Disponer y normar el uso correcto del servicio de Correo Electrónico "Zimbra", para la transmisión y recepción de mensajes para todo el personal que labora en la Fuerza Aérea Ecuatoriana.
2. Establecer las normas, políticas y responsabilidades del uso del correo electrónico "Zimbra".

C. DISPOSICIONES

1. GENERALES

- a. Usar el correo "Zimbra", como medio oficial para todo el personal militar y civil de la Fuerza Aérea, en mensajería instantánea y electrónica.
- b. Transmitir información por este medio, exclusivamente de interés institucional.
- c. El servicio de correo electrónico debe estar disponible para todo el personal de la Fuerza Aérea; el acceso contará con un equipo conectado a la red de las Fuerzas Armadas o hacia internet.
- d. No usar el correo electrónico institucional "Zimbra", para la difusión de cadenas, mensajes personales ajenos a la Institución, cualquier propósito comercial o financiero, político, religioso o temas similares. Su incumplimiento será motivo de sanción de acuerdo a los reglamentos en vigencia.
- e. Transmitir los correos electrónicos oficiales por este medio; se prohíbe el uso de cuentas de servicio gratuito (Hotmail, Gmail, Yahoo, entre otros), controlado directamente por el área tecnológica, que gestiona el acceso a la red de Internet.
- f. No utilizar información de carácter personal o privado desde la cuenta institucional, ya que es de completa responsabilidad del usuario; para su uso lo hará desde correos externos fuera del área de trabajo.

2. ESPECÍFICAS

a. Comandos, Direcciones y Repartos

- 1) Supervisar la disponibilidad del servicio de correo institucional "Zimbra".
- 2) Fomentar el uso de "Zimbra" en sus dependencias.

b. DIRSICOM y SICOM en los repartos

- 1) La DIRSICOM debe nombrar a un señor Oficial como administrador del Correo Electrónico Institucional "Zimbra", con el fin de cumplir y hacer cumplir la regulación.
- 2) Proveer de una cuenta y clave de acceso al personal militar y servidores públicos, en su respectivo reparto.
- 3) Llevar un registro detallado con la nómina de los usuarios que se han registrado para tener acceso al correo electrónico.
- 4) Capacitar a los usuarios en la utilización y explotación del correo electrónico "Zimbra" como medio de transmisión y recepción de mensajes.
- 5) Solucionar en el menor tiempo posible, problemas de orden técnico que se presenten con el correo electrónico.
- 6) Estructurar las cuentas para usuarios de la siguiente manera : la primera letra del nombre seguido del primer apellido (rflores@fae.mil.ec), de existir un homónimo, se utilizará del nuevo usuario, el segundo nombre seguido del apellido carlosflores@fae.mil.ec, continuando con este último proceso en adelante de acuerdo a las circunstancias.
- 7) Almacenar todos los mensajes transmitidos, en el servidor de correo electrónico institucional "Zimbra".
- 8) Mantener la cuenta de correo electrónico, activa mientras el usuario este prestando servicios en la institución; para lo cual, el Departamento de Talento Humano informará las novedades existentes, como ingresos o salidas de la Institución, cambios de grado y designación orgánica.
- 9) Sincronizar y habilitar el correo electrónico, contactos y agenda con dispositivos móviles a través del administrador, previa autorización del Director de la DIRSICOM.
- 10) Ser el responsable del uso y gestión de sus cuentas de correo electrónico.
- 11) Adoptar medidas preventivas, para garantizar el buen funcionamiento del correo electrónico en forma permanente.

c. Dirección General de Talento Humano

- 1) Reportar por escrito a la DIRSICOM, los cambios o novedades del personal civil y militar de la Fuerza Aérea, al ingresar o salir de la institución así como sus cambios orgánicos para su actualización en el sistema.

d. Administrador ZIMBRA:

