Instituto Interamericano de
Cooperación para la Agricultura

Manual de procedimientos sobre las tecnologías de información y comunicación del IICA

Setiembre 2021

Índice

I. Presentación

El presente Manual de procedimientos sobre las tecnologías de información y comunicación instruye a todos los funcionarios del Instituto Interamericano de Cooperación para la Agricultura (IICA o El Instituto), que son responsables y/o usuarios de la plataforma de tecnologías de información y comunicación para garantizar una gestión oportuna, segura, confidencial, pertinente y respetuosa de las normas y estándares internacionales.

Para asegurar el cumplimiento del presente Manual, las disposiciones y los procedimientos, han sido agrupados en tres categorías: Seguridad, Usuarios y gestión de tecnologías de información y comunicación.

En todo momento se debe garantizar el cumplimiento de los lineamientos establecidos en la Política de tecnologías de información y comunicación.

II. Marco normativo

El Instituto está comprometido con ofrecer una plataforma tecnológica que se ajuste a los estándares internacionales para brindar cooperación técnica de excelencia, para lo cual vela por la gestión segura y oportuna de la misma, a través de la Política de tecnologías de información, y por ende este Manual que se enmarca prioritariamente en dicha Política, así como en otras políticas y procedimientos institucionales relacionados, entiéndase manuales o guías.

El presente Manual complementa, desde el punto de vista procedimental, la Política de tecnologías de la información y comunicación.

III. 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 y personal asociado y de proyectos de financiamiento externo en todos los Estados Miembros y la Sede Central, con las cuales el Instituto se relaciona para el cumplimiento de su misión.

IV. Objetivo

Brindar las orientaciones procedimentales a las Representaciones del IICA en los Estados Miembros y las Unidades de la Sede Central, para una adecuada gestión de la plataforma de tecnologías de información y comunicaciones.

V. Objetivos específicos:

1. Brindar al IICA un marco regulatorio acorde a los desafíos y retos de la cooperación técnica en materia de tecnologías de información y comunicación alineado con los estándares internacionales.

2. Cumplir con las disposiciones institucionales contenidas en la Política de tecnologías de la información y comunicación.

3. Ejecutar las orientaciones contenidas en el presente Manual, de forma comprobable, documentada y verificable.

VI. Generalidades:

1. Las excepciones al cumplimiento de este Manual deben ser aprobadas por el Director de Servicios Corporativos. Asimismo, todas las excepciones al mismo deben ser formalmente documentadas y registradas por los Administradores en las Representaciones y la Gerencia de Tecnologías de Información, Comunicación y Agricultura Digital (GTIC-AD) en la Sede Central, según corresponda.

2. Nada de lo dispuesto en este Manual o de lo relativo a éste, se considera una renuncia expresa o tácita a las inmunidades, los privilegios, las exoneraciones y los beneficios que disfruta el Instituto y/o su personal, de acuerdo con el derecho internacional, los tratados y las convenciones internacionales o la legislación nacional de sus Estados Miembros.

VII. Disposiciones y procedimientos institucionales de tecnologías de la información

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

A continuación, se detallan los Procedimientos que conforman este Manual:

N°	Procedimientos	Alcance	Anexo
I.	**Procedimientos de seguridad**		
1	Procedimiento de clasificación de la información	GTIC-AD[1] Representaciones Unidades de la Sede Central	Anexo 1
2	Procedimiento de seguridad de la información		Anexo 2
3	Procedimiento de gestión de incidentes de seguridad de la información		Anexo 3
3.1.	Guía de clasificación de incidentes de seguridad de la información		Anexo 4
4	Procedimiento de conservación y destrucción de información		Anexo 5
5	Procedimiento de generación de respaldos de datos		Anexo 6
6	Procedimiento de prevención, detección y corrección de virus		Anexo 7
7	Procedimiento conexión de acceso remoto		Anexo 8
8	Procedimiento de control de acceso físico al *Data center*	GTIC-AD	Anexo 9
II.	**Procedimientos de usuarios**		
9	Procedimiento de uso de dispositivos móviles	GTIC-AD Representaciones Unidades de la Sede Central	Anexo 10
10	Procedimiento de creación y eliminación de cuentas en servicios informáticos		Anexo 11

[1] La GTIC-AD forma parte de la Sede Central del IICA, sin embargo, para una mayor comprensión a efectos de este Manual se indica como la Unidad encargada de los temas a nivel corporativo en tecnologías de la información y comunicación del Instituto.

N°	Procedimientos	Alcance	Anexo
11	Procedimiento cambio de funciones de usuarios de servicios informáticos	GTIC-AD[2] Representaciones Unidades de la Sede Central	Anexo 12
12	Procedimiento de autorización de BYOD		Anexo 13
13	Procedimiento de administración de claves de usuario		Anexo 14
14	Procedimiento creación cuenta de correo electrónico		Anexo 15
15	Procedimiento eliminación de cuenta de usuario del correo electrónico		Anexo 16
16	Procedimiento creación de cuentas de Red		Anexo 17
17	Procedimiento creación cuenta de intranet		Anexo 18
18	Procedimiento de creación cuenta de sistema de información		Anexo 19
19	Procedimiento de borrado de información en equipos del IICA		Anexo 20
III.	**Procedimiento de gestión de tecnologías de información y comunicación**		
21	Procedimiento para la gestión de activos de tecnología de información y comunicación	GTIC-AD Representaciones	Anexo 21
23	Procedimiento de adquisición de equipos de tecnologías de información y comunicación		Anexo 22
24	Procedimiento solicitud de sistemas nuevos o cambios en sistemas de información		Anexo 23
27	Procedimiento solicitud de mantenimiento de un sistema de información.		Anexo 24

[2] La GTIC-AD forma parte de la Sede Central del IICA, sin embargo, para una mayor comprensión a efectos de este Manual se indica como la Unidad encargada de los temas a nivel corporativo en tecnologías de la información y comunicación del Instituto.

VIII. Responsabilidades

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

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

Los procedimientos contenidos en este Manual deben de ser implementados y cumplidos por cada una de las Representaciones del IICA en los Estados Miembros, 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 del presente Manual y sus Procedimientos, y brindará sus recomendaciones al Director General y al Director de Servicios Corporativos.

IX. 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.

X. Publicación

Este Manual estará disponible en el repositorio institucional, así como en la intranet institucional.

XI. Interpretación

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

XII. Revisión y ajuste

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

Los cambios a los procedimientos contenidos en este Manual serán comunicados y difundidos a toda la institución, para su conocimiento y acatamiento, a través de la GTIC-AD.

XIII. Vigencia:

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

GLOSARIO

1. **Activo de información:** El IICA considera como activo de información, según lo indicado en la norma ISO 27001, todo aquello que tenga valor informativo para la organización, incluyendo soporte digital y físico, tales como:

   a. Los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios.

   b. El *hardware* y el *software* utilizado para el procesamiento, transporte o almacenamiento de información.

   c. Los servicios utilizados para la transmisión, recepción y control de la información.

   d. Las herramientas o utilidades para el desarrollo y soporte de los sistemas de información.

   e. Personas que manejen datos, o un conocimiento específico muy importante para la organización (manejo de información crítica y conocimiento).

2. ***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.

3. **Amenaza persistente avanzada** *(APT por sus siglas en inglés):* Es un ataque dirigido a largo plazo, para lograr obtener información confidencial crítica.

4. ***Authentication cisco server (ACS):*** Es un sistema de control de acceso que opera como servidor *RADIUS* (es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP) y *TACACS+* (permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red), administrando la autenticación del usuario, el control de acceso a dispositivos y políticas de control centralizadas en la red.

5. **Base de Datos:** Conjunto de información, organizada y almacenada en un medio sea físico, o digital.

6. ***Bring Your Own Device (BYOD):*** Es una nueva tendencia tecnológica que permite a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

7. ***Broadcast:*** Es la difusión masiva de información o paquetes de datos a través de redes informáticas. El término se utiliza en la informática y en las telecomunicaciones.

8. ***Buffers:*** es un espacio de memoria en el que se almacenan datos evitando que el programa que los necesita se quede sin datos durante una transferencia.

9. ***Buffer overflow:*** Es un desbordamiento de la capacidad de almacenamiento de los datos en la memoria de la computadora, más allá de los límites de un buffer de longitud-fija.

10. **Código Malicioso (*Malware*):** Cualquier programa que se instala en un sistema operativo, cuyo fin es interferir con el correcto funcionamiento del mismo.

11. **Confidencialidad:** La cualidad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

12. **Controlador de dominio:** Servidor que brinda el servicio de autenticación de usuarios y máquinas en un entorno de red, puede ser centralizado o distribuido.

13. ***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.

14. ***Demilitarized Zone*** **(DMZ):** Zona en la que se brinda servicios al mundo de internet, y que se encuentra física o lógicamente separada de la red interna de una organización.

15. **Denegación de Servicios** *(DOS por sus siglas en inglés):* Es cuando los recursos de un servicio son consumidos por un único usuario, en detrimento del resto de usuarios legítimos.

16. **Dirección de Protocolo de Internet (*IP Address)*:** Es una representación numérica, para identificar un equipo conectado en una red IP, o para identificar un conjunto de equipos (red).

17. **Disponibilidad:** La cualidad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

18. **Equipo de Red:** Cualquier dispositivo activo, que facilita la comunicación entre dos equipos finales, sea que estén en el mismo segmento de red; o que se encuentren en segmentos de redes diferentes.

19. **Evento de seguridad de la información:** La ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.

20. ***File Server:*** Herramienta de tecnologías de información y comunicación que ofrece el servicio de almacenamiento de contenidos digitales de forma oportuna, segura, confidencial, integra.

21. ***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.

22. **Gestión de TI:** Es el proceso de manejo y supervisión de todos los asuntos relacionados con las operaciones y recursos de tecnología de la información dentro de una organización. Más específicamente, aquellos relacionados al tratamiento, almacenamiento y protección de la información. Este es un proceso que involucra la recolección, almacenamiento, selección, comparación y distribución de datos.

23. **Gusano:** Es un *malware*, con capacidad de propagar copias de sí mismo a equipos no infectados, de manera autónoma.

24. ***Hacking:*** Actividades que buscan ganar acceso indebido a un equipo informático (PC, Tablet, Smartphone, equipos de red, otros) que pueden provocar compromiso en su funcionamiento, o robar información.

25. ***Hardware***: Cualquier elemento activo que forme parte de la Infraestructura de Comunicación y Sistemas de Información existentes, 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.

26. **Herramientas de administración remota** *(RAT por sus siglas en inglés):* Es un *software*, que permite tomar control visual, y ejecutar acciones en un equipo remoto; desde un equipo local.

27. ***Host*****:** Es el hospedaje o anfitrión, es cualquier computadora o máquina conectada a una red mediante un número de IP (dirección del Protocolo de Internet) definido y un dominio, que ofrece recursos, información y servicios a sus usuarios.

28. **Integridad:** La cualidad de salvaguardar la exactitud y estado completo de los activos

29. **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.

30. ***Internet Control Message Protocol*** (**ICMP**): Es una red de protocolo que es responsable de reportar errores a través de la generación y envío de mensajes a la dirección IP de origen cuando hay problemas de red que son encontrados por el sistema.

31. ***Malware*** (Código Malicioso): Cualquier programa que se instala en un sistema operativo, cuyo fin es interferir con el correcto funcionamiento de este.

32. ***Malware*** **polimórfico:** Es lo mismo que el *malware*, con la característica que cambia una parte de su código, pero otra permanece igual en cada cambio, para no ser detectado.

33. ***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.

