MANUAL DE POLÍTICAS QUE NORMAN EL USO DE CORREO ELECTRÓNICO INSTITUCIONAL Y EL ACCESO A INTERNET

Acuerdo del Tribunal Supremo de Elecciones en Sesión Ordinaria n.º 072-2011, celebrada el 04 de agosto de 2011

Comunicado por Circular n.º STSE-0019-2011 de 04 de agosto de 2011

1. Gestión del Servicio

1.1. Todo funcionario del Tribunal Supremo de Elecciones con acceso a la red institucional, también tendrá acceso al uso de internet y correo electrónico.

1.2. La cancelación de dichos servicios deberá gestionarse formalmente por parte de la jefatura correspondiente, ante la Sección de Servicio al Cliente de TI, con la justificación respectiva.

2. Normas

2.1. ***Asignación y desactivación de cuentas de correo electrónico***

2.1.1. La capacidad máxima de almacenamiento del buzón de correo será de 10 MB.

2.1.2. Las cuentas de correo serán desactivadas al día siguiente de la fecha en la cual la persona termine oficialmente su vinculación con el TSE o cuando la jefatura así lo solicite. Es responsabilidad de las jefaturas de la institución notificar a la Sección de Atención al Cliente TI los cambios o movimientos del personal a su cargo que cuenten con algún servicio de correo electrónico o Internet, ya sea por traslado, despido o renuncia, entre otros.

2.1.3. Es responsabilidad de Recursos Humanos enviar un correo electrónico mensualmente a la Sección de Atención al Cliente de TI con el listado de movimientos del personal de la institución.

2.1.4. Quienes no utilicen correctamente su cuenta de correo pueden ser sancionados conforme al Reglamento Autónomo de Servicios.

2.2. ***La cuenta de correo electrónico***

2.2.1. Se entiende por cuenta de correo electrónico la asignación por parte del TSE de:

a) Una dirección electrónica con la forma *usuario@tse.go.cr*

b) Un buzón (espacio en disco) para almacenar los mensajes.

c) Una palabra clave o password para acceder de manera privada a la cuenta.

d) La posibilidad de enviar y recibir mensajes dentro del TSE y hacia Internet utilizando la dirección electrónica asignada.

2.2.2. Con el fin de garantizar que la identificación del usuario en la dirección de correo sea única, se seguirán las siguientes reglas para construir cada identificación: se construirá con las iniciales del nombre del usuario y el primer apellido (sin tildes ni signos propios de algunos idiomas). En caso de presentarse coincidencias en la identificación de dos usuarios se resolverá de acuerdo con el orden de procesamiento: el primer usuario recibirá la identificación antes mencionada, el segundo será alterado recurriendo a las primeras letras del segundo apellido. Por ejemplo, si hay dos usuarios, uno José Ramírez Prado y otro Jorge Ramírez Prendas, el primero recibiría la identificación de usuario *jramirez@tse.go.cr* y el segundo sería *jramirezp@tse.go.cr.* Para las personas que cuenten con direcciones de correo definidas desde hace varios años, su identificador de usuario no tendrá validez y será construido uno nuevo bajo esta regla.

2.2.3. La cuenta de correo electrónico es personal e intransferible, por lo que se deben tener claves seguras y no se puede compartir la cuenta. Las dependencias o grupos de trabajo (proyectos) que tengan asignada una cuenta deben nombrar un usuario autorizado para manejarla. Cada persona, o el usuario autorizado, es responsable por la seguridad de su cuenta y de su clave. La primera vez que el usuario reciba su cuenta de correo, deberá cambiar su clave. Por seguridad, la clave debe cambiarse mínimo cada tres meses.

2.2.4. Los usuarios del servicio de correo del TSE podrán recibir y enviar mensajes desde programas (clientes) de correo que utilicen los protocolos

SMTP, POP e IMAP ó a través de navegadores Web. Los clientes de correo autorizados son Outlook Express, Microsoft Outlook, Entourage y Thunderbird. Los navegadores Web autorizados son Internet Explorer, Safari, Firefox y Google Chrome. Es responsabilidad del usuario la selección del cliente de correo que utilizará, cuya configuración podrá ser solicitada a la Sección de Servicio al Cliente de TI, desde el cual se prestará el respectivo servicio.

