POLÍTICA DE USO DE CORREOS ELECTRÓNICOS, INTERNET Y OTROS RECURSOS TECNOLÓGICOS PARA LA PRESIDENCIA DE LA REPÚBLICA

Disposiciones Generales y Definiciones

1. Objetivo

Definir las normas de uso de correos electrónicos, internet y otros recursos tecnológicos para todos los servidores públicos que laboran en la Presidencia de la República, con el fin de proteger la información de la Institución asegurando su disponibilidad e integridad; además de garantizar la eficiente administración de las herramientas sufragadas y mantenidas con fondos públicos y otorgadas exclusivamente para realizar la función pública.

2. Alcance

La presente política funcionará como un instructivo administrativo de aplicación y observancia obligatoria para todos los servidores públicos de la Presidencia de la República (en adelante la institución o CAPRES) que tengan recursos informáticos asignados en razón de sus funciones dentro de la Institución. Cualquier equipo que tenga acceso a la red de interconexión ya sea Internet o Intranet mediante cualquier método de conexión, aunque no sea propiedad de la Institución, quedará sujeto a los términos y condiciones contenidos en esta política. En el momento de la conexión se darán a conocer los términos y condiciones establecidos por la Institución.

La administración, control, supervisión y seguridad de los recursos informáticos de la institución estará a cargo de la Dirección de Innovación Tecnológica e Informática de la Presidencia de la República (ITIGES). Dicha Dirección implementará los mecanismos tecnológicos necesarios para detectar acciones u omisiones que contravengan el presente documento, informando oportunamente al departamento de Recursos Humanos o a las Jefaturas correspondientes para los efectos legales consiguientes.

3. Definiciones

Para los efectos de esta política se entiende por:

a. Contraseña: Mecanismo de autenticación que utiliza una combinación de caracteres y que es conocida por personas autorizadas con el objetivo de ingresar a la información restringida a través de cualquier dispositivo tecnológico.
b. Dirección de Innovación Tecnológica e Informática (ITIGES): Dirección de la Presidencia de la República de El Salvador encargada de la gestión de tecnología.

c. Dispositivos móviles de uso institucional: Comprenden computadoras portátiles, PDA, dispositivos MP3, teléfonos inteligentes y similares provistos por ITIGES.

d. Encriptar: (Cifrar, reducir, compendiar) Procesamiento de transformación de datos, donde el texto plano es convertido en texto "ilegible" a través de un algoritmo que traspone o sustituye los caracteres iniciales por otros no descifrables.

e. Firma Electrónica Certificada: Mecanismo que garantiza la confiabilidad y seguridad de las transacciones y trámites mediante una serie de códigos encriptados y dispositivos para garantizar la autenticidad entre partes que por diversas razones no ha podido, pueden o podrán encontrarse presencialmente.

f. Normativa: Conjunto de leyes, reglamentos, políticas, manuales y normas que regulan en desempeño de la Institución en distintos aspectos.

g. Recurso tecnológico: Equipos informáticos y sus periféricos, servicios y dominios de correo electrónico, espacio físico en servidores, conexión a internet, redes locales y cualquier servicio o equipo electrónico que tenga relación con la actividad de intercambio y manejo de información para CAPRES, sus Secretarías, dependencias y cualquier programa que opere en ellos.

h. Red de comunicaciones: Conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información, recursos, servicios etc.

i. Servidor público de la Institución o servidor público: Persona natural que presta servicios ocasional o permanentemente, remunerados o ad honórem, que ejerzan su cargo por elección, nombramiento, contrato u otra modalidad dentro de la Presidencia de la República.

j. Usuario de los recursos informáticos: Toda persona que, dentro o fuera de CAPRES, ha recibido acceso a cualquier recurso tecnológico previa autorización de ITIGES. Además de aquellos que no pertenezcan a la Institución, pero que conecten sus equipos a la red de CAPRES.

k. 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.

l. Aplicaciones tecnológicas: Comúnmente llamados "software", son un conjunto de códigos lógicos que permiten automatizar uno a varios procesos.

Normas Generales

4. De la utilización de los recursos informáticos

El usuario debe utilizar el correo electrónico, el internet y los otros recursos tecnológicos de la Institución únicamente para el cumplimiento de los fines para los cuales están destinados y que correspondan directamente a las facultades o actividades del ejercicio de su función dentro de la Institución. Por tanto, toda la información que sea almacenada en los recursos tecnológicos deberá de ser de interés y beneficio para la Institución.