34. **Plataforma tecnológica:** es un conjunto de normas, herramientas de *hardware* y *software* que deben permitir:

a. Garantizar la conectividad e interoperabilidad entre las instituciones.

b. Permitir el funcionamiento y desarrollo de sistemas institucionales.

c. Capacidad de trabajo interactivo entre usuarios mediante la implementación de sistemas colaborativos por medios electrónicos.

35. **Polimórfico:** propiedad por la que es posible enviar mensajes sintácticamente iguales a objetos de tipos distintos. El único requisito que deben cumplir los objetos que se utilizan de manera polimórfica es saber responder al mensaje que se les envía.

36. ***Ransomware:*** Es un *malware,* que busca impedir el acceso de los recursos del dispositivo, por parte del usuario, para extorsionarlo y presionarlo a pagar un rescate.

37. ***Roaming*****:** Capacidad de enviar y recibir llamada en redes móviles fuera del área de servicio local.

38. ***Rogueware:*** Es un *malware,* que intenta hacerse pasar por otra aplicación verdadera mediante nombre o apariencia.

39. ***SAP (System Applications and Products in Data Processing):*** Es un sistema informático que utilizan las empresas para administrar correctamente las diferentes acciones de la empresa como la producción, la logística, el inventario, los envíos y la contabilidad.

40. ***Scareware:*** Es un *malware*, que se adquiere mediante publicidad engañosa, o amenazas inexistentes.

41. ***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.

42. **Seguridad:** Mecanismo que garantiza algún buen funcionamiento, previniendo que este falle, se frustre o se violente.

43. **Seguridad informática:** Todo mecanismo que garantiza el buen funcionamiento de los servicios informáticos de la empresa, previniendo que estos fallen, se frustren o se violenten.

44. **Servidores:** *Software* que se instala en un sistema operativo, para atender consultas de los clientes. Puede atender consultas locales, como consultas remotas, para lo cual es necesario que esté conectado en red.

45. **Sistema de gestión:** El conjunto de elementos (personas, sistemas manuales o automatizados, normativa, equipos y otros) que interactúan de manera sistémica para el logro de la adecuada gestión institucional en términos de eficiencia y eficacia.

46. **Sistema de gestión de la seguridad de la información:** La parte del sistema de gestión global, basada en un enfoque hacia los riesgos, para establecer, implementar, operar, dar seguimiento, revisar, mantener y mejorar la seguridad de la información, para ayudar a alcanzar los objetivos organizacionales.

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

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

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

50. ***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 mensajes instantáneos, de texto (SMS), redes sociales o incluso mensajes de voz. Enviar spam es ilegal.

51. ***Spyware:*** Es un *malware*, que se instala en el equipo permaneciendo oculto, que le permite seguir y obtener información en línea de la actividad del usuario; algunas más avanzadas, pueden activar micrófonos y cámaras sin que el usuario se entere.

52. **Troyano:** Es un *malware* que tiene la característica de asemejarse a un código legítimo, para pasar inadvertido, cuyo objetivo no es dañar el funcionamiento del equipo, sino tener acceso a él remotamente.

53. ***Virtual private network (VPN):*** Es una herramienta digital que redirige tu tráfico de internet a través de un túnel seguro, ocultando la dirección IP y encriptando los datos. Así es como una **VPN** mantiene los datos privados y protege frente a ciberataques potenciales.

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

I. ANEXOS: PROCEDIMIENTOS DE SEGURIDAD

Anexo 1 – Procedimiento de clasificación de la información

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de clasificación de la información
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	4
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Establecer, aplicar y clasificar las categorías de la información, tanto la impresa como la electrónica, de los sistemas informáticos que son administrados por la GTIC-AD y las plataformas de información y comunicación.

2. Alcance

Este procedimiento aplica a la información, impresa y electrónica, de los sistemas informáticos responsabilidad del Instituto, que es clasificada por los usuarios responsables de dicha información de acuerdo con sus funciones en el IICA.

El almacenamiento de la información derivada de tecnologías de información y comunicación compete a la GTIC-AD, en las Representaciones en los Estados Miembros esta responsabilidad compete a la administración.

3. Procedimiento general de clasificación de información

Toda la información gestionada por el IICA se clasifica en tres grupos, con base en su contenido. Estos grupos corresponden a:

3. 1. Información confidencial.
3. 2. Información para uso interno.
3. 3. Información para uso público.

A continuación, se detalla la normativa para clasificar la información en cada uno de estos grupos:

3. 1. Información confidencial

Este grupo de información posee un alto nivel de restricción para su acceso. Es de uso restringido para un grupo específico de personas, definido en forma explícita por la jefatura del área responsable de la recopilación o generación de esa información.

Dicha información no puede ser divulgada a personas que no sean las autorizadas, por tener como consecuencia graves daños para Instituto, o para las instituciones relacionadas con el IICA. Estos daños pueden significar el comprometer la imagen institucional, el relacionamiento con otras instituciones y oportunidades de negocios entre otros aspectos.

El carácter de información confidencial será dado por la instancia del IICA que administre esta información con base en criterios técnicos justificados.
Los datos personales se consideran información confidencial.

3. 2. Información para uso interno

Este grupo de información no es de alcance público y posee un nivel medio de restricción para su acceso, la misma es gestionada a través de la plataforma tecnológica de información y comunicación del IICA, misma que es de uso para el personal previamente autorizado.

Esta información no puede ser divulgada por tener como consecuencia daños menores para el IICA, o para las instituciones relacionadas.

El carácter de información para uso interno será dado por la instancia del IICA que administre esta información con base en criterios técnicos justificados.

3. 3. Información para uso público

Esta información puede ser usada por cualquier usuario dentro de la Institución. La divulgación de esta no provoca daños para el Instituto, o para las instituciones relacionadas, no compromete la imagen corporativa del IICA, la relación con otras instituciones, ni las oportunidades de negocios.

El carácter de información para uso público será dado por la instancia del IICA que administre esta información con base en criterios técnicos justificados.

4. Almacenamiento de la información

4. 1. Información confidencial

Los documentos en formato electrónico deben ser almacenados en la carpeta dentro del directorio correspondiente de la unidad responsable en el *File Server*.

Los documentos impresos que sean considerados confidenciales, deben ser almacenada en una caja fuerte, en un mueble de seguridad, o en un mueble metálico bajo llave.

4. 2. Información para uso interno

Los documentos en formato electrónico pueden ser almacenados en el *File Server* o en la Intranet.

Los documentos impresos que sean considerados confidenciales, deben ser almacenada en una caja fuerte, en un mueble de seguridad, o en un mueble metálico bajo llave.

4. 3. Información para uso público

Los documentos en formato electrónico o impreso clasificada como uso público, pueden ser almacenados sin restricciones y se puede publicar en el Sitio Web del IICA iica.int.

5. Tránsito o distribución de la información

La distribución de los documentos internos debe estar controlada a través de un mecanismo que asegure el tratamiento adecuado de la información entregada y es aplicado el criterio del responsable de este en la decisión final de entrega a terceros. No se restringe la entrega de ningún tipo de documento público.

6. 1. Información confidencial

Los documentos electrónicos clasificados como “confidenciales” deberán ser transferidos a un tercero, solo a previa solicitud del responsable de dicha información. En tal caso, la transferencia de la información se realizará por medios seguros, velando en todo momento por la confidencialidad de esta. En casos justificados, se podrá establecer un mecanismo de distribución con una clave de seguridad la cual será provista al receptor de la información confidencial.

6. 2. Información para uso interno

Los documentos electrónicos transitan y se distribuyen sin restricción, cuando se utilicen en formato digital generalmente se utilizará el correo electrónico

institucional, la intranet o un servidor de almacenamiento de datos, base de datos restringidas, etc.

6. Destrucción de la información

7. 1. Información confidencial

Los documentos electrónicos, deben ser destruidos borrando la información de cualquier lugar donde se encuentren almacenados, incluyendo la papelera de reciclaje o inutilizando el medio que lo contiene.

Los documentos impresos, deben ser destruidos en forma manual en una máquina destructora de papeles.

7. 2. Información para uso interno

Los documentos electrónicos, deben ser destruidos borrando la información de cualquier lugar donde se encuentren almacenados, incluyendo la papelera de reciclaje o inutilizando el medio que la contiene.

Los documentos impresos, deben ser destruidos en forma manual en una máquina destructora de papeles.

7. 3. Información para uso público:

Los documentos electrónicos, pueden ser destruidos sin restricciones, incluso puede ser reciclada.

……..…..……última página anexo 1……..…..……

Anexo 2 - Procedimiento de seguridad de la información

IICA	TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
		X	Privado (disponible en la intranet del IICA)
TÍTULO	Procedimiento de seguridad de la información		
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central		
FORMATO	Electrónico – Word		
PÁGINAS	6		
REF. APROBACIÓN	SC/DG-405		

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Establecer las prácticas para garantizar que toda la información contenida en los repositorios y sistemas informáticos que son administrados por el Instituto Interamericano de Cooperación para la Agricultura (IICA), se capta, mantiene, trata y desecha conforme a las mejores prácticas de seguridad de la información.

2. Alcance

Este procedimiento aplica a la información captada, mantenida y tratada por el Instituto Interamericano de Cooperación para la Agricultura (IICA), en los sistemas de información computadorizados.

3. Procedimiento general de seguridad de la información

El IICA tendrá la obligación de mantener la seguridad y confidencialidad de la información de la que es responsable, aplicando medidas técnicas, digitales, análogas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Las medidas se adoptarán teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, alcance, contexto y fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

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.

Se establece que este procedimiento es de acatamiento obligatorio para todos los funcionarios y colaboradores de la institución, a fin de garantizar el logro de los objetivos para la gestión de seguridad de la información, así como para asegurar que todas las actividades dentro de la organización se ejecutan de acuerdo con lo establecido en estos procedimientos. Su incumplimiento será sancionado de acuerdo con la normativa institucional.

Los incidentes de seguridad se gestionan de acuerdo con lo establecido en el Procedimiento de gestión de incidentes de seguridad, Anexo 3 siguiente.

4. Implementación y gestión

La GTIC-AD y las Representaciones deben gestionar de forma adecuada toda aquella información relacionada con la plataforma tecnológica, Las áreas participantes en procesos de captura y mantenimiento de datos, deben establecer, comunicar e implementar los requerimientos de seguridad de acceso y protección, así como los controles necesarios para asegurar su debida protección.

Se establece un procedimiento para el ingreso, salida o cambio de funciones, de funcionarios, colaboradores, practicantes, pasantes y otras personas que presten servicios de manera permanente o temporal, mediante el cual se informe de estos eventos, para el debido mantenimiento de los derechos de acceso e identificación. Para los sistemas críticos, una vez al año se harán revisiones de los permisos sobre los activos de información de los usuarios, debiéndose dejar evidencia de los hallazgos encontrados y las medidas correctivas aplicadas.

Se establecen los mecanismos necesarios para la baja de equipos tecnológicos de procesamiento de datos, de manera que se prevenga la fuga de información valiosa y la protección de la información de carácter personal.

Todos los funcionarios del Instituto o aquellos vinculados que tengan acceso autorizado a sistemas e información del Instituto, deben velar por no dejar información sensible a la vista de terceros de manera que se prevenga la fuga de información valiosa y la protección de la información de carácter personal, y deben bloquear el sistema cuando no está en uso.

4.1. Revisión de los servicios de tecnologías de información y comunicación

La GTIC, realizará una revisión de los servicios de tecnología de información que aplica para la Sede Central y las Representaciones en el caso de los sistemas o servicios tecnológicos corporativos.

