Instituto Interamericano de
Cooperación para la Agricultura

Política de tecnologías de la información y comunicación

Setiembre, 2021

Tabla de contenido´

I. Presentación

Atendiendo el compromiso de mejorar y modernizar los procesos administrativos y tecnológicos para hacer un uso racional, equitativo y transparente de los recursos, el IICA establece las disposiciones contenidas en la presente Política, la cual se complementa con los procedimientos descritos en el Manual de procedimientos de tecnologías de la información y comunicación.

El propósito de este documento es mejorar la eficiencia, eficacia y gestión de los servicios tecnológicos del Instituto, garantizando una gestión oportuna, segura, confidencial, integral, pertinente y respetuosa de las normas y estándares internacionales de las tecnologías de información y comunicación, así como en lo referente a la protección de datos personales.

Para asegurar el cumplimiento de la presente Política, las disposiciones y los procedimientos, han sido agrupados en tres categorías: Seguridad, Usuarios y Gestión de Tecnologías de Información (TI).

II. Aplicabilidad y alcance

Esta Política es aplicable a todos funcionarios del IICA y a las personas con acceso a la plataforma tecnológica del IICA, sean consultores, pasantes, personal asociado y de proyectos de financiamiento externo, en los Estados Miembros y la Sede Central, con las cuales el Instituto se relaciona para el cumplimiento de su misión.

III. Objetivo

Establecer las directrices y los mecanismos para una adecuada gestión de la plataforma de tecnologías de información y comunicaciones del IICA.

IV. Definiciones

1. *Adware*:

Es un *malware* que usualmente está enquistado en el navegador, pero podría también estar en el otra parte del sistema, para presentar anuncios no deseados en el dispositivo.

2. Data center (centro de procesamiento de datos):

Es una instalación, construcción o inmueble de gran tamaño donde se albergan y mantienen numerosos equipos electrónicos como servidores, ventiladores, conexiones y otros recursos necesarios que se utilizan para mantener una red o un sistema de computadoras, información, conexiones y datos.

3. *Firewalls*:

Es un dispositivo de seguridad, el cual regularmente es utilizado para segmentar el mundo público del mundo privado. Mediante un conjunto de reglas definidas, se establece el tráfico permitido y cuál es denegado, y el sentido del mismo.

4. *Hardware*:

Cualquier componente físico que forme parte de la Infraestructura de tecnologías de información y comunicación, tales como Equipos de Cómputo, Servidores, Switches, Routers, Access Point, Firewalls, Dispositivos de Almacenamiento como SAN y NAS, Equipos de Videoconferencia, Plantas Telefónicas, y demás relacionados.

5. *Host*:

Cualquier dispositivo conectado en una red, con capacidad de solicitar y brindar información (datos) con equipos locales (misma red) o remotos.

6. **Interconexión de Sistemas Abiertos** *(OSI por sus siglas en inglés):*

La Organización Internacional para la Estandarización (ISO) ha diseñado el modelo de referencia de Interconexión de Sistemas Abiertos (OSI) que utiliza capas estructuradas. El modelo OSI describe una estructura con siete capas para las actividades de red.

7. *Malware* (Código Malicioso):

Cualquier programa que se instala en un sistema operativo, cuyo fin es interferir con el correcto funcionamiento de este.

8. Phishing:

Es una técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial.

9. *Roaming*:

Capacidad de enviar y recibir llamada en redes móviles fuera del área de servicio local.

10. *Script*:

Es un guión que dirige una escena o secuencia. En programación el ***script*** contiene instrucciones escritas en código que sirven para ejecutar diversas funciones dentro de un programa.

11. Sistema de información:

Aplicación o herramienta informática que le permite al usuario ingresar, almacenar, procesar y obtener información, de manera automatizada.

12. Site:

En lo referente a internet se refiere a un sitio *Web.*

13. Software:

Conjunto de programas digitales, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

14. *Spam*:

Es cualquier forma de comunicación no solicitada que se envía de forma masiva (correo electrónico masivo no solicitado). Sin embargo, el "*spamming*" también existe a través de menajes instantáneos, de texto (SMS), redes sociales o incluso mensajes de voz. Enviar spam es ilegal.

15. Virus:

Es un *malware,* con la capacidad de replicarse, que es desencadenado por una acción del usuario.

V. Disposiciones institucionales de tecnologías de la información

El Instituto mediante la presente Política y el Manual de procedimientos de tecnologías de la información y comunicación establecen las disposiciones institucionales para asegurar que la plataforma de tecnología de la información y comunicación en el IICA se gestione de manera segura, oportuna y de acuerdo con los estándares internacionales.