5. **De las cuentas de correo electrónico institucional**

Podrá asignarse una cuenta de correo electrónico institucional a los servidores públicos para el cumplimiento de sus facultades o el ejercicio de sus funciones, por solicitud del jefe o funcionario superior inmediato. Estas cuentas son intransferibles, inviolables y su creación deberá ser solicitada mediante comunicación escrita a ITIGES a través de los procedimientos establecidos por dicha Dirección.

6. **De la conexión de los recursos informáticos**

Todos los equipos que se conecten a la red de la Presidencia de la República deben recibir una dirección IP única que los identifique, un nombre de red asignados por ITIGES y contar con un soporte de Antivirus. Además de ser incluidos en la base de datos correspondiente junto con la información del responsable del equipo. Para llevar a cabo la conexión de cualquier equipo informático a la red deberá seguirse el procedimiento establecido por ITIGES.

7. **De las limitaciones de uso**

La Institución podrá establecer limitaciones con respecto al uso de los recursos, incluyendo el número máximo de mensajes de correo electrónico que pueden ser enviados o recibidos por una cuenta, el tamaño máximo de algún mensaje de correo electrónico que pueda ser enviado o recibido y el espacio de disco máximo que será asignado en los servidores de la Institución para su beneficio.

8. **De la confidencialidad de la información**

Todo el personal de la Institución deberá garantizar el buen uso y manejo de la información contenida en todos los recursos tecnológicos que le han sido asignados por la Institución exclusivamente para el desempeño de sus labores.

Ningún servidor público de CAPRES podrá divulgar, extraer, recopilar o sustraer información de los equipos informáticos de la institución sin la autorización del titular de la información.

Instalación, contraseñas y manejo de los recursos

9. **Instalación de recursos informáticos**

La instalación y reinstalación de cualquier recurso tecnológico será realizada por ITIGES de acuerdo a la solicitud de parte de la unidad administrativa que lo requiera. Posterior a la instalación, se prohíbe el traslado del recurso a otro lugar sin el conocimiento previo de ITIGES, pues en ese caso no se garantiza el cumplimiento de los requerimientos técnicos necesarios de instalación y funcionamiento. Se consideran casos excepcionales a la obligación anterior los supuestos de fuerza mayor tales como: incendios, terremotos, calamidades públicas y en general cualquier situación que amenace con la pérdida o destrucción de información de CAPRES; en cuyo caso la obligación del servidor público recae en ubicar el equipo informático en un lugar seguro.

10. Configuración de contraseñas

Todo servidor público que tenga asignado cuenta de correo electrónico institucional, internet o acceso a otros recursos informáticos, deberá asignar y administrar su contraseña (*password*) de acuerdo a las indicaciones provistas por ITIGES.

11. Manejo de recursos

Previo al manejo del recurso tecnológico asignado, es responsabilidad de ITIGES como del usuario corroborar que se cumplan los siguientes puntos:

a. Al momento de recibir cualquier recurso tecnológico, el usuario al que se le está asignando dicho recurso deberá revisar el estado del mismo e informar a ITIGES de cualquier daño o desperfecto que presente o cualquier accesorio que faltara.
b. Antes de utilizar cualquier recurso tecnológico de la Institución, el usuario deberá estar previamente capacitado para su manejo. Para ello ITIGES instruirá, capacitará o proveerá guías a los nuevos usuarios en los aspectos que considere necesarios;
c. El usuario siempre manipulará el recurso atendiendo las indicaciones proporcionadas por ITIGES; si al estar utilizando el recurso se presentara algún problema o sufriere daños, deberá reportarlo inmediatamente a ITIGES.

Operación de recursos

12. Lugar y horario de operación

El usuario utilizará los recursos dentro de los horarios laborales establecidos que cada unidad establecerá con base a sus necesidades. En caso que el usuario necesite trabajar más allá del horario establecido o en días no hábiles, deberá notificarlo al jefe de su unidad especificando las razones y el uso que le dará al equipo fuera del horario establecido; a su vez, será notificado a ITIGES de acuerdo al procedimiento previamente indicado por dicha Dirección para este aspecto. Si el usuario, por las funciones que desempeña, está autorizado para utilizar algunos de los recursos tecnológicos fuera de la Institución deberá tomar medidas de seguridad y protección de los recursos informáticos.