En el caso de las Representaciones que cuenten con servicios específicos, la administración deberá velar su respectiva verificación y gestión tecnológica.

Tanto para el caso de los servicios tecnológicos corporativos, así como los específicos de las Representaciones, esta revisión deberá realizarse al menos una vez al año.

La GTIC y las Representaciones deberán considerar en sus revisiones, los siguientes aspectos:

4.1.1. La especificación del periodo de conservación de cada uno de los activos de información identificados.

4.1.2. Especificar claramente el responsable de cada activo de información.

4.1.3. Especificar los controles del proceso que garantizan el cumplimiento de los niveles de confidencialidad, integridad y disponibilidad de cada activo de información.

4.1.4. Para aquellos activos cuyo nivel de confidencialidad corresponda a los niveles de máxima seguridad, asegurar que se incluyen como parte del inventario de activos de Seguridad de la Información.

4.1.5. El tratamiento de la información del Instituto tendrá las siguientes características de: confidencialidad, integridad, disponibilidad y seguridad.

5. Obligaciones del personal

Todo el personal del IICA, está obligado al cumplimiento de las siguientes funciones y obligaciones, de forma que un incumplimiento de estas podría suponer una infracción de sus obligaciones laborales:

5. 1. Acceder únicamente a los datos que necesite para el ejercicio de sus funciones.

5. 2. Mantener confidencialidad respecto a todos los datos de carácter personal de terceros que, con motivo del desempeño de las tareas que les sean encomendados o puedan conocer, debiendo guardar estricta reserva al respecto, no divulgándolos más allá de lo estrictamente necesario para realizar su trabajo, incluyendo la confidencialidad de las comunicaciones electrónicas.

5. 3. No dejar su pantalla de acceso a los sistemas de información activa cuando, por cualquier causa, se ausente momentáneamente de su puesto de trabajo, debiendo bloquear el sistema.

5. 4. Borrar periódicamente los ficheros temporales u obsoletos con datos de carácter personal, de acuerdo con las disposiciones contenidas en la Política sobre la protección de datos.

5. 5. Conocer, respetar y cumplir estrictamente las normas, políticas y procedimientos de seguridad de información del IICA.

5. 6. No destruir, alterar o dañar de cualquier otra forma los datos, programas o documentos electrónicos del IICA, o de terceros.

5. 7. No borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.

6. Registro y gestión de eventos de seguridad

El IICA cuenta con mecanismos para detectar actividades sospechosas, no autorizadas y posibles violaciones en el uso de los sistemas de información provistos por la institución, realizadas por funcionarios a nivel general del IICA y personas externas al IICA.

La GTIC-AD implementa medidas para detectar y alertar de potenciales incidentes de seguridad que puedan afectar los activos de información del IICA, de acuerdo con el Procedimiento de gestión de incidentes de seguridad, contenido en el presente Manual, en el caso de los servicios de tecnologías corporativos; en el caso específico, las representaciones deberán de implementar las medidas correspondientes.

La GTIC-AD vela por el respeto de los siguientes lineamientos:

6. 1. Almacenamiento de forma precisa y consistente de las bitácoras que considere relevantes para colaborar en análisis posteriores que colaboren en el reforzamiento de los controles de seguridad.

6. 2. Las bitácoras de los servidores deben al menos tener la retención que se indica a continuación:

a. Controladores de Dominio, 1 mes.
b. Bases de Datos, 3 meses.
c. Servidores ubicados en la DMZ que publican contenido en Internet, 1 mes.

6. 3. Todo sistema crítico donde se activen las **bitácoras** deberá registrar en las mismas, como mínimo, la información que se indica a continuación:

6.3.1. **Servidores**

a. Usuario y/o máquina que generó el evento.
b. Fecha y hora en que se generó el evento.
c. Tipo de evento o servicio.
d. Intentos fallidos y exitosos de acceso al sistema.
e. Intentos fallidos y exitosos de acceso a los recursos del sistema.
f. Uso de privilegios elevados.
g. Uso de utilidades y aplicaciones.
h. Cambios en las configuraciones de sistema.
i. Intentos de acceso y modificación de bitácoras.

6.3.2. **Equipo de Red**

a. Origen del evento (dirección IP).
b. Descripción del evento.
c. Si la conexión fue permitida o denegada.
d. Fecha y hora del evento.

6.3.3. **Máquinas de escritorio**

a. Modificaciones a las configuraciones del usuario.
b. Uso de utilidades y aplicaciones.
c. Uso de privilegios elevados.
d. Intentos fallidos y exitosos de acceso al sistema.
b. Registro de intentos fallidos y exitosos de acceso a los recursos de información.

La GTIC-AD en la Sede Central y quien corresponda en las Representaciones deberá configurar todos los equipos para el procesamiento de servicios críticos del IICA para que sincronicen su reloj interno con la misma fuente común, para velar por la integridad de las transacciones.

La GTIC-AD en la Sede Central y quien corresponda en las Representaciones, implementará mecanismos para monitorear el estado de los sistemas críticos del IICA, con el fin de mantener la disponibilidad, integridad y confidencialidad de la información.

La GTIC-AD en la Sede Central y quien corresponda en las Representaciones, implementará mecanismos para almacenar y analizar de forma precisa y consistente las bitácoras de los sistemas que soportan las operaciones críticas del IICA, para colaborar en análisis posteriores que coadyuven en el reforzamiento de los controles de seguridad implementados.

7. Seguridad y Protección de datos personales

El Instituto mediante la Política sobre la Protección de Datos Personal y el Manual de Procedimientos sobre Protección de Datos, establece las disposiciones y procedimientos institucionales para el tratamiento adecuado y correcto de los datos personales de terceros a los cuales tenga acceso para la realización de sus actividades.

Prevalecerá el derecho de toda persona física o su dato de contacto como persona jurídica, a la protección de sus datos personales, a la confidencialidad, al tratamiento de estos de acuerdo con los principios enmarcados en la Política sobre la Protección de datos personal, al establecimiento de medidas de seguridad para la protección y salvaguarda de los datos, y a los lineamientos de acceso y/o comunicación.

Los datos personales de terceros son por definición, clasificados como confidenciales. Esta confidencialidad define cómo se manejará, administrará y difundirá la información privada de una persona física o jurídica. La confidencialidad de los datos personales debe, en todo momento, ser respetada por el Instituto y su personal al tratar dichos datos.

……..…..……última página anexo 2……..…..……

Anexo 3 - Procedimiento de gestión de incidentes de seguridad de la información

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de gestión de incidentes de seguridad de la información
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	2
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Brindar un marco de trabajo para la atención de los incidentes de seguridad que se presenten en la institución, de manera que todo se realice de una manera estandarizada y cumpliendo con las mejores prácticas. Así como garantizar que toda la información relevante a cada uno de los incidentes de seguridad se documente y se guarde para futuras referencias.

2. Alcance

Este procedimiento aplica a la información captada, mantenida y tratada por el Instituto Interamericano de Cooperación para la Agricultura (IICA), en los sistemas de información computarizados.

La GTIC-AD y las representaciones implementarán un proceso de atención de incidentes de seguridad tecnológica con tareas y roles específicos para asegurar que tanto las sospechas, como los eventos e incidentes de seguridad tecnológica sean reportados prontamente y escalados a las instancias adecuadas con el fin de atender dichos reportes de manera apropiada.

3. Procedimiento para la gestión de un incidente de seguridad

3. 1. El funcionario del IICA debe reportar las sospechas, eventos o incidentes de seguridad tecnológica a la Mesa de Ayuda (sistema *help desk*) de la Sede Central o a la Administración de las Representaciones.

3. 2. De acuerdo con los datos suministrados de clasifica el incidente de seguridad de acuerdo con lo definido en la Guía de clasificación de Incidentes de Seguridad que se encuentra en el Anexo 4 de este Manual.

3. 3. Se deberá investigar sobre las posibles causas por las que se dio el incidente, cómo puede afectar a los activos de la organización o de terceros, posibles medidas que se pueden tomar para contenerlo, para erradicarlo y para reducir la probabilidad de que éste vuelva a ocurrir. Se definen y ejecutan las acciones de respuesta inmediata para empezar con la contención del evento.

3. 4. En caso de identificarse que no corresponde a un incidente de seguridad, se contesta y se cierra la solicitud.

3. 5. Se debe generar el informe de incidente de seguridad, documentando toda la atención del caso y registrándolo en la bitácora de incidentes de seguridad. Cada Representación implementará su propia versión de la bitácora de los incidentes de seguridad.

……..…..……última página anexo 3……..…..……

Anexo 4 - Guía de clasificación de incidentes de seguridad de la información

IICA TIPO DE DOCUMENTO			Público (disponible en el Sitio Web del IICA)
		X	Privado (disponible en la intranet del IICA)
TÍTULO	Guía de clasificación de incidentes de seguridad de la información		
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central		
FORMATO	Electrónico – Word		
PÁGINAS	5		
REF. APROBACIÓN	SC/DG-405		
VERSIÓN	**FECHA**	**AUTOR**	
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura	

1. Objetivo

Definir la clasificación y la severidad de todo incidente de seguridad. Ante cualquier incidente de seguridad se debe realizar la clasificación correcta y la severidad de éste, reportado según el proceso de gestión de incidentes de seguridad.

2. Alcance

Esta guía aplica a la información captada, mantenida y tratada por el Instituto Interamericano de Cooperación para la Agricultura (IIICA), en los sistemas de información computadorizados.

3. Clasificación del evento detectado:

Se clasifica según los siguientes criterios al evento reportado (se utiliza como referencia el documento de ISO 27035: *"Information Technology- Security Techniques- Information security incident management*").

3. 1. Accesos no autorizados (*Hacking*)

3.1.1. Intentos de extraer archivos de contraseñas.

3.1.2. Ataques de "*buffer overflow"* para ganar privilegios mayores.

3.1.3. Explotación de vulnerabilidades del protocolo para ocultar acciones maliciosas detrás de conexiones de red legítimas.

3.1.4. Intentos de elevar privilegios a los recursos de información detrás de los privilegios que un usuario o administrador legítimamente posee.

3.1.5. Acceso no autorizado causado por medios no técnicos causados por brechas físicas, sistemas operativos mal-configurados o funciones inadecuadas del *software o hardware*.

3. 2. Código Malicioso (*Malware*)

3.2.1. Robo o pérdida de equipo de TI con información sensible:

Cuando un activo de la organización se ve afectado por un virus, gusano, troyano, *adware*, *scareware*, *spyware, ransomware,* herramientas de administración remota RAT, *rogueware, malware* polimórfico y amenaza persistente avanzada (APT).

Algunos de los síntomas de un equipo infectado pueden ser:

a. Equipo trabaja más lento de lo habitual.
b. El protector y fondo de pantalla cambiaron por ninguna razón aparente.
c. Se abren o cierran las ventanas de los navegadores sin interacción del usuario (Pop-ups).
d. Aparecen mensajes de error en la estación de trabajo.
e. Hay iconos nuevos en el escritorio que el usuario no puso.
f. Las aplicaciones instaladas en el equipo actúan de manera diferente a la esperada (se cierran sin motivo aparente, se abren solas, etc.).
g. El equipo se reinicia solo.
h. Hay alertas de indicadores de compromiso que demuestran que el equipo está enviando tráfico de administración remota no autorizada hacia internet o hacia equipos internos pertenecientes a la organización.
i. Existen mensajes mostrados al usuario indicando que para recuperar la información del usuario es necesario pagar un monto por rescate.
j. Existen alertas de indicadores de compromiso que demuestran que el equipo tiene instalado *software* malicioso no detectado por los controles antivirus tradicionales o existen indicios de transformación del *software* malicioso dentro del equipo producto de una revisión profunda del equipo.
k. Existen reportes de las herramientas de detección y respuesta que indican posible compromiso del equipo de usuario final.