- 1) Mantener el servicio disponible las 24 horas del día los 365 días del año, con el servicio de correo electrónico, pudiendo exceptuarse por tareas de mantenimiento previamente planificadas o por motivos de fuerza mayor, las cuales deben ser informadas a los usuarios; todas las áreas relacionadas a la provisión de este servicio, trabajaran en conjunto para una mejora constante del nivel porcentual de disponibilidad del servicio.
- 2) Diseñar e implementar la arquitectura o diseño de la solución de correo electrónico usando el software "Zimbra" en todos los repartos de la Fuerza Aérea y ajustarse a los requerimientos y mejores prácticas que el fabricante del software defina en los documentos de diseño que ha generado para este fin, contando indispensablemente con alta disponibilidad en todos sus componentes y capacidad de crecimiento de infraestructura.
- 3) Administrar eficientemente la infraestructura de correo electrónico compuesta básicamente por:
 - Hardware de alta disponibilidad.
 - Software de alta disponibilidad.
 - Infraestructura de respaldos.
 - Entidad de Certificación para emisión de Certificados Digitales.
 - Infraestructura de sincronización y réplica.
- 4) Diseñar e implementar mecanismos de respaldo; es responsabilidad de la Dirección de Sistemas de Información y Comunicaciones FAE, proveer de los medios para este fin y que sean ligados a la configuración de una solución de respaldo como del hardware para su almacenamiento.
- 5) Actualizar constantemente a las nuevas versiones que el fabricante del software haya liberado, previo a que la versión que esté en funcionamiento haya salido de soporte.
- 6) Establecer el espacio designado para el buzón de correo de cada usuario, en función del perfil del usuario y del espacio de almacenamiento disponible.
- 7) Crear las cuentas de los usuarios y establecer una contraseña de acceso temporal, que deberá ser cambiada por el usuario, la primera vez que ingrese a la cuenta de correo electrónico, ajustándose a los requerimientos que para este fin se han definido.
- 8) Activar, cancelar o suspender las cuentas de correo electrónico, previa notificación al usuario o del ente que administre la gestión del Talento Humano.
- 9) Definir los procedimientos a seguir por los usuarios finales en caso de:
 - Capacitación a Usuario Final.
 - Actualización de plataforma tecnológica.
 - Aplicación de parches y factibilidad de recuperación al estado anterior en caso de falla de instalación.
 - Pérdida de claves y percepción de robo de información.
 - Comprometimiento de certificados digitales y claves de usuario final.

- Fraudes y delitos cibernéticos ligados al uso de correo electrónico.
 - Presencia de SPAM.
- 10) Identificar y coordinar con el CSIRT (Computer Security Incident Response Team), área de seguimiento a delitos cibernéticos del Comando Conjunto de las Fuerzas Armadas los incidentes reportados y detectados relacionados con la afectación a la disponibilidad, confidencialidad e integridad de la información que fluye por el servicio de correo electrónico, generada por entes internos o externos a la red de datos de las Fuerzas Armadas.
 - 11) Planificar y ejecutar pruebas de validación de estado de los servicios de Alta disponibilidad y continuidad del Correo Electrónico.
 - 12) Realizar monitoreo continuo de los servicios de la infraestructura de correo electrónico así como de los reportes generados por el servicio Anti Virus/Anti Spam detectando anomalías y corrigiéndolas, como resultado de este trabajo se deberá manejar bitácoras de seguimiento y monitoreo, las cuales serán definidas por el ente administrador del servicio.
 - 13) Validar constantemente el estado y capacidad de reposición de información (respaldos), generados por el mecanismo automático de respaldo.
 - 14) Establecer las clases de servicio del sistema de correo electrónico y asignar a los usuarios según su rol y perfil con la respectiva publicación y autorización de la Dirección de Sistemas de Información y Comunicaciones Fuerza Aérea Ecuatoriana.
 - 15) Revisar que los respaldos de información correspondientes a cuentas de usuario y buzones de correo se realicen correctamente.
 - 16) Brindar a los usuarios el soporte y la asistencia que requieran en coordinación con el área de soporte técnico de acuerdo a sus procesos.
 - 17) Es responsabilidad del administrador la instalación y configuración del cliente para sincronización en los dispositivos móviles de los usuarios autorizados.

e. Usuarios correo ZIMBRA

- 1) Administrar la cuenta, la identificación y la clave de acceso es responsabilidad exclusiva del usuario de la misma.
- 2) Verificar el tamaño máximo para el envío de mensajes, sea de 10 Mb, evitando la saturación en el buzón y en el canal de comunicaciones; sin embargo este tamaño podrá ser modificado en base a un requerimiento escrito formulado al Director de la DIRSICOM de la Fuerza Aérea.
- 3) De existir la necesidad, de enviar información en tamaños extensos y a fin de evitar problemas de red con otros usuarios, anchos de banda y errores en la infraestructura instalada, solicitar su requerimiento por escrito.
- 4) No enviar archivos con extensión .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta, y cualquiera que en la evolución del tiempo, se lo considere riesgoso o que facilite la propagación de virus. Los archivos se eliminarán automáticamente al ser identificados como virus, enviándose una notificación al usuario de la

acción realizada. En caso de existir necesidad de enviar este tipo de archivos y se conoce de manera real su origen, es indispensable que previamente sean comprimidos y enviados.