1. Adquisición y uso de *Hardware* y *Software*

Esta política define las directrices para la definición y compra de *hardware* y *software* con el fin de gestionar un crecimiento organizado, lógico y estructurado de la arquitectura tecnológica del Instituto.

La política proporciona además los lineamientos a tener en cuenta al momento de adquirir algún *software* de propósito específico para el IICA, garantizando siempre que se cumpla con la normatividad vigente respecto de los temas de licenciamiento y de adquisición de bienes y servicios.

Cuando un *software* se vuelve crítico para los procesos de operación del IICA y contiene parametrizaciones y/o desarrollos a la medida, se convierte en un Sistema de Información.

La determinación de la estructura tecnológica que conlleva la adquisición de *hardware* y *software* de carácter institucional será responsabilidad de la Gerencia de Tecnologías de Innovación, Comunicación y Agricultura Digital (GTIC-AD), en el caso de necesidades particulares en las Representaciones la responsabilidad de este proceso es del Administrador conjuntamente con el Representante y en coordinación con la GTIC-AD. En ambos casos es requerida la autorización del Director de Servicios Corporativos.

Los procedimientos relacionados con la adquisición y uso de h*ardware* y s*oftware* se encuentran detallados en el Manual de procedimientos de tecnologías de información.

2. Seguridad de la información:

El IICA tendrá la obligación de mantener la seguridad de la información de la que es responsable, aplicando medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Se establece para estos fines una estructura de normalización, seguimiento, control y mejora del sistema de seguridad de la información institucional mediante una estructura de gobierno basada en las mejores prácticas, con el fin de asegurar la protección de los activos de información de usos no autorizados, modificación, daños o destrucción accidental o intencional. Adicional a los esquemas de seguridad digital, el IICA a través de un proceso de inducción y capacitación a los funcionarios, se generarán cápsulas informativas en las cuáles se hará énfasis en la importancia, el deber y la responsabilidad de los funcionarios del IICA de no divulgar, compartir datos personales de terceros, incluyendo sus comunicaciones

electrónicas debido a que esto se considera un derecho fundamental de la confidencialidad.

La adecuada definición de roles, permisos, niveles de acceso de los funcionarios del IICA a los diferentes sistemas de información, así como a la plataforma tecnológica del IICA o a los *data center* físicos del IICA, respectivos mecanismos de respaldo y de recuperación de la información, planes de contingencia, protección de datos, etc., buscan prevenir incidentes a la seguridad de la información del instituto.

2. 1. Normas para la seguridad de la información:

2.1.1. El IICA cuenta con un equipo centralizado en alta disponibilidad para la autenticación, y autorización, de equipos *(hosts)* así como de usuarios, para el acceso a los recursos informáticos de la Sede Central; para lo cual se utilizan plataformas, de acceso remoto, inalámbrica y cableada.

2.1.2. El acceso físico al *Data center* de la Sede Central, se realiza mediante un sistema de acceso solo para el personal autorizado.

2.1.3. Cuenta con equipo de seguridad perimetral de última generación, para la seguridad de los recursos locales, ante amenazas informáticas externas; así como una exhaustiva base de datos de firmas de aplicaciones que usan puertos de uso común para enviar información sensible.

2.1.4. Se cuenta con una plataforma de antivirus, que incluye un módulo de detección de amenazas.

2.1.5. El acceso a los diferentes sistemas de información del IICA, cuentan con un tratamiento de seguridad en diferentes capas del modelo de Interconexión de Sistemas Abiertos (OSI por sus siglas en inglés); que, aunado a prácticas de programación seguras, por parte de los desarrolladores; brindan una mayor protección de la información en ellos contenida.

3. Uso del correo electrónico institucional

El servicio de correo electrónico *(e-mail)* institucional (iica.int), es una herramienta institucional a disposición de los funcionarios, pasantes, consultores y personal asociado para realizar su trabajo.

Todos los recursos informáticos institucionales, incluyendo el uso de las cuentas de correo electrónico, están sujetos a mecanismos preventivos de mantenimiento y supervisión que garanticen la seguridad e integridad de la plataforma tecnológica del Instituto.

3.1 Normas para el uso del correo electrónico institucional

3.1.1. El servicio de correo electrónico institucional debe ser utilizado estrictamente para la comunicación y el trámite de asuntos institucionales. Los mensajes y documentos enviados por medio de este servicio tienen para todos sus efectos el carácter de oficial y, por lo tanto, pueden ser utilizados para transmitir aprobaciones y autorizaciones o como medios probatorios. Cada funcionario, pasante, consultor y personal asociado dispone de una clave personal para operar la cuenta de correo que le ha sido concedida, por lo que tiene plena responsabilidad de todo correo enviado desde su cuenta.