3. 3. Denegación de Servicios (DOS), común o distribuido

Cuando un usuario autorizado no pueda acceder a algún servicio, equipo, información o activo de la organización. Entre los cuales se encuentran:

a. Abuso del ancho de banda con tráfico de respuesta debido a solicitudes *icmp* a direcciones *broadcast*.
b. Abuso del ancho de banda con el establecimiento de múltiples conexiones en TCP sin finalizar la negociación de tres vías común en este protocolo.
c. Envío de datos en un formato no esperado a un sistema, servicio o red, en intento de hacer fallar al sistema, o interrumpir su operación normal.
d. La apertura de sesiones múltiples no autorizadas a un sistema en particular, servicio o red para ocupar todos sus recursos.

3. 4. Ingeniería Social

Cuando un tercero ha intentado obtener información de algún empleado del IICA por el medio que sea (teléfono, en persona, por correo electrónico).

3. 5. Mal uso (es un usuario autorizado y con mala intención)

Cuando un activo de la organización se vea afectado debido a un abuso de privilegios, manipulación inapropiada, uso de aplicaciones no autorizadas, incumplimiento de las políticas institucionales. Algunos ejemplos son:

a. El bajar e instalar herramientas para *Hacking*.
b. La utilización de los recursos institucionales para levantar un sitio web no autorizado.
c. La utilización del correo electrónico para promocionar negocios personales y el envío de correo no deseado (*Spam*).
d. La utilización de redes “punto a punto” para adquirir o distribuir archivos relacionados con la piratería (música, video o programas).

3. 6. Error (usuario autorizado y sin intención)

Si un activo de la organización se ve afectado por una mala configuración, un mantenimiento realizado, omisión de ejecutar algún control que protege al activo.

3. 7. Ambiental

Cuando un activo del IICA se haya visto afectado por fugas de agua, desastres naturales (inundación, huracán, rayería, tornados, erupción volcánica, terremoto), altas temperaturas, estática, interferencia electromagnética, polvo y suciedad.

3. 8. Recolección de Información

Actividades relacionadas con la recolección de información de acceso restringido, confidencial o datos personales, para uso posterior en actividades maliciosas en contra de la Institución o las personas físicas o jurídicas. Entre las cuales está:

a. La existencia del objetivo, y el entendimiento de la topología de red que lo rodea, así como la comunicación del objetivo con otros equipos.

b. Vulnerabilidades existentes en el objetivo, o en el ambiente de red donde se encuentra las cuales podrían ser explotadas.

c. Registros de DNS o transferencias entre zonas DNS.

d. Tráfico de reconocimiento ICMP para determinar qué equipos están activos y respondiendo.

e. Identificación de características del sistema (sistema operativo, versiones).

f. Escaneo de puertos de red disponibles en el sistema para identificar servicios relacionados.

g. Escaneo de uno o más servicios vulnerables en un rango de direcciones IPs disponibles.

h. Eventos de fuga de información o modificación no autorizada de la información.

i. Robo de propiedad intelectual perteneciente a la institución.

j. Brechas en los sistemas de bitácoras, borrado de bitácoras y fuga de la información.

k. Robo de información criptográfica detectable.

3. 9. Alteración datos personales

Actividades relacionadas con la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma.

3. 10. Severidad del incidente

Si el evento reportado se puede catalogar como incidente de seguridad se procede a determinar de acuerdo con las siguientes descripciones la severidad del incidente reportado.

3. 11. Severidad baja:

a. Cuando de 1 a 3 individuos no puedan realizar sus labores con normalidad debido al evento reportado.
b. Cuando información clasificada como de "uso interno" fue accedida, alterada o divulgada sin autorización.
c. Cuando uno o varios servicios no críticos han sido degradados debido al evento reportado.
d. Cuando activos con disponibilidad baja no puedan ser accedidos por usuarios autorizados.

3. 12. Severidad media:

a. Cuando una o varias áreas no puedan realizar sus labores con normalidad debido al evento reportado.
b. Cuando información clasificada como de carácter personal fue accedida, alterada o divulgada sin autorización.
c. Cuando un servicio crítico ha sido degradado.
d. Cuando uno o varios servicios no críticos se han visto interrumpidos debido al evento reportado.
e. Cuando activos con disponibilidad media no puedan ser accedidos por usuarios autorizados.

3. 13. Severidad alta:

a. Cuando toda un área administrativa no pueda realizar sus labores con normalidad debido al evento reportado.
b. Cuando información clasificada como "confidencial" fue accedida, alterada o divulgada sin autorización.
c. Cuando uno o varios servicios críticos se han visto interrumpidos debido al evento reportado.
d. Cuando activos con disponibilidad alta y muy alta no puedan ser accedidos por usuarios autorizados.

……..…..……última página anexo 4……..…..……

Anexo 5 - Procedimiento de conservación y destrucción de información

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de conservación y destrucción de información
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	2
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Definir los lineamientos para la conservación y destrucción de información contenidos en los sistemas de información y apoyo administrados por el Instituto Interamericano de Cooperación para la Agricultura (IICA).

2. Alcance

Este procedimiento aplica a la información captada, mantenida y tratada por el Instituto Interamericano de Cooperación para la Agricultura (IICA), en los sistemas de información computadorizados.

3. Procedimiento para la conservación y destrucción información

3. 1. La información institucional, quedará disponible con los debidos mecanismos de seguridad y confidencialidad en la plataforma tecnológica del IICA para que la persona encargada del tema o del área analice la necesidad de conservar o destruir la información. Los plazos de conservación y destrucción de la información estarán definidos por la normativa institucional aplicable.

3. 2. El Instituto como responsable del tratamiento de datos personales y bajo el principio de que dichos datos deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados; establecerá un límite para su plazo de conservación, el cual se

establece en la Política sobre la Protección de Datos Personal y el Manual de Procedimientos sobre Protección de Datos Personales.

3. 3. Una vez cumplido el plazo de conservación, se procederá con la destrucción de la información de acuerdo con la normativa institucional. GTIC AD y los Administradores en las Representaciones llevarán un control de la destrucción de la información llevado a cabo. En el caso de los “encargados”, los mismos procederán con la destrucción una vez cumplido el plazo de conservación, enviando la documentación que demuestre dicha destrucción a la GTIC-AD o a los Administradores en las Representaciones, según corresponda.

……..…..……última página anexo 5……..…..……

Anexo 6. Procedimiento de generación de respaldo de datos

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de generación de respaldo de datos
APLICACIÓN	GTIC-AD y todas las Representaciones del IICA
FORMATO	Electrónico – Word
PÁGINAS	3
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Establecer los lineamientos para aplicar el respaldo, salvaguardar y proteger el capital intelectual del IICA con el propósito de asegurar la continuidad operativa del Instituto, con el menor impacto posible.

2. Alcance

El procedimiento considera el respaldo de los siguientes datos:

a. Sistemas de información y sus bases de datos que estén en uso y sean administrados por la sede central.
b. Web (*legacy*).
c. Intranet.
d. Servidor de archivos.
e. Y cualquier otro que sea relevante para la institución.

3. Procedimiento para la generación del respaldo de datos

3. 1. Los respaldos realizados en el IICA deben ser sistemáticos y permanentes. Estos respaldos, se efectuarán tres veces a la semana (martes, jueves y viernes).

3. 2. En la Sede Central, el área responsable de los respaldos corresponde a Redes y Telecomunicaciones, perteneciente a la GTIC-AD.

3. 3. Los funcionarios del área de sistemas en las Representaciones que tengan a su cargo algún servicio informático (intranet, internet, aplicaciones web) o un sistema de información deberán explicitar al encargado de generar los respaldos, cuáles son los archivos que deben ser respaldados, así como cualquier cambio que amerite ser considerado en el respaldo.

3. 4. Cada tres meses el responsable de realizar el respaldo deberá corroborar la lista de archivos respaldados en conjunto con cada funcionario del área de sistemas. Dicho proceso se hará mediante correos electrónicos que el funcionario responsable de los respaldos deberá guardar como apoyo documental del proceso.

3. 5. Los respaldos deben quedar debidamente rotulados. En el caso de cintas de respaldos que se envían a empresas externas de custodia, deben estar rotuladas con el mes y año que corresponde. Los respaldos regulares, se les rotula con la fecha y se enumeran consecutivamente dependiendo de la cantidad de cintas.

3. 6. Se deberán realizar pruebas de legibilidad una vez que finalice el proceso de respaldo, con el fin de verificar que las cintas se encuentran en buen estado, estas pruebas deberán registrarse en una bitácora creada para tales efectos.

3. 7. Para cada respaldo periódico se debe establecer:

a. Información a respaldar.
b. Periodicidad de las copias.
c. Medio por el cual respaldar.
d. Tipo de respaldo.

3. 8. El almacenamiento de las copias de seguridad debe realizarse en una ubicación diferente de donde reside la información primaria.

3. 9. La ubicación de los respaldos debe ser en un lugar con acceso restringido y preferiblemente, con dispositivos de seguridad y de prevención de incendios. (Bóvedas, bancos, centro de datos externos).

3. 10. Cuando se programen tareas extraordinarias donde se produzcan modificaciones o cambios de *software* y/o *hardware*, debe asegurarse que se hagan los respaldos correspondientes previos a ese trabajo.

3. 11. La información y las cintas de respaldo deben tener un nivel apropiado de protección ambiental y físico. Cada cinta debe tener como máximos 20 sobreescrituras.

3. 12. Se debe mantener un registro y la fecha de envío de la cinta a la empresa de custodia.

3. 13. En caso de una recuperación de respaldos, se deberá registrar en la *Bitácora de recuperación de respaldos*, la siguiente información: Fecha, Solicitante, #Solicitud, Archivo(s) recuperado(s), Cinta utilizada.

3. 14. Una vez que las cintas de respaldo alcancen las 20 sobreescrituras ó los cinco años de almacenamiento desde su primer uso, deben ser deshabilitadas para su uso, para esto deben quedar debidamente registradas en el libro de *Actas de Destrucción de Respaldo de Datos.* Sin embargo, por instrucciones superiores ninguna cinta será destruida, sino que serán almacenadas en la GTIC-AD.

……..…..……última página anexo 6……..…..……

Anexo 7. Procedimiento de prevención, detección y corrección de virus

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de prevención, detección y corrección de virus
APLICACIÓN	GTIC-AD y todas las Representaciones del IICA
FORMATO	Electrónico – Word
PÁGINAS	3
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Implementar las acciones para prevenir, detectar y corregir los virus informáticos en la plataforma tecnológica del Instituto.

2. Alcance

Este procedimiento aplica a todas las estaciones de trabajo (computadores y portátiles) conectadas o que deseen conectarse a la red del IICA.

3. Procedimiento para la prevención, detección y corrección de virus

3. 1. Toda computadora y portátil perteneciente al dominio de red del IICA, debe tener instalado el antivirus corporativo.

3. 2. No se permitirá la instalación de antivirus que no sea el corporativo.

3. 3. El área de Soporte Redes en la GTIC-AD es la responsable de la administración del *software* antivirus corporativo y velará porque el proceso de actualización de versiones se lleve a cabo sin inconvenientes.

3. 4. El área de Soporte TIC de la GTIC-AD en la Sede Central es responsable de configurar correctamente el antivirus en las estaciones de trabajo. En el caso de las Representaciones el Administrador es el encargado, en caso de tercerizar este servicio, el Administrador es el responsable de coordinar con GTIC-AD para velar por el cumplimiento de las disposiciones institucionales en esta materia.

