# Uso del Correo Electrónico

DISTRIBUCIÓN FORMATO PDF

| Elaboró: | Revisó: | Autorizó: |
|---|---|---|
| Carlos Mauricio Bolaños Guerrero<br>Coordinador de Área de Infraestructura Tecnológica | Héctor Armando Chinchilla Salegio<br>Gerente de Tecnologías de Información y Comunicación | Jorge Alberto Hernández Recinos<br>Director General de Administración |
| 24/04/2019 | 26/04/2019 | 07/05/2019 |

**INDICE**

## I OBJETIVO

Que el personal usuario conozcan los criterios, obligaciones y controles para lograr el uso correcto y eficiente del correo electrónico del MARN.

## II CAMPO DE APLICACIÓN

Aplicable por la Gerencia de Tecnologías de Información y Comunicación y por todo el personal del MARN que tenga asignado una cuenta de correo electrónico institucional.

## III BASE LEGAL

| ARTÍCULO | NOMBRE DE LA NORMATIVA APLICABLE |
|---|---|
| NORMAS TÉCNICAS DE CONTROL INTERNO ESPECÍFICAS DEL MARN<br>DECRETO NÚMERO 14; DE 07 JUNIO 2016; DIARIO OFICIAL NO.132, TOMO NO.412 DE FECHA VIERNES 15 DE JULIO DE 2016 | |
| Art.25 | El Ministro deberá establecer a través de la Unidad organizativa encargada de las Tecnologías de Información y Comunicación, la normativa interna para la administración y conservación de equipo de comunicaciones, cómputo, software, red y base de datos. |
| Art.30 | Las políticas y procedimientos de los controles generales de los sistemas de información automatizados, del uso de equipo informático se establecerán en la Normativa interna respectiva |
| Art.49 | Se establecerán políticas y procedimientos, que permitan el control en la asignación, uso y seguridad física del equipo de cómputo, servidores, impresores y cualquier otro equipo relacionado con su funcionamiento.<br><br>Todos los programas o aplicativos instalados deberán están amparados con licencias para la instalación y uso, extendidas por el fabricante. |

## IV DEFINICIONES

**Antivirus**: programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido o cualquier medio de almacenamiento

**Gerencia de Tecnologías de Información y Comunicación (GTI):** unidad organizativa del MARN del Nivel de apoyo, que tiene como objetivo[1] Usar de forma racional e innovadora las herramientas de Tecnologías de Información y Comunicación (TIC), entregando servicios de calidad a las diferentes áreas del ministerio, facilitándoles así el acceso oportuno a la información necesaria para la toma de decisiones y a los recursos para optimizar las operaciones diarias.

**Encriptación:** operación que transforma datos legibles en ilegibles con el objeto de resguardar cierta información que viaja por la red.

**Firewall:** sistema o programa que se coloca entre un ordenador o red local e Internet para garantizar que todas las comunicaciones sean seguras, previniendo de esta manera el ataque de los hackers y crackers a los puertos del sistema.

**Hardware:** es lo que se conoce como la parte física tanto del ordenador como de los diferentes periféricos

[1] Manual de Organización MARN

**Password:** palabra o conjunto de caracteres que se usa para identificar a un usuario autorizado.

**PC:** computadora Personal: computador personal u ordenador, conocida como PC (siglas en inglés de personal computer), es un tipo de microcomputadora diseñada en principio para ser utilizada por una persona a la vez. Una computadora personal es generalmente de tamaño medio y es usada por un solo usuario.

**Red:** sistema de comunicación de datos que conecta sistemas informáticos situados en diferentes lugares.

**Servidor:** computadora con infraestructura tecnológica robusta, donde se ejecutan programas que realizan alguna tarea en beneficio de otras aplicaciones o PC clientes.

**Software:** diferentes programas que pueden utilizar las máquinas y que permiten realizar las diferentes acciones o tareas al hardware.

**Spyware:** tipo de software que se instala en las computadoras sin el conocimiento ni el consentimiento de estos, y recopilan información o habilitan acciones que podrían exponer a la máquina a algún tipo de ataque.

**Username (Nombre de usuario):** cadena de caracteres que se utiliza para identificar a un usuario en la entrada a un sistema (login), como un servicio online, un sistema operativo, una red..

**Usuario:** conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso, (persona, máquina, programa).

**Virus:** programa que "infecta" una computadora. Software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información.

**Web:** sistema de información basado en el "hipertexto". Los usuarios pueden crear, editar y visualizar documentos de hipertexto.