- 5) El usuario debe recordar que el uso del correo electrónico institucional es personal e intransferible.
- 6) Cada usuario es responsable de la contraseña de acceso a su cuenta de correo institucional; en caso de que sea comprometida y accedida por terceros, será su responsabilidad, así como las consecuencias que esto pudiera ocasionar.
- 7) Se debe crear la contraseña ajustándose a las normas de seguridad, la que debe ser de al menos 10 caracteres en combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
- 8) Evitar la reutilización de contraseñas por motivos de seguridad; la clave debe ser cambiada periódicamente, al menos una vez por mes.
- 9) No escribir las contraseñas, en papeles junto a las estaciones de trabajo o libretas, estas deben ser memorizadas por el usuario.
- 10) Solicitar en caso de olvido o pérdida de la contraseña, al administrador del servicio la generación de una nueva clave; este procedimiento no implicará pérdida de información en la cuenta de correo electrónico del usuario.
- 11) Transmitir toda la información o contenido, por medio del correo electrónico es su única responsabilidad, que de ser supuesta prueba de delito deberá ser sometida a un debido proceso legal.
- 12) Enviar cifrada todo mensaje que contenga información calificada.
- 13) Enviar la información en forma masiva, será previa autorización de la DIRSICOM. El número máximo de destinatarios establecido es de 10.
- 14) Depurar continuamente las carpetas de mensajes recibidos y enviados, para no tener problemas con el espacio de almacenamiento asignado a su buzón.
- 15) Mover los mensajes no solicitados, o de origen desconocido (SPAM) a la carpeta de SPAM y la base de conocimiento sea retroalimentada, es su responsabilidad. SPAM, es un correo comercial no solicitado o simplemente correo basura a los mensajes enviados de forma automatizada y masiva.
- 16) Compartir, delegar libretas de contactos, agenda, maletín o carpetas designadas por el dueño de la cuenta está autorizado; sin embargo no se exime de responsabilidad en el cumplimiento de tareas o responsabilidades asignadas; independientemente de la acción de la persona a quien delegue.
- 17) Revisar que todos los mensajes enviados cuenten con un PIE DE FIRMA, en el que se detalle claramente:
 - Nombre del Emisor y Cargo.
 - Rango o Título profesional.
 - Entidad y departamento a la que pertenece el emisor.

- Números de contacto telefónicos .
 - Mensaje de uso correcto de información entregada por este medio.
 - Mensaje de responsabilidad del emisor de los criterios emitidos por este medio y que no son de responsabilidad de la Institución.
- 18) No catalogar todos los mensajes, como de acceso público; deberán ser enviados de manera cifrada y firmados digitalmente.
- 19) De acceder al servicio de correo electrónico, desde Internet y haciendo uso de lugares públicos; es su responsabilidad los posibles problemas que puedan presentarse, ya que al no contar con conocimiento de los equipos y el software instalado en los mismos, facilita la interceptación de la información confidencial, como usuarios y contraseñas, que no le exime de las consecuencias por pérdida de información.
- 20) Aceptar y firmar el documento de conocimiento y aceptación de políticas de uso del servicio de correo electrónico y certificados digitales previo a la habilitación del servicio.

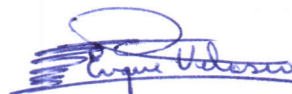
D. VIGENCIA

A partir de la fecha de aprobación sin perjuicio de su publicación en la Orden General de la Fuerza Aérea.

E. DEROGATORIA

Dejase sin efecto la Regulación General REGSICOM No.2010-02 del 23 de julio 2010 PARA LA UTILIZACION DEL CORREO ELECTRONICO LOTUS NOTES.

Quito, D.M..... 29 MAR 2014



Enrique Velasco Dávila
Teniente General

COMANDANTE GENERAL DE LA FUERZA AÉREA



Autenticado



Raúl Banderas Dueñas
Brigadier General

JEFE DEL ESTADO MAYOR GENERAL DE LA FUERZA AÉREA

Distribución: Comando General - Grandes Comandos - Unidades y Repartos FAE

 SFC/RMQ/ SML/P. Paz y Miño