3. 5. El manejo del antivirus corporativo se debe realizar a través de consolas centralizadas para la administración, monitoreo y detección de cualquier amenaza de virus.

3. 6. Se deben realizar las actualizaciones de *software* para la detección o reparación de virus. Las actualizaciones deben realizarse de lunes a viernes.

3. 7. Se debe ejecutar la revisión de los computadores del dominio de red del IICA como medio de control preventivo, a lo menos, dos veces a la semana (días lunes y jueves).

3. 8. Se debe dejar un registro de las actividades que se realizan en las visitas de mantenimiento.

3. 9. Las máquinas que no tienen instalado sistemas operativos basados en tecnología Microsoft, están exentas de cumplir con la política prevención, detección y corrección de virus.

3. 10. La tercera semana de cada mes se deberá generar un reporte de verificación de revisión de virus, que será la base para coordinar revisiones en las computadoras que presenten problemas asociados a virus.

3. 11. Deben existir planes de continuidad del negocio apropiados para la recuperación ante los ataques de código malicioso, incluyendo todos los datos y *software* necesarios de respaldo y las disposiciones para la recuperación de los servidores.

3. 12. Se debe implementar un procedimiento para recolectar de forma regular información, tal como suscripción a las listas de correo y/o comprobación de los sitios web que brindan la información sobre nuevo código malicioso.

3. 13. Se deben implementar procedimientos para verificar toda la información relativa al *software* malicioso y asegurarse que los boletines de alerta son precisos e informativos. Los responsables deberán asegurar que se diferencien los códigos maliciosos reales de los falsos avisos, usando fuentes calificadas, por ejemplo, revistas expertas, sitios de Internet fiables o proveedores de *software* contra código malicioso. Se deberá advertir a los usuarios sobre el problema de los falsos avisos de código malicioso y qué hacer en caso de recibirlos.

……..…..……última página anexo 7……..…..……

Anexo 8. Procedimiento de conexión de Acceso Remoto

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de conexión de Acceso Remoto
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Definir normas para la conectividad desde equipos y/o redes del exterior hacia la red del Instituto Interamericano de Cooperación para la Agricultura (IICA).

2. Alcance

Este procedimiento aplica a todo usuario autorizado a utilizar el acceso por la Red Virtual Privada a la plataforma institucional.

3. Procedimiento de conexión de acceso remoto

3. 1. Las solicitudes para conexiones remotas deben ser extendidas al área de Soporte Redes, por la jefatura de la unidad correspondiente por OTRS. En el caso de las oficinas, el Administrador de la Representación envía la solicitud por correo electrónico con copia al Representante.

3. 2. El área de Soporte Redes es el único autorizado en proveer los mecanismos para establecer las conexiones remotas.

3. 3. El único servicio de acceso remoto permitido hacia la red institucional es a través de la red privada virtual (VPN).

3. 4. Las conexiones de VPN hacia la red institucional, deben controlarse a través de un nombre de usuario y clave, extendidas por la Gerencia de

Tecnología de Información, Comunicación y Agricultura Digital del IICA.

3. 5. Toda estación conectada a la red del IICA, deberá estar claramente identificada con una dirección IP, y se deberá especificar un responsable de la conexión.

3. 6. Cada usuario podrá tener una única conexión activa por VPN.

3. 7. Es responsabilidad de los usuarios autorizados que utilicen el acceso remoto a las redes de la Institución, asegurarse de tener las mismas consideraciones como si estuvieran directamente conectados a la red de la Institución.

3. 8. Todos los equipos que se conecten a las redes internas del IICA a través de conexión remota, deben tener su antivirus al día.

3. 9. El usuario autorizado no deberá proporcionar información de acceso remoto a ninguna otra persona.

3. 10. En caso de que se trate de conexiones temporales, se deberá indicar en la solicitud la fecha en que debe finalizar el permiso de acceso a la VPN institucional.

……..…..……última página anexo 8……..…..……

Anexo 9. Procedimiento de control de acceso físico al *Data center*

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de control de acceso físico al *Data center*
APLICACIÓN	GTIC-AD (Sede Central únicamente)
FORMATO	Electrónico – Word
PÁGINAS	5
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Establecer los lineamientos que deben ser considerados para el control de acceso al Centro de datos del Instituto y garantizar el resguardo de la información y la continuidad de los servicios de red bajo estrictas medidas de seguridad.

2. Alcance

Esta política aplica a todos quienes trabajen en el IICA, personal externo y visitas autorizadas, a la hora de ingreso al centro de datos.

3. Procedimiento para la administración de claves de usuario:

3. 1. El perímetro de seguridad del área del centro de datos deberá estar claramente definido, la ubicación y la resistencia de cada uno de los perímetros dependerán de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una evaluación de riesgos.

3. 2. El perímetro del centro de datos deberá tener solidez física (por ejemplo, no debe tener zonas que puedan derribarse fácilmente); los muros externos del lugar deben ser sólidos y todas las puertas exteriores deberán estar convenientemente protegidas contra accesos no autorizados, mediante mecanismos de control, por ejemplo, barreras, alarmas, cerraduras, etc., puertas y ventanas deberán estar bloqueadas cuando se encuentren descuidadas.

3. 3. Cualquier visitante incluyendo funcionarios, personal de contrato y empleados de terceros deberán utilizar algún tipo de identificación visible.

3. 4. Los derechos de acceso a las áreas seguras deben ser regularmente revisados y actualizados, y revocados cuando sea necesario.

3. 5. Se deben tomar en cuenta las regulaciones y normativas pertinentes en materia de salud y seguridad vigentes.

3. 6. Se debe tomar en consideración cualquier amenaza de seguridad presentada por las instalaciones vecinas, por ejemplo, incendios, inundaciones o explosiones.

3. 7. Solo personal autorizado puede ingresar al centro de datos, el acceso de personal externo al centro de datos debe quedar registrado, detallando motivo, nombre y apellido, identificación de la empresa, fecha, hora de entrada/ salida y quien autoriza el ingreso.

3. 8. El ingreso al centro de datos debe tener acceso restringido, mediante autenticación por clave y tarjeta de acceso.

3. 9. La clave de ingreso al centro de datos será definida por el usuario junto con el encargado de seguridad perimetral directamente en el sistema de acceso al centro de datos. Esta clave puede tener hasta un máximo de 6 dígitos.

3. 10. Las tarjetas de control de acceso son intransferibles, por lo que queda estrictamente prohibido el préstamo o intercambio de estas entre personal de la Gerencia de Tecnología de Información, Comunicación y Agricultura Digital del IICA.

3. 11. En caso de pérdida de la tarjeta de control de acceso, el funcionario de la GTIC-AD deberá enviar una solicitud por "*help desk"* a Soporte Redes, con el fin de informar y otorgar una nueva tarjeta de acceso.

3. 12. Las tarjetas de visita, entregadas por el oficial de seguridad, deben estar visibles durante la permanencia del personal externo en la institución.

3. 13. El centro de datos debe estar protegido por puertas de seguridad que resistan fuego, intentos de ingreso a la fuerza, etc.

3. 14. La puerta del centro de datos debe estar equipada con dispositivos que la cierren automáticamente.

3. 15. Cuando un funcionario de la GTIC-AD deja de prestar funciones debe devolver la tarjeta de control asignada y se debe eliminar la clave de acceso al centro de datos.

3. 16. Los materiales peligrosos o combustibles deberán ser almacenados a una distancia prudente de al menos 25 metros de un área segura. Los suministros a granel tales como los materiales de oficina no deben almacenarse dentro de un área segura.

3. 17. El equipo de reserva y los medios de respaldo deberán estar ubicados a una distancia prudente para evitar daños producto de un desastre que afecten al emplazamiento principal.

3. 18. No es permitido el ingreso de comidas o líquidos al centro de datos ya que puedan dañar la integridad de los equipos.

3. 19. No se permite fumar dentro del centro de datos.

3. 20. El centro de datos debe tener detectores de humo y equipo para mitigar incendios.

3. 21. No se permiten las conexiones en cadena de varias Unidades de Distribución Energética (PDU por sus siglas en inglés) conocidas como regletas. Esto aumenta el riesgo de ocasionar un incendio y una potencial sobrecarga de los circuitos eléctricos, resultando en la pérdida de energía del PDU o del circuito completo.

3. 22. Todos los elementos de soporte, tales como electricidad, abastecimiento de agua, aguas residuales, calefacción/ventilación, y aire acondicionado deberán ser adecuados para los sistemas que están apoyando. Los elementos de soporte deberán ser examinados regularmente y probados adecuadamente de manera de asegurar su funcionamiento apropiado y reducir cualquier riesgo de mal funcionamiento o falla.

3. 23. Deberá existir un suministro eléctrico apropiado conforme con las especificaciones del fabricante del equipo.

3. 24. Se deberá contar con una fuente de energía ininterrumpida (UPS) para asegurar el correcto apagado o el funcionamiento continuo del equipo que soporta las operaciones críticas del negocio.

3. 25. Los equipos de UPS y los generadores se deberán inspeccionar regularmente para asegurar que tienen la capacidad requerida y probarlos de acuerdo con las directrices del fabricante.

3. 26. El equipo de telecomunicaciones deberá estar conectado con el proveedor al menos a través de dos rutas distintas para prevenir fallas en el servicio de una de las rutas de conexión imposibilitando los servicios de voz. Los servicios de voz se deberían adecuar para alcanzar los requisitos legales locales para comunicaciones de emergencia.

3. 27. Se deberán adoptar controles para reducir al mínimo el riesgo de amenazas físicas potenciales, por ejemplo, hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo.

3. 28. Las condiciones ambientales, tales como temperatura y humedad, deberán ser supervisadas para verificar que las mismas no afectan negativamente el funcionamiento de las instalaciones de procesamiento de la información. Esta supervisión se realizará de forma diaria al inicio y al final de la jornada laboral y se registrará la temperatura y la humedad relativa reportada por el equipo de monitoreo.

3. 29. Se deberán colocar pararrayos sobre todos los edificios y se deberán aplicar filtros de protección contra rayos a todas las líneas entrantes de energía y de comunicaciones.

3. 30. Se deberán utilizar marcas claramente identificables en cables y equipo para reducir al mínimo los errores de manejo, tales como conexiones accidentales erróneas de los cables de red.

3. 31. Se deberá utilizar una lista documentada de las conexiones para reducir la posibilidad de errores.

3. 32. El equipo que se encuentra dentro del centro de datos deberá recibir el mantenimiento necesario de acuerdo con los niveles de servicio establecidos en el contrato de mantenimiento.

3. 33. Sólo el personal de mantenimiento debidamente autorizado podrá realizar reparaciones y mantenimiento a los equipos.

3. 34. Se deberán mantener registros de todos los fallos, reales o sospechas, así como de todo el mantenimiento preventivo y correctivo.

3. 35. Se deberán implementar los controles adecuados en los casos en que sea necesario dar mantenimiento a equipos que contengan información confidencial, de manera que la información se mantenga convenientemente resguardada.

3. 36. Se deberá cumplir con todos los requisitos impuestos por pólizas de seguros.

……..…..……última página anexo 9……..…..……

II. ANEXOS: PROCEDIMIENTOS DE USUARIOS

Anexo 10 - Procedimiento para el uso de dispositivos móviles

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento para el uso de dispositivos móviles
APLICACIÓN	Unidades de la Sede Central y todas las Representaciones del IICA
FORMATO	Electrónico – Word
PÁGINAS	
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Establecer y asegurar la aplicación de los criterios esenciales sobre el uso de los dispositivos móviles provistos a los funcionarios del Instituto Interamericano de Cooperación para la Agricultura (IICA), de manera que se haga un uso conveniente y razonable de este tipo de recursos institucionales.