Internet

13. Uso responsable y racional

El usuario del equipo es responsable por el buen uso del Internet, este recurso es estrictamente para el desarrollo de sus funciones y como apoyo para cada actividad que necesite en sus labores diarias. El recurso de Internet es limitado y compartido por todos los usuarios de la Institución por lo que debe limitarse su uso a exclusivamente a este fin.

14. Bloqueo y restricciones

Por el resguardo de la seguridad del personal y la integridad de los equipos, automáticamente se bloquean sitios de las categorías de pornografía, crimen, ocio, entretenimiento, juegos, películas y otros similares que no estén vinculados con el trabajo de la Institución según esté estipulado en el reglamento de usos tecnológicos de CAPRES. Los usuarios que necesiten navegar en sitios bloqueados que por su trabajo lo requieran, pueden solicitar por medio de una justificación autorizada por su jefe inmediato los desbloqueos permanentes, temporales o por horarios, según sea el caso.

Software de escritorio

15. Instalación de software

La instalación de programas es responsabilidad exclusiva de ITIGES. Todos los equipos de la Institución poseen instalado aplicaciones tecnológicas de seguridad como antivirus y/o antimalware. En el caso de que no se encuentre instalado, los usuarios deberán notificarlo a ITIGES para su inmediata instalación. Si para el desempeño de sus funciones, algún usuario necesita software adicional deberá notificarlo a ITIGES con previa autorización de la jefatura inmediata.

16. Restricciones

No está permitida la descarga, instalación o utilización de las siguientes categorías de aplicaciones tecnológicas o software:

a. Software de entretenimiento o aquel cuyo objetivo sea establecer relaciones personales ajenas a los objetivos del trabajo que el usuario tiene asignado en la Institución. Concretamente, queda prohibido el uso de juegos, programas de mensajería instantánea y similar.
b. Software cuyo objetivo es evitar las limitaciones que los administradores establecen sobre recursos informáticos, por ejemplo, aquellos programas que permiten acceder a sitios Web prohibidos por los administradores.
c. Software que puede servir para el pirateo de programas o infracción de los derechos de la propiedad intelectual, como programas P2P (*Peer-to-peer*) o similares.

17. Licencias de programas

El uso de los programas se ajustará a las indicaciones contenidas en los contratos de licencias; cualquier duda sobre las operaciones que legalmente están autorizadas para realizarse dentro o con los programas deberá consultarse con ITIGES. Se prohíben las copias ilícitas de cualquier programa y por ende la venta de los mismos. La reproducción o copia de software se ajustará a lo que determine la licencia del mismo.

18. Otras consideraciones

A continuación se especifican ciertas consideraciones que deben aplicarse y tenerse en cuente en el empleo de los recursos tecnológicos desarrollados en esta sección.

a. En equipos propiedad de la Institución se debe utilizar únicamente fondos y protectores de pantalla institucionales proporcionados por ITIGES.
b. Para usar diskettes, CD, DVD o memorias USB, estos deberán ser analizados previamente a través del programa antivirus.
c. La extracción de sistemas de almacenamiento removibles (como memorias USB o cualquier otro dispositivo de almacenamiento) se realizará solo después de utilizar la opción que para ello existe en el sistema operativo.
d. Se deben extraer de la computadora los medios removibles (CD-ROM, USB o cualquier otro dispositivo de almacenamiento) que contengan datos confidenciales o información reservada.
e. Nunca invalidar, desinstalar o detener la ejecución de aplicaciones de la Institución y/o software (por ej.: controles de seguridad, antivirus, etc.)
f. En caso de ausencias, el usuario deberá apagar los dispositivos completamente o bloquear la sesión y apagar el monitor. Las ausencias incluyen tiempo de almuerzo, reuniones en otras oficinas o fuera de la Institución.
g. Al final de la jornada laboral, el usuario deberá apagar el equipo mediante la opción de "Apagar" del sistema operativo y no desconectando el equipo de la alimentación eléctrica ni presionando directamente el botón de encendido.

19. Correo electrónico institucional

La cuenta de correo electrónico institucional es personal, inviolable e intransferible. Si una cuenta no presenta ningún tipo de transacción en el periodo de treinta días, esta se bloqueará automáticamente; y luego de 90 días se eliminará del servidor. La utilidad primordial del correo electrónico institucional es facilitar la comunicación e intercambio de insumos de trabajo entre los usuarios de la Institución o con personas externas a la misma; es importante aclarar que cada unidad administrativa decidirá aquellos asuntos que deberán tratarse por canales tradicionales de comunicación.