3.1.2. El sistema de correo electrónico institucional aplica filtros y mecanismos de seguridad que evitan la entrada de mensajes, archivos o enlaces que pueden afectar la integridad y seguridad de la plataforma tecnológica del Instituto. Para evitar que esas medidas de protección eliminen o bloqueen mensajes personales de los funcionarios, las comunicaciones personales deben gestionarse a través de otras cuentas de correo electrónico.

3.1.3. Entre las acciones para las que no está permitido el uso del correo electrónico institucional están las siguientes:

a. Envío de información confidencial o de propiedad exclusiva del Instituto a terceras personas no relacionadas con la Institución.

b. Envío de correos que promuevan actos ilícitos, deshonestos, contrarios a la moral y a las buenas costumbres, que difamen o perjudiquen la reputación de otras personas, que contengan asuntos de carácter obsceno o pornográfico o que promuevan la discriminación en cualquier sentido (por razones de raza, credo, nacionalidad o género). Tampoco se podrá utilizar el correo electrónico institucional para asuntos de política partidaria o para hacer campañas electorales de cualquier índole.

c. Envío de correos tipo *"spam"* que contenga virus, cadenas de correo, *phishing* o alguna otra característica que afecte la seguridad de la plataforma tecnológica del Instituto o que sature el tráfico de mensajes a través de ella.

d. Envío a terceros de lista de direcciones de correo de los funcionarios del Instituto.

e. Envío a los grupos de direcciones (p. ej. gmundo.iica) de correos que no son de atención o información colectiva o masiva.

f. Obtención, envío o tratamiento de datos personales de terceros, que no cumplan con las disposiciones establecidas en la Política y Manual sobre dicha materia.

g. Cuándo se requiere enviar archivos mayores a 25 MG a través del correo electrónico se sugiere utilizar otro tipo de mecanismos.

3.1.4. Los programas de mensajería instántanea (ofrecidos por la plataforma Teams, Google, Skype y similares autorizadas en el Instituto) pueden ser utilizados por los funcionarios como medios de comunicación para asuntos de trabajo, por lo que se autoriza su instalación y actualización y uso en los equipos que el Instituto pone adisposición de los funcionarios, pasantes, consultores y personal asociado; siempre que contribuyan al desempeño eficiente de las funciones institucionales.

4. Uso de Internet institucional

El servicio de acceso o conexión a Internet es una serie de recursos de *hardware* y *software* que son escasos y de alto costo, razón por la cual la GTIC-AD es la encargada de velar por su buena utilización.

El desarrollo tecnológico cada vez más acelerado, ha incrementado la demanda sobre el uso de este recurso para atender temas de interés personal, educativo, investigativo y profesional. Debido a esto, administrar y priorizar el uso de este recurso debe ser una tarea constante y responsable, ya que el canal de Internet por donde circula la información entre las distintas Representaciones, Unidades, Instituciones y personas vinculadas al quehacer del IICA, no siempre es el deseado y por él compiten una serie de paquetes de información de los cuales algunos son útiles para el Instituto y otros no.

4. 1. **Normas para el uso del internet Institucional:**

4.1.1. Queda prohibido el uso de cuentas y claves de acceso en los navegadores de las computadoras del IICA por personas distintas al usuario asignado, con o sin autorización del responsable.

4.1.2. El servicio de navegación en Internet es para uso exclusivo de actividades institucionales.

4.1.3. Queda prohibida la conexión, desconexión o reubicación de equipos dentro de la infraestructura tecnológica del IICA sin la autorización de la GTIC-AD.

4.1.4. Queda prohibido el uso de sitios de intercambio de archivos punto a punto (como por ejemplo *Ares, eMule, Torrents, Limewire*).

4.1.5. Las páginas a las que se ingrese por medio del servicio de Internet son sujetas a ser revisadas por la GTIC-AD, el cual ha sido asignado como responsable de área para monitorear y prevenir el uso de este, así como por los superiores directos de cada uno de los usuarios.

4.1.6. Uso, distribución o propagación de cualquier programa, *script* o comando diseñado para interferir con el uso, funcionalidad o conectividad de cualquier usuario, *host*, sistema o *site* dentro de Internet (como el propagar, vía email o mensajes conteniendo virus, caracteres de control, etc.)