**Xls:** extensión de archivos elaborados en Microsof Excel

## V DESARROLLO

### A. Instrucciones generales de uso del correo electrónico

Todo personal que se le asigne una cuenta de correo electrónico institucional debe hacer un buen uso de esta y del resto de medios. Con ese objetivo debe cumplir estas normas:

a. El MARN facilita una cuenta de correo electrónico institucional a los empleados de esta Cartera de Estado, ya sea que estén contratados con fondos GOES o externos;
b. Cada empleado que tenga una o más cuentas de correo asignadas es responsable de todas las acciones que se lleven a cabo en su utilización;
c. Este servicio tecnológico es controlado por la GTIC, y podrá ser monitoreado e intervenido cuando se detecte algún tipo de comportamiento inusual en el envió o recepción de mensajes

d. Las cuentas de correo electrónico institucionales son publicadas en el sitio web del MARN y estarán a disposición del público en cumplimiento de la legislatura correspondiente.

**B. Usos admitidos y no admitidos del correo electrónico**

Para el uso de correo electrónico institucional el personal del MARN tiene permitido lo siguiente:

a. La cuenta de correo electrónico institucional puede emplearse con fines personales o domésticos que no sea abusivo y no perjudique la seguridad de los sistemas de información de la institución, ni el normal desarrollo de las funciones que la persona tenga encomendadas;
b. El acceso al correo institucional puede hacer a través de dos vías: web y aplicación instalada en cada computadora o dispositivo móvil;
c. Se permite el envío de adjuntos hasta un máximo de 25mb dependiendo del cliente de gestión del correo configurado en el equipo;
d. Se permite el uso de cuentas de correo personales y en caso de contingencia podrán ser utilizadas para envío de información oficial.

Para el uso de correo electrónico institucional el personal del MARN tiene prohibido lo siguiente:

a. Utilizar la cuenta de correo electrónico para actividades profesionales ajenas a las tareas institucionales encomendadas;
b. Que los usuarios que tengan atribuida la gestión de cuentas de correo genéricas institucionales asociadas a determinados trámites, no podrán en ningún caso hacer uso de ellas con fines personales;
c. El envío de correos masivos (spam) utilizando la dirección de correo electrónico;
d. El uso del correo electrónico corporativo vulnerando los derechos de terceros, o para la realización de actos de carácter ilícito;
e. El envío y recepción de adjuntos con extensiones ZIP, BAT, CMD, EXE, COM, PIF, REG, SCR, VB, VBE, CAB, YAR, VBS.

**C. Plataforma Antispam**

El MARN cuenta con una plataforma para el filtrado del correo, en la cual se analiza todos los correos entrantes y salientes considerando criterios ya establecidos. Para los correos entrantes la plataforma agrupa los considerados sospechosos y notifica al usuario 3 veces al día para que los depure.

La depuración consiste en liberar o eliminar el correo, con esto, queda guardada la opción elegida y la próxima vez que llegue un correo con los mismos criterios la plataforma le dará el tratamiento elegido.

Cuenta con un portal de administración de correos permitidos y bloqueados, a la que todos los usuarios pueden acceder para cambiar las preferencias.

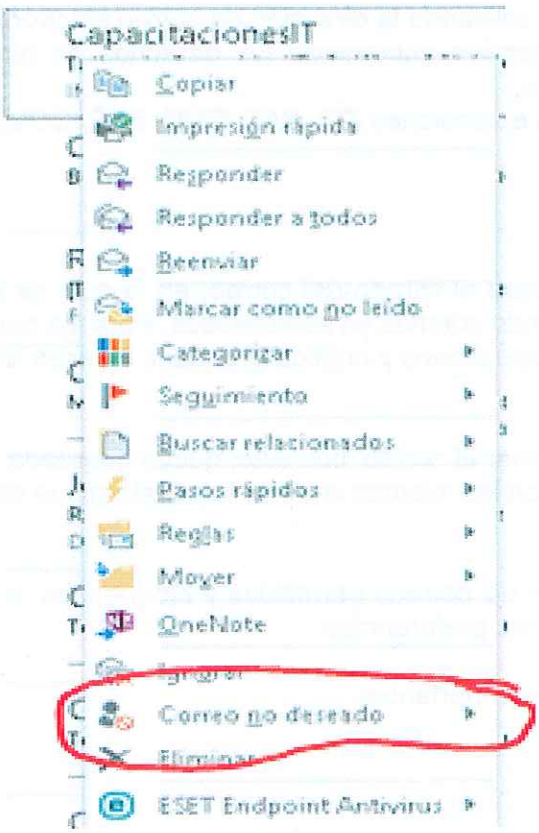
Para el usuario hay dos consideraciones importantes:

a. Si recibe un correo con las características de la imagen presentada a continuación, fácilmente puede elegir si lo acepta (Liberar), o lo borra (Borrar).