2.2.5. Aunque la Institución cuenta con un servicio de revisión de virus para los mensajes de correo entrante, los usuarios deberán verificar que los mensajes que se reciban o se envíen no incluyan virus, para lo cual su programa antivirus deberá estar activo y mantenerse actualizado. Es responsabilidad de cada usuario verificar lo anterior, en caso de duda deberá comunicarse con la Sección de Servicio al Cliente de TI.

2.2.6. Para reportar problemas, hacer sugerencias o realizar cualquier solicitud que tenga relación con cuentas de correo o el servicio de correo electrónico en general, debe efectuarse una llamada o enviar una comunicación a la Sección de Servicio al Cliente de TI.

2.2.7. Es responsabilidad de cada usuario tener copias de respaldo (backup's) de los mensajes de sus carpetas de correo y de su agenda de direcciones electrónicas.

3. Políticas de Administración del Servicio de Correo Electrónico.

3.1. La violación de la seguridad de los sistemas de Internet y/o de la red, puede acarrear responsabilidad civil y/o penal de conformidad con la legislación vigente. En caso de que se inicie una investigación al respecto, el TSE colaborará con las autoridades correspondientes.

3.2. La Sección de Infraestructura del DTIC, con la ayuda de herramientas especializadas, procederá con el filtrado de los archivos que vengan anexados al correo electrónico, con extensiones tales como: .exe, .bat, .wav, .mp3, .mpg, entre otros que pudieran considerarse peligrosos, con el fin de garantizar la seguridad de la red.

4. Uso del Correo Electrónico

Es responsabilidad de los usuarios:

4.1. Usar su cuenta con fines laborales de acuerdo con su función en el TSE y lo establecido en el documento integral de políticas de seguridad en su numeral del 080108 uso aceptable del correo electrónico, aprobado por el Tribunal Supremo

de Elecciones en sesión ordinaria Nº 36-2007, comunicado mediante oficio Nº STSE-1865 del 24 de abril de 2007.

4.2. Usar un lenguaje apropiado en sus mensajes.

4.3. No se utilizará el logo institucional.

4.4. El correo (e-mail) no tiene garantía de ser privado. Recuerde que existen personas que se dedican a tratar de "capturar" información que viaja a través de Internet, por lo tanto nunca ponga en un mensaje de correo información que no pondría en un sobre.

4.5. Una buena regla es: sea conservador en lo que mande y liberal en lo que reciba. No debe mandar mensajes "calientes" (llamados "flames") aunque sea provocado. No se sorprenda si recibe "flames" y es prudente no responderlos.

4.6. En general, se aconseja al menos revisar el asunto (subject) antes de responder un mensaje y asegúrese que los mensajes que responda vayan dirigidos a usted.

4.7. Sea cuidadoso cuando envíe su correo. Hay algunas direcciones que pueden ir a un grupo, pero que parece ser la de una persona. Cerciórese a quién le manda datos o información.

4.8. Conozca a quien contactar por ayuda. Usualmente tendrá recursos cerca y a la mano. Además sepa a quien recurrir si recibe algo cuestionable o ilegal. Para ayuda en estos casos puede recurrir a la Sección de Servicio al Cliente de TI.

4.9. Las expectativas para comportarse por medio de e-mail, dependen de las relaciones con una persona y el contenido de la comunicación. Las normas aprendidas en un ambiente de e-mail particular, no necesariamente aplican en general a los mensajes a través del Internet. Sea cuidadoso con los vulgarismos o acrónimos locales.

4.10. El costo de la entrega del mensaje es compartido entre el que lo manda y quien lo recibe. Esta es una razón económica fundamental por la cual el correo no solicitado no es bienvenido.

4.11. No envíe ni conteste cadenas de correo o cualquier otro esquema de "pirámide" de mensajes.

4.12. No use su cuenta para fines comerciales.

4.13. No se debe transmitir virus o programas de uso mal intencionado.

4.14. Los usuarios no deben leer correo ajeno ni generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.

4.15. Se prohíben las violaciones de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia del TSE.

4.16. No se debe introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, etcétera).

4.17. No revele la clave ó código de su cuenta, ni permita su uso a terceros para actividades ajenas a la misión del TSE. La prohibición incluye particulares.