4.1.7. Configurar o definir una página del Web para actuar de manera maliciosa contra los usuarios que la visiten.

4.1.8. Toda actividad realizada con el servicio de navegación en Internet es de única responsabilidad del usuario.

4.1.9. Es responsabilidad del usuario proteger la identidad de su cuenta y su clave de acceso.

4.1.10. Al realizar declaraciones o expresar opiniones personales mediante el servicio de Internet, se deberá indicar claramente que éstas son de carácter personal y de ninguna manera reflejan o representan las del IICA.

4.1.11. Se prohíbe el acceso a los sitios o páginas Web que contengan materiales pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano; para el caso de sitios redes sociales, blogs, web de comentarios y páginas de intercambio de documentación que sean catalogados como amenazadores, la GTIC-AD los bloqueará por defecto a través de los mecanismos de seguridad, si por alguna razón se desea visitar estos sitios web deberán solicitar la autorización para su acceso la GTIC-AD con previa autorización de su jefe inmediato, debiendo el usuario justificar debidamente que es necesario para el desarrollo de sus funciones institucionales.

4.1.12. Hacer uso del servicio de manera tal que constituya una molestia, abuso, amenaza o que de cualquier forma atente contra la integridad de los usuarios del servicio de Internet.

4.1.13. Tratar de evitar o alterar los procesos o procedimientos de medida del tiempo, utilización del ancho de banda o cualquier otro método utilizado por la GTIC-AD para registrar el uso de los productos y servicios.

4.1.14. Violar la seguridad de los sistemas, *sites o host* sin previa autorización de su dueño.

4.1.15. Está prohibido a los usuarios interferir o tratar de interferir con los servicios de cualquier otro usuario, *host* o red dentro de Internet (Ataques de negación de servicio). Ejemplos de estas actividades prohibidas incluyen sin limitaciones: (a) envío de cantidades excesivas de datos (como el saturar con cualquier tipo de tráfico que exceda las normas aceptables en cuanto a tamaño y/o frecuencia) con la intención de sobrecargar los sistemas, llenar los circuitos y/o hacer fallar a los *hosts*; (b) tratar de atacar o deshabilitar a un usuario, *host o site*; (c) uso, distribución o propagación de cualquier programa, *script* o comando diseñado para interferir con el uso, funcionalidad o conectividad de cualquier usuario, *host*, sistema o *site* dentro de Internet (como el propagar, vía email o mensajes conteniendo virus, caracteres de control, etc.).

4.1.16. Cambiar la información de identidad con el objetivo de hacerse pasar por otra persona o entidad.

5. Uso del servicio de comunicación móvil

La telefonía móvil se ha constituido en un instrumento valioso para potenciar el desarrollo de las organizaciones, fortaleciendo los procesos de comunicación haciéndolos más eficaces a nivel global.

Por tratarse de una tecnología que está inmersa en un proceso de transformación permanente y de muy corto plazo, se convierte en un recurso de alto costo institucional, tanto en la adquisición, como en su actualización.

Esta política tiene como objetivo establecer los lineamientos para regular la asignación y uso de teléfonos celulares, los servicios de comunicación (voz y datos) que pueden ser autorizados a los funcionarios y la responsabilidad de éste para hacer un uso racional de la telefonía móvil y los dispositivos asignados.

5. 1. Normas para el uso del servicio de comunicación móvil:

5.1.1. La adquisición de teléfonos celulares deberá realizarse de acuerdo con los lineamientos técnicos de la GTIC-AD y lo estipulado en el Manual de adquisición de bienes y contratación de servicios, dando prioridad a la obtención de dispositivos celulares mediante planes de telefonía celular, que garanticen al Instituto el servicio requerido al menor costo.

5.1.2. El dispositivo por adquirir debe cumplir con los requisitos tecnológicos del cargo para el cual va a ser asignado.

5.1.3. La contratación de los servicios adicionales como *Roaming*, servicios de internet y telefonía internacional, queda delimitado a la necesidad y pertinencia del cargo.

5.1.4. Criterios para la asignación de servicios y teléfonos celulares:

a. Naturaleza de las funciones asignadas al cargo dentro de la estructura organizacional que justifiquen una comunicación constante con las instancias institucionales pertinentes, o bien atención de situaciones de emergencia del Instituto.

b. Los cargos dentro de la estructura a los cuales se le asignará servicio y teléfono celular institucional, tanto dispositivo como consumo mensual serán aquellos que defina el Director General.

5.1.5. Criterios para el pago de servicios celulares mensuales:

El Instituto cubrirá únicamente el pago por:

a. Llamadas telefónicas por factura nacional.

b. Llamadas telefónicas por facturación de tráfico internacional, utilizado para funciones oficiales.

c. Servicios de *Roaming,* utilizado durante viajes oficiales.

d. Servicio de Internet, cuando haya sido autorizado.