2. Alcance

Estos lineamientos aplican a todo funcionario que haga uso de dispositivos móviles (computadores portátiles, *smartphones* y PDA's) institucionales. Entiéndase por dispositivo móvil, cualquier dispositivo electrónico portable, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar a cabo otras funciones más generales.

El uso de los dispositivos móviles mencionados en este Manual está regulado por la orden ejecutiva No. 19rev.

3. Procedimiento para para el uso de dispositivos móviles

3. 1. Cada dispositivo móvil institucional es asignado mediante un documento formal a una persona responsable quien será garante de su custodia y buen uso.

3. 2. El uso del dispositivo es exclusivo de la persona responsable, excepto en los casos en que se designe el dispositivo como de uso común para una respectiva dependencia, esto con el fin de evitar usurpación de identidad, mal uso o fuga de información institucional.

3. 3. Los dispositivos móviles cuyo valor sea mayor a $100, deberán ser registrados en el inventario institucional siguiendo los procedimientos oficiales vigentes.

3. 4. Los dispositivos móviles institucionales independientemente de su ubicación física deben estar bien resguardados, por parte de la persona responsable, de manera que se minimice al máximo la exposición a daños, pérdida o robo.

3. 5. Cuando los dispositivos móviles se encuentren dentro de las instalaciones del Instituto, deben ser resguardados en condiciones ambientales y de seguridad apropiadas, evitando la exposición innecesaria del aparato.

3. 6. Cuando los dispositivos móviles se encuentren fuera de las instalaciones del Instituto, éstos deben permanecer en lugares seguros y siempre bajo la supervisión del responsable.

3. 7. En caso de viaje deben tomarse las precauciones necesarias para evitar que el equipo pueda verse afectado de alguna manera. En los viajes por avión, autobús, tren o algún otro medio público, los dispositivos móviles deben viajar como equipaje de mano junto al pasajero, y no documentarse como carga o equipaje. No se recomienda dejar a la vista ninguna etiqueta que identifique al equipo como propiedad del IICA.

3. 8. Ningún dispositivo móvil debe ser dejado desatendido dentro de los vehículos. Se recomienda no dejar los dispositivos móviles en los automóviles o en la cajuela de estos, ya que se exponen a robos o daños por severas temperaturas.

3. 9. Si es necesario dejar una computadora portátil desatendida en alguna oficina, cuarto de reuniones o cuarto de hotel, debe utilizar el cable (candado) de seguridad, para sujetar el dispositivo al escritorio. En

caso de no contar con el cable de seguridad, el responsable deberá tenerla consigo siempre.

3. 10. Cuando se trate de cualquier otro dispositivo móvil más pequeño, deberá estar custodiado todo el tiempo por la persona responsable, esto con el fin de evitar la pérdida o robo de información, así como del aparato.

3. 11. Los Oficiales de Seguridad tendrán la obligación de asegurar que, en periodos vacacionales, fines de semana, o nocturnos no haya acceso sin excepción de personal a las oficinas. Para tener acceso en estos periodos deberá contar con un permiso expreso del responsable de la Unidad o del Representante. Los Oficiales deberán llevar un registro del personal que ingresa, anotando el motivo del acceso de las oficinas fuera de horario regular, hora de ingreso/salida, así como, verificar a la entrada y salida de los equipos y activos de la Oficina.

3. 12. Los funcionarios deberán asegurarse de que los equipos portátiles o móviles deberán ser guardados en lugares que ofrezcan la mayor seguridad, es responsabilidad de los funcionarios responder sobre el activo. En caso para las oficinas que no tienen un esquema de seguridad para salvaguardar los equipos móviles en periodos de ausencia, pueden buscar asesoría a la GTIC-AD en el caso de la Sede Central, o la Administración en la Representación, para salvaguardar el equipo con las medidas necesarias para evitar robos o mal uso de los equipos.

3. 13. Se debe evitar el almacenamiento de información sensible en los dispositivos móviles, a menos que cuenten con mecanismos seguros de encriptación. Se recomienda no guardar contraseñas o información clasificada como confidencial para el Instituto. Esto para evitar la pérdida o robo de información sensible del Instituto.

3. 14. Cualquier daño que pueda presentar un dispositivo móvil propiedad del Instituto, ya sea por accidentes u otra causa, debe ser reportado lo más pronto posible a la GTIC-AD en el caso de la Sede Central, o la Administración en la Representación, por medio de una solicitud, de tal manera que se pueda realizar la reparación correspondiente. La GTIC-AD y la Administración en la Representación se hace responsable por reparos únicamente en dispositivos móviles que sean propiedad del Instituto.

3. 15. En caso de pérdida, robo o hurto del dispositivo móvil, el responsable del activo deberá informar de lo sucedido a las instancias

institucionales correspondientes en cumplimiento con la normativa institucional vigente.

3. 16. Cualquier *software* adicional, cambio de configuración o de seguridad requerido deberá ser instalado únicamente por personal autorizado.

3. 17. Se requiere que las computadoras portátiles tengan un nivel aceptable de funcionalidad, por lo tanto, en caso de cualquier instalación de *software* detectada y que pueda poner en riesgo la seguridad de la información institucional, la GTIC-AD se reserva el derecho realizar la desinstalación correspondiente. En el caso de las Representaciones esto será coordinado con la GTIC-AD.

3. 18. Es responsabilidad del usuario que está conectado a la red institucional mediante su dispositivo móvil asegurarse que todos los requisitos de su conexión se mantengan tan seguros como si se estuviese en su computadora de oficina, deberá asegurarse que no contiene virus, *software* malicioso, o algún otro *software* que pueda poner en peligro la plataforma tecnológica, en caso de dudas se deberá contactar a la GTIC-AD en el caso de la Sede Central, o la Administración en la Representación, para la asesoría correspondiente. La GTIC-AD se reserva el derecho de eliminar el acceso de un dispositivo móvil a cualquier punto de red que ponga en riesgo los sistemas, información, usuarios o red institucional, en el caso de las Representaciones la Administración debe velar por la seguridad institucional.

3. 19. Cualquier dispositivo móvil configurado para acceder los recursos del Instituto mediante redes inalámbricas, debe realizar sus conexiones con la apropiada autenticación provista por la GTIC-AD en el caso de la Sede Central, o la Administración en la Representación. En caso de que exista sospecha de incidentes de accesos no autorizados a los recursos del Instituto (correo, intranet, etc.), se debe indicar inmediatamente a la GTIC-AD mediante el *“help desk”* institucional, y al Administrador en el caso de las Representaciones

3. 20. En caso de renuncia, todos los dispositivos móviles y sus respectivos accesorios deben ser devueltos a las Unidad respectiva el último día de trabajo, en caso de las Representaciones, al Administrador.

……..…..……última página anexo 10……..…..……

Anexo 11 - Procedimiento de creación, acceso y eliminación de cuentas en servicios informáticos

TIPO DE DOCUMENTO			
			Público (disponible en el Sitio Web del IICA)
		X	Privado (disponible en la intranet del IICA)
TÍTULO	Procedimiento de creación, acceso y eliminación de cuentas en servicios informáticos		
APLICACIÓN	GTIC-AD y todas las Representaciones del IICA		
FORMATO	Electrónico – Word		
PÁGINAS	5		
REF. APROBACIÓN	SC/DG-405		
VERSIÓN	**FECHA**	**AUTOR**	
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura	

1. Objetivo

Establecer los lineamientos para la creación y eliminación de cuentas de usuarios de los diferentes servicios informáticos que provee la GTIC-AD y las Representaciones con el fin de garantizar el funcionamiento adecuado de la plataforma tecnológica del Instituto.

2. Alcance

Aplica a todos los usuarios autorizados para utilizar los servicios informáticos administrados por la GTIC-AD.

3. Procedimiento para la creación de cuentas de usuarios de servicios informáticos

3. 1. La plataforma tecnológica propiedad del Instituto Interamericano de Cooperación para la Agricultura (IICA), será administrada por la GTIC-AD y las Representaciones. Dicha plataforma estará a disposición de los diferentes tipos de usuarios del Instituto y solo deberá ser utilizada para propósitos específicos del Instituto.

3. 2. La plataforma tecnológica está compuesta por una infraestructura tanto de *software* como de *hardware* que provee diversos servicios a sus usuarios entre los cuales están: red institucional, correo electrónico, intranet, internet, sistemas de información, VPN y telefonía IP y herramientas de seguridad entre otros.

3. 3. Por ser la GTIC-AD la encargada de gobernar y gestionar la infraestructura tecnológica del Instituto, las solicitudes de acceso a los servicios informáticos serán canalizadas directamente a través de ésta. Esta Gerencia con insumos de la Gerencia de Talento Humano y las Representaciones mantendrá un registro actualizado de los usuarios con accesos activos en los servicios informáticos del IICA.

3. 4. La cantidad de recursos informáticos es limitada, por lo que se deberá considerar al resto de los usuarios con los que se comparten estos recursos.

3. 5. Corresponde a todos los usuarios mantener la confidencialidad de sus claves de acceso (*passwords*) a los diferentes servicios tecnológicos: red, correo electrónico, intranet y sistemas de información, entre otros.

3. 6. Cuando se suministra equipo informático al usuario (computador de escritorio o portátil), este equipo debe contar con todo el *software* necesario para realizar sus labores, así como los esquemas de seguridad necesarios, el usuario no deberá instalar ningún *software* o herramienta sin autorización de la GTIC-AD o del Administrador en el caso de las Representaciones.

3. 7. No se deberá almacenar en los servidores institucionales archivos o información no institucional, como por ejemplo (fotografías personales, música, videos). En caso de que la GTIC-AD encontrase este tipo de contenidos, los archivos serán eliminados de forma inmediata. Misma labor, deberá realizar la Administración en las Representaciones.

3. 8. Para la eliminación de cuentas de usuarios de la plataforma se debe proceder, de acuerdo con la solicitud respectiva por parte de la Gerencia de Talento Humano o de la Administración en las Representaciones.

4. Tipos de usuarios

De acuerdo con la normativa institucional, el IICA establece diferentes criterios de clasificación del personal, consultores y proveedores de bienes y servicios; estas clasificaciones poseen diferentes roles y responsabilidades, así como derechos y deberes dentro del Instituto. Para cada una de estas clasificaciones se han definido una serie de normas en cuanto al uso de la plataforma tecnológica del Instituto.

5. Acceso al correo electrónico

La cuenta de correo electrónico de los usuarios será definida como nombre.apellido@iica.int. El identificador (ID) del usuario estará compuesto por nombre.apellido, en caso de que ya exista, se utiliza nombre.nombre2.apellido ó en su defecto nombre.apellido.apellido2.

Cada vez que se ingrese o elimine un usuario de correo, la acción será registrada el sistema automatizado de registro de solicitudes.

6. Acceso a la red

6. 1. A la red institucional de la Sede Central y en las Representaciones podrán ingresar únicamente los usuarios autorizados, quienes deberán superar el proceso de autenticación de *Windows* para acceder a la red institucional.

6. 2. El identificador de usuario de red estará compuesto por la primera letra del nombre junto con el primer apellido completo, en caso de que ya exista se utilizará adicionalmente la primera letra del segundo nombre con el primer apellido completo ó la segunda letra del primer nombre junto con el primer apellido completo.