4.18. El usuario debe evitar suscribirse a cualquier lista de correo que genere mensajes cuyo contenido no tenga que ver con las funciones del TSE.

4.19. Se prohíbe el uso del correo electrónico con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil, sin importar el idioma, la periodicidad o tamaño del mensaje.

4.20. Se prohíbe hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios del TSE.

4.21. Se prohíbe realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios. Entre las acciones que contravienen la seguridad de la red se encuentran (aunque no están limitadas por éstas) acceder a datos cuyo destinatario no es usted, ingresar a una cuenta de un servidor o de una aplicación para la cual no está autorizado. Para efectos de estas políticas la palabra "interrupción" incluye, pero no está limitada a, capturar tráfico de la red, inundar de pings la red, realizar spoofing de paquetes, ataques de negación de servicios (DoS) o falsificar información de enrutamiento y de configuración de los equipos con el objetivo de aprovechar alguna vulnerabilidad de los sistemas.

4.22. Se prohíbe el uso de comandos o programas o el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

4.23. Se prohíbe el envío de mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado ese tipo de material (e-mail

spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).

4.24. Es obligación de los usuarios reportar a la Sección de Servicio al Cliente de TI cualquier tipo de irregularidad o abuso de estos servicios, para evitar que esto le vuelva a suceder o que le ocurra a otros funcionarios.

4.25. El usuario se asegurará de no responder a todas las personas cuando se envíen comunicados generales o para un grupo específico de personas, a excepción de que ésta sea la finalidad de la respuesta.

4.26. El TSE se reserva el derecho de monitorear mediante el DTIC las cuentas que presenten un comportamiento sospechoso para su seguridad, lo que no incluye acceso al contenido de los correos.

4.27. El tamaño de los mensajes con archivos adjuntos no debe exceder los 3 MB. Este tamaño puede ser chequeado por medio de las propiedades de cada archivo, desde el Explorador de Windows o bien seleccione el archivo y presione ALT+ENTER para ver el tamaño. Para esto tome en cuenta lo siguiente:

a) Si el archivo adjunto excede de 3 MB, se requiere enviar un correo electrónico al Jefe de la Sección de Infraestructura, dirección *infraestructurati@tse.go.cr* con el fin de que incremente el límite para tal envío; para este propósito se requiere conocer las direcciones tanto del emisor como de lo(s) receptor(es). El administrador de correo procede a aumentar este límite, el cual será temporal y será válido únicamente para el día solicitado.

4.28. Con el fin de agilizar el envío de información, no se podrán enviar mensajes masivos (que involucre a todos los usuarios del TSE), a menos que sea un asunto oficial. El usuario será el responsable por el contenido de los mensajes a efecto que cumplan la característica de ser mensajes oficiales y de carácter laboral.

5. Con respecto al servicio de Internet

El uso de la red Internet y del correo electrónico, constituye una herramienta y recursos que la Institución pone al servicio de sus funcionarios para que puedan realizar de una forma más eficiente y eficaz sus labores y así contribuyan al logro de los objetivos y metas institucionales. En tal sentido se debe acatar lo establecido en el documento integral de políticas de seguridad en su numeral del 080106 uso aceptable de internet, aprobado por el Tribunal Supremo de Elecciones en sesión ordinaria Nº 36-2007, comunicado mediante oficio Nº STSE-1865 del 24 de abril de 2007 y las siguientes normas:

5.1. Evitar la **transferencia de cualquier tipo de archivos**, a través de servicios de mensajería como ICQ, MSN Messenger**,** etc.

5.2. No bajar **música** y **video** (especialmente no emplear servicios como KaZaA, Morpheus, GNUtella, o similares).

5.3. No participar en **juegos** de entretenimiento en línea (por ejemplo: World Fusion, MSN Games, etc.)

5.4. Verificar que todos los archivos que se copien a su computadora no contengan **virus**.

5.5. Emplear el menor número de instancias del explorador de Web en forma simultánea; es decir, no tener innecesariamente varias ventanas abiertas a la vez.

5.6. Si no está navegando por el Web, debe cerrar todas las ventanas abiertas de su explorador.

5.7. Corre por cuenta o riesgo del usuario cualquier información que obtenga por medio del servicio de Internet.

5.8. Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. En ningún momento dichos mensajes podrán emplearse en contra de los intereses institucionales, de personas individuales, así como de ninguna otra institución.