5.1.6. Debe incentivarse el uso del servicio de conexión inalámbrica wi-fi (seguras), así como el uso de herramientas de colaboración y comunicación que reduzca el uso de itinerancia *Roaming*, tales como *Microsoft Teams, Open Scape* (App para utilizar telefonía convencional en dispositivos móviles), así como cualquier otra opción tecnológica.

5.1.7. Responsabilidades en caso de pérdida, por extravío o robo:

a. Gestionar ante la Administración en el caso de las Representaciones, o ante la Gerencia de Servicios Administrativos en el caso de la Sede Central, la cancelación del servicio celular en forma inmediata.

b. El funcionario deberá remitir una explicación escrita de su jefe inmediato, con copia a la Gerencia de Servicios Administrativos en la Sede Central y a la Administración en las Representaciones, indicando las circunstancias en las cuales se produjo la pérdida o robo.

5.1.8. La Gerencia de Servicios Administrativos en la Sede Central y los Administradores en las Representaciones, suministrarán al funcionario a quien se haya asignado un servicio y teléfono celular institucional, un detalle de los servicios y costos facturados mensualmente por el proveedor para su revisión y verificación.

6. Protección de Datos Personales

Tiene por objeto garantizar el derecho que tienen todas las personas a conocer, actualizar y rectificar los datos personales que se hayan recogido sobre ellas en las bases de datos o archivos que el instituto haya recopilado. Para efectos de la presente política, el IICA es el responsable del tratamiento de estos datos.

La Política será aplicable a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento que se encuentre en poder de la organización y dicho tratamiento será normado por lo definido en el Manual de procedimientos de tecnologías de la información; la Política sobre la Protección de Datos Personales y su respectivo Manual de procedimientos sobre la protección de datos personales.

VI. Generalidades

Las excepciones al cumplimiento de esta Política de Tecnologías de la Información y el Manual de procedimientos de tecnologías de información deben ser aprobadas por el Director de Servicios Corporativos. Asimismo, todas las excepciones a estos instrumentos normativos deben ser formalmente documentadas y registradas por los Administradores en las Representaciones y la GTIC-AD en la Sede Central, según corresponda.

VII. Responsabilidades

La implementación y el cumplimiento de la presente Política y el Manual son responsabilidad de todos los miembros del Instituto y personas vinculadas al Instituto que sean autorizadas a acceder a la plataforma tecnológica de información y comunicación del IICA.

Los Representantes y Administradores en las Representaciones y el Director de Servicios Corporativos en la Sede Central, velarán por el cumplimiento de esta Política.

Las directrices contenidas en la presente Política deben de ser implementadas y cumplidas por la Administración de cada una de las Representaciones del IICA, aun cuando, por su tamaño de operaciones no cuente con un funcionario especializado en tecnología de la información y comunicación. En la Sede Central, esta responsabilidad recae en la GTIC-AD.

Solo aquellos procesos, procedimientos, sistemas que sean de carácter corporativo, serán gobernados directamente por la GTIC-AD, en tal caso, de dicha Gerencia, emanarán las orientaciones y la atención de los requerimientos.

La Auditoría Interna realizará revisiones de la aplicación y cumplimiento de la presente Política y sus Procedimientos, y brindará sus recomendaciones al Director General y al Director de Servicios Corporativos.

VII. Denuncias

El IICA dispone de dos medios para recibir y atender las denuncias, a fin de que las personas remitan y canalicen de forma confidencial sus denuncias o quejas, referentes a los temas que dicta la presente Política:

1. El sitio de internet oficial: www.iica.int, sección REPORTES/DENUNCIAS; y,

2. El correo electrónico ec.ce@iica.int.

Toda denuncia, queja, investigación, informes e información referente al tema denunciado, será examinada y analizada de forma objetiva por el Comité de Ética del Instituto, quién establecerá su abordaje, medidas disciplinarias y acciones correspondientes.

VIII. Publicación

Esta Política estará disponible en el repositorio institucional, en el sitio web del Instituto, así como en la intranet institucional.

IX. Interpretación

Los aspectos no contenidos en la presente Política o que puedan prestarse a diversas interpretaciones serán aclarados por la GTIC-AD, y autorizados por el Director de Servicios Corporativos.

X. Revisión y ajuste

El Director de Servicios Corporativos, o quien él designe, será el responsable de mantener actualizado el contenido de esta Política, de acuerdo con los estándares internacionales en la materia dentro del quehacer institucional.

XI. Vigencia:

Esta Política entrará en vigor a partir de la fecha de su comunicación por parte del Director General.