La información transmitida mediante el servicio de correo electrónico institucional es responsabilidad única y exclusiva del usuario que la genera. El contenido de los mensajes de correo electrónico institucional no gozará de validez jurídica, en tanto no correspondan formalmente a un procedimiento administrativo previsto en cualquier normativa aplicable a la Institución. Se exceptúan los correos electrónicos remitidos por servidores públicos a particulares en cumplimiento de una habilitación legal.

20. Prohibiciones de uso

Se prohíbe utilizar la cuenta de correo electrónico institucional para los siguientes fines:

a) Como dirección de contacto para asuntos personales, fines comerciales, políticos y religiosos.

b) Para suscribirse a noticias, boletines, publicidad y cadenas de correo diferentes a los fines de la institución.

c) Realizar comunicaciones de contenido pornográfico, ilícito o degradante en cualquier forma entre servidores públicos de la Presidencia y particulares.

Queda estrictamente prohibido la instalación del correo electrónico institucional en dispositivos móviles y equipos informáticos no autorizados por ITIGES.

21. Conservación

Es responsabilidad de cada usuario tener copias de respaldo (*backup's*) de los mensajes de sus carpetas de correo electrónico y de su agenda de direcciones electrónicas; en caso de desconocer las herramientas para la realización de estas acciones podrá solicitar asistencia a ITIGES. Los usuarios deberán extraer de la cuenta institucional aquellos correos electrónicos que tengan información relevante y respalden elementos de algún procedimiento desarrollado en la Institución, almacenando los correos en el expediente o procedimiento correspondiente.

22. Recepción de correo

Para evitar la posibilidad de virus, se recomienda no abrir mensajes del correo electrónico institucional cuando se reciban mensajes no esperados – Aunque provengan de personas conocidas - y estos contengan archivos adjuntos. Además, se deben borrar los mensajes catalogados como *spam* o correo basura sin leerlos de forma periódica. En caso de duda, se podrá consultar al soporte tecnológico de ITIGES.

23. Envío de correo

Son de obligatorio cumplimiento las indicaciones para el correcto envío de correos electrónicos dentro de la Institución, las cuales consisten en: a. Verificar el destinatario y el contenido del mensaje antes de enviarlo; b. Al enviar un archivo adjunto se debe comprimir - siempre que sea posible - e indicar en el asunto del mensaje el contenido de dicho archivo; c. Usar la firma automática institucional que especifica el puesto y el aviso de confidencialidad institucional; d. No desinstalar la firma automática del gestor de correo; e. Las listas de distribución de correo solo deberán usarse para mensajes relacionados con la finalidad de las mismas. Los usuarios podrán consultar con ITIGES para conocer las indicaciones de uso de las listas de distribución.

Dispositivos tecnológicos

24. Protección de dispositivos móviles

El usuario deberá asignar una contraseña segura para proteger el dispositivo y minimizar el riesgo en caso de extravío o robo según se encuentre estipulado en el reglamento sobre el uso de los recursos tecnológicos de

CAPRES. Además, deberá asegurarse que cuente con software de encriptamiento, antivirus, antimalware y firewall personal - cuando sea aplicable – y que dicho software esté actualizado y activo en todo momento. En ausencias de la Institución, los dispositivos móviles serán guardados en un lugar no visible y asegurados de forma física, preferiblemente bajo llave.

25. Reporte de extravío, robo o hurto

Cuando un recurso tecnológico sea extraviado, robado o hurtado, los usuarios inmediatamente notificarán a ITIGES por medio de un escrito formal. Para el caso de robo o hurto, los usuarios deberán anexar al escrito la certificación extendida por la Policía Nacional Civil o por la Fiscalía General de la República que respalde el robo o hurto, según sea el caso. Dicha certificación será gestionada directamente por el usuario involucrado.

26. Devolución de equipo informático

Una vez finalizada la utilización de cualquier recurso tecnológico gestionado por ITIGES, el usuario deberá entregar el equipo al departamento de Recursos Humanos, quien a su vez notificará de inmediato a ITIGES para que esta Dirección revise las condiciones de devolución del bien. Las razones por la finalización de la utilización incluyen renuncia, despido, finalización de contrato, traslado de unidad o asignación de nuevo equipo.