5.9. La demanda de servicios puede ocasionalmente exceder la disponibilidad, por lo que serán establecidas las prioridades, dando la más alta a las actividades consideradas esenciales para llevar a cabo la misión del TSE.

5.10. La "navegación" en Internet queda delimitada única y exclusivamente para fines propios del TSE, los cuales están referidos a búsqueda de información necesaria para la elaboración, ampliación o referencia de temas relacionados con el trabajo de la Institución.

5.11. Se prohíbe el uso de Internet para cualquier actividad que sea lucrativa o comercial de carácter individual o privado.

5.12. No se podrá acceder a sitios con contenido sexual o pornográfico, ni bajar o ver material inapropiado, no sólo referido a juegos, música y pornografía, sino a cualquier otro material inaudito, que atente contra los principios morales, sociales y en general que no se relacionen con los objetivos de la institución.

5.13. El acceso a este servicio del TSE (tse.go.cr) es una concesión que puede ser revocada en cualquier momento, si se detecta uso indebido o acción que contradiga lo dispuesto en este documento. Cualquier violación de las normas acá descritas puede resultar en la revocatoria temporal o permanente del acceso al servidor, sin perjuicio de las sanciones contempladas en la normativa atinente.

5.14. No se deberá usar este servicio para fines no identificados con la misión de la institución y con la optimización de su eficiencia administrativa.

5.15. El uso de Internet no debe interferir negativamente con la dedicación de los usuarios a sus actividades laborales.

5.16. No se podrán cambiar las configuraciones originales dejadas por los técnicos de la Sección de Servicio al Cliente de TI.

5.17. Se prohíbe el uso ftp, telnet, etc, sin autorización salvo casos justificados y tramitados mediante la Sección de Servicio al Cliente de TI.

5.18. Se prohíbe estrictamente que un computador conectado a la red del TSE se comunique a Internet por medio de un *módem.* El usuario que requiera conectarse a Internet por esta modalidad, deberá gestionarlo ante la Sección de Servicio al Cliente de TI, de conformidad con lo que se establece en el punto 1 de este documento.

5.19. Es interés del DTIC el proteger la información de la institución de los riesgos externos que se encuentran en Internet, por lo que este departamento a través de la Sección de Infraestructura procederá a filtrar la navegación a los sitios de internet que visitan los funcionarios de la institución según el contenido de las páginas , a través de herramientas especializadas para ello, las siguientes son las premisas básicas del filtrado:

a.) Sitios permitidos: Se permitirá la navegación en aquellos sitios que estén referidos a búsqueda de información necesaria para la elaboración, ampliación o referencia de temas relacionados con el trabajo de la institución;

b.) Sitios bloqueados: Se bloquearan aquellos sitios que contengan pornografía, chats, juegos de entretenimiento, azar y apuestas, sitios racistas y de odio, música y video, transferencia de cualquier tipo de archivos a través de mensajería, servicios de radio y TV por demanda y todos aquellos que no estén asociados a los propósitos laborales de la institución.

5.20 Las jefaturas de departamento tendrán la potestad de solicitar a la Sección de Servicio al Cliente TI, reportes o informes de navegación hacia internet de los funcionarios a su cargo cuando lo consideren pertinente.

Términos y definiciones

Protocolo:	Conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.
Protocolo SMTP *(Protocolo simple de transferencia de correo)*:	Protocolo utilizado para el intercambio de mensajes de correo electrónico
Protocolo IMAP *(Protocolo de acceso a mensajes de Internet)*:	Protocolo de acceso a mensajes en Internet con el que es posible examinar el correo directamente desde el servidor del mismo modo que si estuviese descargado en la PC.
Protocolo POP *(Protocolo de oficina de correos)*:	Permite únicamente recibir o recoger correos electrónicos de un servidor.
Protocolo FTP *(Protocolo de transferencia de archivos)*	Es un protocolo para la transferencia de archivos entre sistemas conectados a una red, desde un equipo se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.
Protocolo TELNET *(TELecommunication NETwork)*	Protocolo que permite acceder a otra máquina para manejarla remotamente, para que esta conexión funcione, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones.
Gestor de correo	Aplicativo que facilita la tarea de recepción, revisión y envío de correo electrónico a través de una cuenta configurada en un único programa.
Gestor de correo Outlook Express	Es un cliente de correo electrónico producido por Microsoft para las plataformas Windows.
Gestor de correo Microsoft Outlook	Programa que opera como cliente de correo electrónico de Microsoft y brinda múltiples servicios como buzones compartidos, calendarios comunes, etc.
Gestor de correo Entourage	Es un cliente de correo electrónico y gestor de información personal que se utiliza en los equipos MAC OS. Proporciona calendario, libreta de