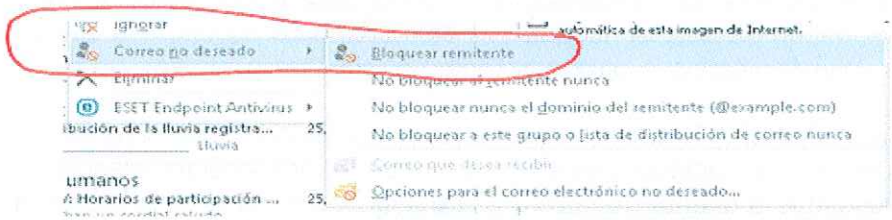

b. Hay correo que la herramienta AntiSpam no los cataloga como correo no deseado, pero que para nosotros como usuarios si lo son. Para estos casos existen 2 opciones:

- Bloquearlo para que no ingrese a ninguna cuenta del MARN: Para lograrlo, cada usuario debe reenviarlo inmediatamente a la cuenta soportetecnico@marn.gob.sv, y colocaremos la cuenta de correo no deseada en los filtros de protección perimetral.
- Bloquearlo solo para mi cuenta: Si el correo recibido, lo considera no deseado, pero probablemente sea de interés para otros usuarios, se debe bloquear desde su cuenta personal, siguiendo en outlook los siguientes pasos:

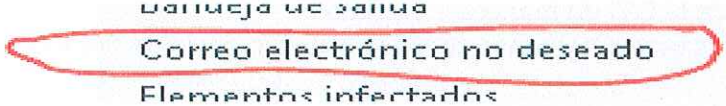
  En la bandeja de entrada se selecciona el correo a bloquear dando click derecho, despliega el siguiente listado y seleccionamos: Correo no deseado.



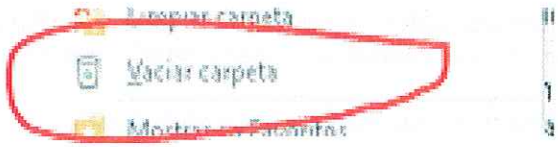
Al seleccionar correos no deseados nos despliega el siguiente listado en el cual seleccionamos: Bloquear remitente.




Así quedará bloqueado ese correo llegando a la carpeta de correos electrónicos no deseados.




El cual se tiene que vaciar periódicamente dándole clic derecho para encontrar la opción de vaciar carpeta.




**D. Envíos masivos**

Para el envío de correos a más de 25 direcciones simultaneas y que sea de manera recurrente, se debe hacer por medio de listas, creadas en sus clientes gestores de correo electrónico o solicitar a la GTIC la creación de una lista de correo en el servidor.

**E. Gestión del buzón de correo**

Corresponde a cada usuario velar que la gestión de la información contenida en su buzón de correo electrónico sea adecuada. Para ello debe revisar periódicamente la bandeja de entrada y la de salida, como mínimo una vez al día. En este sentido, se recomienda eliminar los mensajes que no deban conservarse y archivar el resto en la carpeta o subcarpeta apropiada, especialmente los que tengan contenido laboral.

Los mensajes que formen parte de un procedimiento, u otros que deban conservarse, tienen que estar debidamente archivados en el expediente correspondiente, puesto que es previsible que se borren al cabo de un tiempo o se llegue a un tope de capacidad.

Los correos electrónicos con fines privados deben ser borrados o movidos cada día por si es necesario hacer un traspaso o eliminación de la cuenta por motivos laborales.

## F. Medidas de seguridad

Los usuarios deben cumplir las siguientes medidas de seguridad:

a. La contraseña del correo estará embebida en la configuración del cliente de correo electrónico;
b. Los empleados deben guardar el usuario y la contraseña de acceso a la cuenta de correo de forma segura y no facilitarlos a otras personas, ni siquiera a efectos de mantenimiento del sistema;
c. No utilizar una contraseña fácilmente deducible, cumpliendo con los criterios establecidos por el servidor, que son: 8 caracteres con al menos 1 número y 1 letra mayúscula;
d. Bloquear el acceso a la cuenta de correo y el equipo informático, en caso de ausentarse del puesto de trabajo durante la jornada;
e. No seguir cadenas de mensajes piramidales;
f. No abrir mensajes sospechosos;
g. En caso de detectar una incidencia durante el uso del correo electrónico, el usuario debe hacerlo del conocimiento de la GTI de manera inmediata;
h. La GTI no envía correo solicitando ingresar a un vínculo web o envió de credenciales.