27. Impresiones y fotocopias

En lo que se refiere a la impresión y fotocopias, con el fin de hacer un uso responsable de los recursos, el usuario deberá:

a. Promover los mecanismos necesarios para que los diferentes departamentos de la institución puedan gestionar y realizar transferencia de documentación de forma electrónica, ya sea mediante correo electrónico, dispositivos tecnológicos o aplicaciones tecnológicas de gestión documental. Minimizando así el uso de papel de forma innecesaria.
b. Fomentar la lectura de documentos de forma digital para minimizar la impresión de los mismos. Imprimir solamente en casos necesarios y que no fuera posible archivar la información en versión digital. Se deben imprimir únicamente documentos relacionados con las actividades laborales.
c. Imprimir documentos en doble cara y emplear programas administradores de impresión que permitan imprimir varias páginas por cara, cuando esto sea posible. Además, reutilizar el papel reciclado para imprimir o hacer fotocopias siempre que el papel no contenga información confidencial o reservada.
d. Implementar el uso de aplicaciones tecnológicas de flujos de trabajo y mecanismos de firma electrónica certificada para la aprobación de documentos sin necesidad de imprimirlos según lo permita la ley.
e. Utilizar dentro de los diferentes departamentos de la Institución el uso del mecanismo de "control de cambios" de los procesadores de texto para realizar cambios e imprimir un documento cuando este sea la versión final.

f. Recoger los documentos directamente de la impresora, especialmente cuando estos contengan información confidencial.

28. Respaldo de información

El usuario deberá realizar una copia de cualquier comunicación electrónica realizada con fines institucionales, en el equipo informático asignado para su uso. ITIGES borrará quincenalmente los correos electrónicos cuya antigüedad en los servidores sea mayor a una semana. Si por permisos laborales o asignación de misiones oficiales fuera del país, el usuario no ha tenido acceso a su cuenta de correo electrónico institucional, deberá notificar a ITIGES para evitar el borrado automático.

29. Protección de recursos tecnológicos

Para mantener en las óptimas condiciones los recursos tecnológicos y garantizar la integridad de la información contenida en los mismos, los servidores públicos deberán:

a. Almacenar información en formato digital únicamente en los equipos suministrados por la Institución.
b. Los recursos tecnológicos deberán ser operados únicamente por el usuario asignado, a excepción de autorizaciones para algunas jefaturas que sean notificadas previamente a ITIGES.
c. No abrir los equipos para tratar de repararlos o para extraer o adicionar componentes de los mismos.
d. Abstención de golpes, destrozos o movimientos bruscos de los equipos informáticos, así como de tensionar excesivamente los cables que los conectan.
e. Evitar ingerir alimentos y bebidas cerca o cuando se trabaja directamente con el equipo informático.
f. No colocar adhesivos, calcomanías o *stickers* sobre el equipo que no tengan relación con el trabajo de la institución.

30. Sanciones

El incumplimiento de las presentes normas dará lugar a la aplicación de sanciones administrativas previstas en la ley para los servidores públicos de la Institución. En el procedimiento de la aplicación de sanciones deberá otorgarse los plazos legales para que el servidor público infractor haga valer su defensa ante la imputación que se le atribuya. En caso de sanción, la decisión se anexará al expediente personal del empleado.

31. Disposición final

Para el desarrollo adecuado de la presente política, la Dirección de Innovación Tecnológica de la Presidencia desarrollará y comunicará lineamientos, instructivos o manuales que permitan ejecutar los procedimientos

relacionados con el manejo de los recursos informáticos apegados a esta normativa. La presente política entrará en vigencia a partir de esta fecha.

El presente instrumento se emite en cumplimiento al Acuerdo No.210 de fecha 23 de julio de 2014, por medio del cual el Presidente de la República faculta al Secretario Privado de la Presidencia para que a Propuesta del Director de Innovación Tecnológica e Informática de la Institución, emita y autorice la Política de Uso de Correos Electrónicos, internet y otros Recursos Tecnológicos para la Presidencia de la República.

San Salvador, 29 de julio de 2014

Autorización: _____

Lic. José Manuel Melgar Henriquez
Secretario Privado de la Presidencia de la República

Propuesto y Elaborado: _____

Ing. Jorge Alberto Oliva Viscarra
Director en funciones Dirección de Innovación Tecnológica de la Presidencia