6. 3. Al usuario se le indicará la clave de acceso inicial para que pueda ingresar a la red, misma que deberá modificar la primera vez que logre ingresar a la red, esto por solicitud expresa y de forma automática del sistema operativo.

6. 4. La clave definida por el usuario deberá ser mayor o igual a 8 caracteres y estará compuesta únicamente por letras y/o números.

6. 5. El cambio de clave será automático, con una periodicidad de 90 días.

6. 6. La clave que defina el usuario no podrá ser igual a las últimas 5 claves anteriormente utilizadas.

6. 7. Cada vez que se ingrese o elimine un usuario de red, la acción será registrada en el sistema automatizado de registro de solicitudes.

7. Acceso a intranet

7. 1. Cada usuario institucional podrá ingresar a la intranet utilizando el usuario de correo electrónico.

7. 2. Para acceder a la intranet institucional el usuario podrá utilizar cualquier navegador, sin embargo, se recomienda utilizar *Microsoft Edge* o *Google Chrome* para que tenga acceso a todas las funcionalidades del sitio.

7. 3. La dirección (URL) será facilitada por la GTIC-AD a los usuarios, misma que deberá ser ingresada en el navegador para que puedan ingresar a la intranet institucional.

8. Acceso a los sistemas de información

Para la creación de cuentas de usuarios de la plataforma tecnológica del IICA, se debe proceder, de acuerdo con la solicitud respectiva por parte de la Gerencia de Talento Humano o de la Administración en las Representaciones. Posteriormente se le asignarán los respectivos roles de acuerdo a su perfil, a la cuenta creada por parte de la Gerencia de Tecnología de Información, Comunicación y Agricultura Digital.

Las aplicaciones que se utilizan mediante la intranet, validarán la cuenta y contraseña del usuario de intranet, es decir, para que el usuario acceda al sistema debe ingresar a la intranet con su ID y clave y desde ahí podrá acceder a los sistemas para los que posea las autorizaciones correspondientes.

Las aplicaciones de escritorio (que no están en intranet), validarán su ingreso de acuerdo al ID y clave de red, esto significa que el usuario desde el escritorio de su PC, podrá ingresar a los diferentes sistemas indicando para cada uno, el mismo ID y clave que utiliza en la red. Si la clave de red es modificada, para acceder a los sistemas el usuario deberá utilizar la nueva clave, sin ejecutar ningún paso adicional.

En el caso de los sistemas integrados, cada uno tendrá sus lineamientos de administración de usuarios, como se presenta un ejemplo a continuación:

Sistema	ID usuario	Clave inicial	Tamaño mínimo de la clave	Vigencia de la clave	Distinción mayúsculas y minúsculas	Histórico claves
SAP	Primera letra del nombre y primer apellido	IIabvaaaa: II Iniciales nombre y apellido abv: abreviatura del mes aaaa: Año	8 (con al menos 3 dígitos numéricos)	90 días	NO	14

En el caso de que se requiera crear cuentas genéricas de dominio o cuentas genéricas en sistemas, deberán registrarse con una justificación y el responsable que lo solicita.

……..…..……última página anexo 11……..…..……

Anexo 12. Procedimiento cambio de funciones de usuarios de servicios informáticos

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento cambio de funciones de usuarios de servicios informáticos
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	2
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Definir los lineamientos para cambiar las funciones en servicios informáticos de los usuarios de estos servicios.

2. Alcance

Este procedimiento aplica a todos quienes tengan asignada una cuenta de usuario de red ya sea en la Sede Central o en las Representaciones.

3. Procedimiento para el cambio de funciones de usuarios de servicios informáticos

3. 1. Es posible que un usuario del IICA cambie sus funciones por diversas razones, cuando esto sucede la Gerencia de Tecnología de Información, Comunicación y Agricultura Digital (GTIC-AD) debe ser notificada formalmente del cambio, a partir de qué fecha se hace efectivo y si este cambio es temporal o permanente. De manera que se cuente con la información necesaria para realizar los cambios requeridos, en cuanto a grupos de correo, archivos compartidos, aplicaciones web, aplicaciones de escritorio o cualquier otra donde la administración de los usuarios se encuentre bajo la responsabilidad de la GTIC-AD. Para esto es necesario que la jefatura de cada

Unidad de trabajo involucrada le indique a la GTIC-AD los permisos y accesos que deben ser creados, modificados o eliminados.

3. 2. Si se realizan cambios a nivel de cuenta de red, se debe tener en consideración que, si se elimina la cuenta de red del *Active Directory*, serán eliminados los accesos por *VPN* y a las aplicaciones de escritorio.

3. 3. Si se realizan cambios con respecto a los grupos de usuarios, éstos deben quedar debidamente documentados en la herramienta de administración de grupos de usuarios.

3. 4. Si se realizan cambios con respecto a la cuenta de intranet, éstos deben ser registrados en la bitácora respectiva. Cabe mencionar que al eliminar la cuenta de intranet se elimina automáticamente el acceso a los sistemas *web* en los que el usuario haya sido incluido con anterioridad. No así el registro del usuario dentro de cada sistema, por eso se recomienda además eliminar la cuenta de usuario definida en cada sistema (*web* o escritorio).

3. 5. Si se realizan modificaciones relacionadas con accesos a diversas aplicaciones, se deben actualizar las bitácoras de cada aplicación según sea el caso. Cabe mencionar que solamente se hará en las aplicaciones cuya administración de usuarios sea responsabilidad de la GTIC-AD. En caso de que el administrador de usuarios en alguna aplicación conozca que, en alguna área, o para algún grupo o tipo de usuarios se hicieron cambios, sin haberse notificado a la GTIC-AD, contactará al responsable en el área usuaria para procurar la actualización de los permisos.

3. 6. De ser necesario se deshabilitará o eliminará la extensión telefónica, y se reactivará o creará una nueva extensión telefónica, según sea especificado por la jefatura de la Unidad correspondiente.

……..…..……última página anexo 12……..…..……

Anexo 13 - Procedimiento de autorización de *Bring Your Own Device (BYOD)*

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de autorización de BYOD
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	2
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Autorizar y registrar dispositivos BYOD para el desempeño de las funciones en el IICA.

2. Alcance

A todos los funcionarios, consultores, personal asociado y pasantes que requieran utilizar sus equipos personales para el desempeño de sus actividades en el marco de la relación contractual con el IICA.

3. Procedimiento para la autorización y registro de dispositivos BYOD para el desempeño de las funciones en el IICA:

3. 1. Cuando un funcionario desea utilizar dispositivos móviles personales en sus labores en el IICA debe contar con autorización expresa para ello.

3. 2. En el caso de la Sede Central y la Representación en Costa Rica la solicitud de autorización de equipo móvil personal se realizará la GTIC-AD, exponiendo las razones por las que el funcionario interesado requiere de usar su dispositivo personal en sus labores en el IICA. Para las demás Representaciones la solicitud debe ser dirigida a la Administración con la debida justificación.

3. 3. En caso de que se autorice el uso del dispositivo personal para el desarrollo de las labores, se debe validar que el dispositivo móvil cumpla con los requerimientos tales como: sistema operativo y antivirus actualizados.

3. 4. La GTIC- AD en la Sede Central y la Administración en las Representaciones debe levantar una lista de las aplicaciones y bases de datos del IICA a las que el funcionario podrá acceder desde su dispositivo.

3. 5. La GTIC- AD en la Sede Central y la Administración en las Representaciones debe registrar el BYOD en la bitácora de dispositivos personales autorizados, correspondiente.

3. 6. La GTIC- AD en la Sede Central y la Administración en las Representaciones deben velar por que al dispositivo se le instalen protecciones adicionales adecuadas en caso de que con el dispositivo se pueda acceder a información clasificada como confidencial.

……..…..……última página anexo 13……..…..……

Anexo 14. Procedimiento de administración de claves de usuarios

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de administración de claves de usuarios
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	4
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Especificar los lineamientos de seguridad para la creación, protección y frecuencia de cambio de las claves de usuario y garantizar una administración apropiada de la plataforma tecnológica del Instituto.

2. Alcance

Incluye a todo el personal que tiene bajo su responsabilidad alguna clave de: usuario de dominio (incluye clave de administración de servidores), administración de equipos de comunicaciones, correo electrónico y aplicativos adquiridos por el Instituto. La responsabilidad de este procedimiento aplica para la Sede Central y las Representaciones del IICA.

3. Procedimiento para la administración de claves de usuario:

4.1.1. Se debe realizar cambio de clave por parte de los usuarios posterior al primer ingreso en el computador y/o sistema que corresponda, a excepción de las aplicaciones que no dispongan de esa funcionalidad.

4.1.2. El usuario debe cambiar las claves cada tres meses o cuando se sospeche que alguien conoce la contraseña. Este lineamiento aplica para la clave de dominio de red, y SAP, entre otros.

4.1.3. En la medida de lo posible, se recomienda que el usuario no utilice la misma clave para las cuentas de la institución y para otras cuentas

que no tengan relación con la misma. Se recomienda no utilizar la misma clave para acceder a diferentes cuentas.

4.1.4. El usuario será responsable por el mal uso que se haga de su clave cuando de forma voluntaria o involuntaria comparta sus claves con terceros.

4.1.5. Se deben habilitar accesos temporales en el caso de usuarios que realicen suplencias en forma temporal.

4.1.6. Se recomienda no activar las características de recordatorio de claves que traen las aplicaciones y/o navegadores *web*, para evitar una eventual suplantación de identidad. Por ejemplo, si un usuario tiene acceso al computador de su superior, quien a su vez utiliza el recordatorio de claves, podría acceder a la intranet (usurpando la identidad de su superior) y llenar el formulario de *websense* para auto-asignarse permisos para visitar sitios web restringidos. En este caso se verá perjudicado tanto el usuario que usurpa el computador así como el usuario (superior) que utiliza el recordatorio de claves del navegador que utilice.

4.1.7. El usuario no debe revelar datos sobre la forma o estructura de sus claves.

4.1.8. El usuario no debe escribir sus claves en papel.

4.1.9. El usuario no debe usar claves antiguas o ejemplos dados como claves. Cuando el usuario define una nueva clave o contraseña, la misma no podrá ser igual a las últimas cinco claves anteriormente utilizadas (histórico de claves).

4.1.10. La clave debe estar configurada para aceptar un mínimo de 8 caracteres. [3]

4.1.11. Siempre que los niveles de seguridad de los sistemas lo permitan, la clave debe contener caracteres alfabéticos y numéricos.

4.1.12. Se hará distinción entre mayúsculas y minúsculas.

[3] A excepción de las claves para intranet cuando no se pueda utilizar la clave de red para el ingreso.

4.1.13. El acceso a los sistemas será bloqueado después del tercer intento de acceso denegado.[4]

4.1.14. Los bloqueos por intento fallido de conexión serán levantados solo por los administradores de sistemas.

4.1.15. En caso de que el usuario solicite un cambio de clave, éste no podrá modificarla en los siguientes 4 días, posteriores al ingreso de la nueva clave.

4.1.16. El usuario deberá bloquear (Ctrl+Alt+Supr) la sesión de trabajo cada vez que deba ausentarse del escritorio para evitar el mal uso de sus privilegios.

4.1.17. Las claves de administradores de la plataforma tecnológica deben estar resguardadas en un sobre sellado almacenado en la caja fuerte.

4.1.18. Las claves de administradores de servidores deben ser cambiadas cada 90 días o cuando sea abierto el sobre sellado almacenado en la caja fuerte por una situación de emergencia.

4.1.19. Las claves del administrador de dominio y de equipos de comunicación deberán ser modificadas una vez al año.

4.1.20. Las claves de administradores de los sistemas deber ser cambiadas al menos una vez al año o según las necesidades de cada sistema.