	direcciones, lista de tareas, lista de notas, etc.
Gestor de correo Thunderbird	Gestor de correo electrónico, soporta IMAP/POP, similar al Outlook Express.
Navegador Web	Aplicación que permite interpretar sitios web o información de archivos los cuales podemos acceder a través de Internet.
Navegador Internet Explorer	Navegador web desarrollado por Microsoft para sistemas operativos Windows.
Navegador Safari	Navegador Web desarrollado por Apple, disponible para sistemas operativos MAC, iPhone, iPod Touch, iPad y Microsoft Windows.
Navegador Firefox	Navegador web libre y de código abierto, multiplataforma ya que está disponible para varios sistemas operativos como Microsoft Windows, MAC OS X, Linux, etc.
Navegador Google Chrome	Navegador desarrollado por Google, al igual que el Firefox es multiplataforma.
Mensajes calientes "flames"	Cualquier tipo de mensaje ofensivo que llega por medio de email, grupo de noticia o de chat, cuando se responden estos tipos de mensajes inicia un ataque al cual se denomina Flame War.
Cadena de mensajes	Consiste en un mensaje que intenta inducir al receptor a realizar algún número de copias de este para luego pasarlas a uno o más receptores.
Cadena de mensajes por correo esquema de pirámide	Es un tipo de cadena que utiliza correo electrónico como forma de propagación, su razón es su capacidad de crecimiento exponencial y comportamiento de progresión. Estos mensajes pierden efectividad cuando el conjunto de re-emisores han leído y comienzan a recibirlo de vuelta.
Virus	Es un programa dañino que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Pueden destruir de manera intencionada los datos almacenados en los equipos, también existen otros más inofensivos que se caracterizan por ser molestos.
Software malicioso y Programas de uso mal	Llamado Malware es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento del propietario, existe una amplia variedad de software hostil, intrusivo o molesto que causa efectos específicos en el computador, pensados por el autor a la hora de crearlo.

intencionado *(Malware)*	
Worms	Un gusano es un tipo de software dañino que tiene la propiedad de duplicarse a sí mismo, a diferencia de un virus este no precisa de alterar los archivos de programas, sino que reside en la memoria y se duplica a si mismo provocando como por ejemplo, problemas de consumo de ancho de banda en la red.
SPAM o Ráfagas de correo electrónico no solicitado	Llamados mensajes basura son mensajes no solicitados o no deseados o de remitente desconocido, habitualmente de tipo publicitario y generalmente enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.
Capturar tráfico de la red	La utilidad principal de los programas que capturan tráfico de la red es la de analizar el tráfico o paquetes que se transmiten o reciben con la intención de conocer o modificar el contenido de la información que se transfiere por la red sin que sea advertido por las víctimas.
Pings a la red & Ataques de denegación de servicio (DoS)	Su objetivo es degradar considerablemente o detener el funcionamiento de un servicio o dispositivo de red, se puede realizar de varias formas. Por ejemplo; enviando comandos masivos de Windows llamados PING que no permiten que circulen los paquetes de información de los usuarios, bloqueando cuentas por excesivos intentos de login fallidos, o envío de archivos de información mal configurados de manera que la aplicación que debe interpretarlo no puede hacerlo y colapsa.
Falsificar información de enrutamiento	Se utiliza para hacer que los sistemas proporcionen información errónea (mientan entre sí), y así provocar una denegación de servicio o hacer que el tráfico de paquetes o información siga una ruta que, normalmente no seguiría, esto permitiría el monitoreo de la información a través de una conexión insegura por parte de un atacante.
Spoofing de paquetes	Sucede cuando un atacante modifica la dirección de la estación origen, falsificando su identificación para hacerse pasar por otro usuario, de esta manera, un atacante puede asumir la identificación de un usuario valido de la red, obteniendo sus privilegios.