## G. Normas de buen uso del correo electrónico

a. Utilizar la opción de reenviar solo en los casos en que la persona destinataria pueda acceder tanto al emisor del mensaje como a su contenido, y a toda la información de la cadena de correos que formen parte de él;
b. Colocar pie de página institucional con el nombre, cargo, dirección o jefatura, y números de contacto. Cuando se trate de mensajes con fines personales, deberá suprimirse el pie de la firma;
c. Revisar el tamaño del documento a enviar y verificar que no sobrepase los 25mb;
d. Valorar la utilización de la opción de copia oculta para enviar un correo electrónico a múltiples destinatarios;
e. Deberán eliminarse las direcciones de los destinatarios que no estén involucrados con el tema a tratar, con objeto de no difundir injustificadamente direcciones de correo de terceros al reenviar un correo electrónico;
f. Identificar de forma clara y concisa el asunto;
g. No incluir datos personales en el asunto;
h. Evitar palabras o expresiones que puedan activar los programas antispam (reguladas por estándares internacionales).

## H. Ausencia del usuario

En caso de ausencia programada superior a 3 días, el titular de la cuenta de correo debe notificar a la GTI para activar el mensaje de ausencia de oficina, y facilitar otra dirección de contacto que garantice la continuidad de la actividad.

## I. Cese de la relación laboral

a. El MARN cancelará la prestación del servicio de correo electrónico en el momento de finalizar la relación contractual con el empleado o cuando el usuario esté haciendo un mal uso de dicho servicio, a no ser que el jefe de la unidad solicite expresamente lo contrario;

DIRECCIÓN GENERAL DE ADMINISTRACIÓN 1

b. El usuario tiene derecho a obtener los mensajes personales de las cuentas de correo que en aquel momento estén almacenados en la carpeta de mensajes personales que designe o que puedan identificarse como tales. El resto de mensajes pueden analizarse con el fin de determinar si resultan necesarios para la continuidad de la actividad o bien si pueden suprimirse.

## J. Acceso al correo electrónico fuera del MARN

Cuando se utilice el correo electrónico institucional en computadoras fuera de la institución debe tenerse en cuenta lo siguiente:

a. No hacer uso de la opción de guardar la contraseña;
b. Borrar el historial de navegación y cerrar la sesión, al terminar, siempre que se utilice una computadora de uso compartido para acceder al correo vía web;
c. Asegurarse que la computadora cuenta con antivirus.

## K. Acceso a los correos electrónicos por parte de la GTI

La GTI puede hacer controles automatizados sobre el uso del correo electrónico en la aplicación de los clientes, para velar por el normal funcionamiento de la plataforma (volumen de tráfico, volumen de los mensajes enviados, etc.). Solo se accederá al contenido de los mensajes o de los documentos adjuntos cuando no puedan utilizarse otros mecanismos menos intrusivos, concretamente en los siguientes casos:

a. Para llevar a cabo tareas de mantenimiento o vinculadas a la seguridad del sistema. En tales casos, se informará al usuario de las tareas que deben llevarse a cabo y se le ofrecerá la posibilidad de estar presente;
b. Para comprobar, en relación con una información reservada o un procedimiento disciplinario, el uso del correo electrónico, en aquellos casos en los que haya indicios de que el usuario ha hecho un mal uso. El acceso debe hacerse en su presencia.

## L. Consecuencias del incumplimiento de estas normas de uso del correo electrónico

El incumplimiento de lo establecido en este instructivo, será advertido formalmente por escrito, por parte de la GTI, sin perjuicio de la aplicación, si procede, del régimen disciplinario correspondiente.

## VI REGISTROS

| CÓDIGO | REGISTRO |
|---|---|
| | |
| | |
| | |

## VII HOJA DE CONTROL DE MODIFICACIONES

| REVISIÓN ANTERIOR | REVISIÓN ACTUAL | DESCRIPCIÓN DEL CAMBIO | FECHA |
|---|---|---|---|
| | | Revisión inicial. | 07/05/2019 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

DIRECCIÓN GENERAL DE ADMINISTRACION 1