4. Estándar para desarrollo de aplicaciones

4. 1. Los especialistas en tecnología de información y comunicación encargados del desarrollo de aplicaciones deben asegurar que sus programas contengan las siguientes precauciones:

4.1.1. Los accesos a los sistemas deben controlarse a través de un nombre de usuario.

4.1.2. El almacenamiento de las claves se debe realizar utilizando mecanismos de encriptación resguardando la confidencialidad e integridad de estas.

[4] En el caso de SAP, al tercer intento fallido cancela la sesión y al quinto intento fallido bloquea el usuario.

4.1.3. La asignación de identificaciones de usuario (IDs) y contraseñas se debe realizar de forma individual con el fin de establecer responsabilidades.

4.1.4. Los usuarios podrán seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para evitar errores al introducirlas.

4.1.5. Los usuarios deberán utilizar contraseñas válidas.

4.1.6. Los usuarios deberán modificar sus contraseñas periódicamente de acuerdo con lo que indique este Manual.

4.1.7. Los usuarios deberán modificar su contraseña temporal en su primera conexión.

4.1.8. Los sistemas deberán mantener un registro de las anteriores contraseñas utilizadas, e impedir su reutilización.

4.1.9. Los sistemas no mostrarán en pantalla la contraseña cuando ésta se introduce en el proceso de autenticación.

4.1.10. Los sistemas deberán almacenar los archivos de contraseñas en lugares diferentes de los datos del sistema de aplicaciones.

4.1.11. Los sistemas deberán almacenar y transmitir las contraseñas en formatos protegidos (por ejemplo, cifradas).

5. Acceso remoto

El acceso a las redes del Instituto en forma remota, debe ser controlado usando autenticación por clave (a través de la red privada virtual, VPN). La autenticación de usuarios IICA es en el "*active directory*" y el personal externo se autentica mediante "*authentication cisco server* (ACS)".

……..…..……última página anexo 14……..…..……

Anexo 15. Procedimiento creación cuenta de correo electrónico

IICA TIPO DE DOCUMENTO			Público (disponible en el Sitio Web del IICA)
		X	Privado (disponible en la intranet del IICA)
TÍTULO	Procedimiento creación cuenta de correo electrónico		
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central		
FORMATO	Electrónico – Word		
PÁGINAS	1		
REF. APROBACIÓN	SC/DG-405		
VERSIÓN	**FECHA**	**AUTOR**	
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura	

1. Objetivo

Definir los lineamientos para crear una cuenta de usuario de correo electrónico para funcionarios del Instituto.

2. Alcance

Este procedimiento aplica a todos quienes tengan asignada una cuenta de usuario de correo electrónico ya sea en la Sede Central o en las Representaciones.

3. Procedimiento para la creación de cuentas de correo electrónico:

3. 1. La GTIC-AD en coordinación con la Gerencia de Talento Humano en la Sede Central y el Administrador en las Representaciones debe enviar la solicitud de creación de la cuenta de correo electrónico.

3. 2. Con base en los datos suministrados por la unidad solicitante (en la herramienta de *help desk* OTRS), la cuenta de correo electrónico es creada, siguiendo los estándares y políticas utilizadas en la GTIC-AD.

3. 3. El funcionario de soporte a usuarios realizará la configuración del acceso a la cuenta de correo electrónico.

……..…..……última página anexo 15……..…..……

Anexo 16. Procedimiento eliminación de cuenta de usuario del correo electrónico

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento eliminación de cuenta de usuario del correo electrónico
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	2
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Definir los lineamientos generales para eliminar una cuenta de usuario de correo electrónico institucional.

2. Alcance

Este procedimiento aplica a todos quienes tengan asignada una cuenta de correo electrónico ya sea en la Sede Central o en las Representaciones.

3. Procedimiento para la eliminación de cuentas de correo electrónico

3. 1. La jefatura de la Unidad interesada en la Sede Central y el Administrador en las Representaciones debe enviar la solicitud de eliminación de la cuenta de correo electrónico a la GTIC-AD.

3. 2. Con base en los datos suministrados por la unidad solicitante (en la herramienta de *help desk* OTRS), se inhabilita la cuenta para envío de correo a partir de la fecha indicada en el formulario. El buzón de correo no será eliminado en ese momento, se dará un plazo de 30 días naturales, excepto que explícitamente se indique otro plazo en la solicitud o que se indique que el buzón de correo se debe eliminar de forma inmediata.

3. 3. El buzón de correo se eliminará permanentemente 30 días naturales a partir de la fecha en que se inhabilite la cuenta de correo electrónico. Excepto que expresamente se solicite por las autoridades del Instituto lo contrario.

3. 4. Se registran los datos de la eliminación permanente del buzón de correo en la bitácora correspondiente.

……..…..……última página anexo 16……..…..……

Anexo 17. Procedimiento creación cuenta de usuario de red

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento creación cuenta de usuario de red
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	1
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Definir los lineamientos generales para crear una cuenta de usuario de red tanto para la Sede Central como para las Representaciones.

2. Alcance

Este procedimiento aplica a todos quienes tengan asignada una cuenta de usuario de red ya sea en las Sede Central o en las Representaciones.

3. Procedimiento para la creación de cuentas de usuarios de red

3. 1. La jefatura de la Unidad interesada en la Sede Central y el Administrador en las Representaciones debe enviar la solicitud de creación de la cuenta de red a GTIC-AD.

3. 2. Se le habilitan los permisos necesarios para que el nuevo usuario tenga acceso a las impresoras, carpetas y archivos compartidos de la unidad donde iniciará labores, según sea indicado en el formulario de solicitud.

3. 3. Se le entrega al usuario el ID y la clave, indicándole que el controlador de dominio le solicitará cambiar la clave la primera vez que lo acceda. Además, se le brindarán al usuario las recomendaciones para el cambio de la clave de acuerdo con los lineamientos institucionales.

Anexo 18. Procedimiento creación cuenta de intranet

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento creación cuenta de intranet
APLICACIÓN	GTIC-AD y todas las Representaciones
FORMATO	Electrónico – Word
PÁGINAS	
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Definir los lineamientos generales para crear una cuenta de usuario de intranet para usuarios del Instituto.

2. Alcance

Este procedimiento aplica a todos quienes tengan asignada una cuenta de usuario de intranet ya sea en la Sede Central o en las Representaciones.

3. Procedimiento para la creación de cuentas de usuarios de intranet

3. 1. La jefatura de la Unidad interesada en la Sede Central y el Administrador en las Representaciones debe enviar la solicitud de creación de la cuenta de red a GTIC-AD.

3. 2. De acuerdo con los datos suministrados en la solicitud (en la herramienta de *help desk* OTRS), la cuenta de intranet es creada en el *Sistema de administración de usuarios de intranet*, acatando los estándares y políticas utilizadas en la GTIC-AD

3. 3. Se informa al administrador del directorio institucional para que se incluyan los datos del nuevo usuario en los archivos correspondientes.

……..……última página anexo 18……..…..……

Anexo 19. Procedimiento creación cuenta de usuario de sistema de información

TIPO DE DOCUMENTO			
			Público (disponible en el Sitio Web del IICA)
		X	Privado (disponible en la intranet del IICA)
TÍTULO	Procedimiento creación cuenta de usuario de sistema de información		
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central		
FORMATO	Electrónico – Word		
PÁGINAS	2		
REF. APROBACIÓN	SC/DG-405		

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Definir los lineamientos generales para crear una cuenta de usuario para acceder a un sistema de información.

2. Alcance

Este procedimiento aplica a todos quienes tengan asignada una cuenta de usuario de un sistema de información ya sea en la Sede Central o en las Representaciones.

3. Procedimiento para la creación de una cuenta de usuario de un sistema de información

3. 1. La jefatura de la Unidad interesada en la Sede Central y el Administrador en las Representaciones debe enviar la solicitud de creación de la cuenta de red a GTIC-AD.

3. 2. Con base en los datos suministrados, se crea el identificador de usuario y la clave, siguiendo los estándares y lineamientos de la GTIC-AD.

3. 3. Se le asigna al usuario el rol solicitado y se actualiza la matriz de roles correspondiente.

3. 4. En caso de ser necesario se coordina la instalación de la aplicación en la PC del usuario para que éste pueda acceder a la aplicación.

……..…..……última página anexo 17……..…..……

Anexo 20. Procedimiento de borrado de información en equipos que dejaron de ser utilizados por el personal del IICA

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de borrado de información en equipos que dejaron de ser usados por el personal del IICA.
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	2
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Establecer los pasos para la eliminación de la información que de carácter personal o institucional se almacena en una estación de trabajo o equipo portátil propiedad del IICA, cuando se termina la relación laboral o se le asigna al funcionario un nuevo equipo.

2. Alcance

Este procedimiento aplica a todos los usuarios autorizados para utilizar los servicios informáticos administrados por la GTIC-AD y las Representaciones.

3. Procedimiento para el borrado de información en equipos que dejaron de ser utilizados por el personal del IICA

3. 1. La jefatura de la Unidad interesada en la Sede Central y la Administración de la Representación de Costa Rica debe enviar la solicitud a la GTIC-AD solicitando el formateo del equipo usado anteriormente por un funcionario, con lo que se eliminará toda la información de carácter institucional que se almacenaba en ese equipo. En el caso de las otras Representaciones dirige la solicitud de borrado de información del equipo liberado, al encargado de estos asuntos en la Representación.

3. 2. Retirar el equipo liberado, asegurándose de que se realice el traslado de inventario correspondiente.

3. 3. En caso de que el equipo cumpla con los estándares de capacidad definidos por la GTIC-AD, formatear los dispositivos de almacenamiento que posea, instalando una nueva versión del sistema operativo y los programas de trabajo y seguridad estándar del IICA para mantener el equipo en el inventario de reserva para asignación futura. Cuando el equipo no cumple con los estándares se deben eliminar los volúmenes de almacenamiento que posea el equipo, de forma que se elimine toda la información y posteriormente mantener en reserva o desechar el equipo. Misma función corresponde a la Administración en las Representaciones.

……..…..……última página anexo 20……..……

III. ANEXOS: PROCEDIMIENTOS DE GESTIÓN DE TECNOLÓGIAS DE INFORMACIÓN Y COMUNICACIÓN

Anexo 21. Procedimiento para la gestión de activos de tecnología de información

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento para la gestión de activos de tecnología de información
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	3
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Mantener un nivel apropiado de protección de los activos de tecnologías de información de la institución, de acuerdo con su criticidad.

2. Alcance

Este procedimiento aplica a todos los activos de tecnologías de información de la Sede Central y las Representaciones del IICA, considerando como activo de tecnología de información cualquier elemento que tenga valor para la Institución desde el punto de vista tecnológico.

3. Procedimiento para la gestión de activos de tecnología de información

3. 1. Anualmente se debe realizar una revisión al inventario de activos de tecnologías de información. Este inventario debe contemplar al menos:

a. Nombre del activo.
b. Responsable.
c. Custodio técnico.

3. 2. Tipo de activo (información, *software, hardware*, servicios). A continuación, se citan algunos ejemplos por tipo de activo:

a. Información: manuales técnicos, políticas y procedimientos de la Gerencia de Tecnología de Información, Comunicación y Agricultura Digital del IICA.

b. *Software:* licencias de ofimática, licencias de SAP y otras aplicaciones/sistemas institucionales y aplicativos propios.

c. *Hardware:* servidores, *notebooks, desktops*.

d. Servicios: Internet, Intranet, comunicaciones, *websense, active directory, e-courier* y cualquier otro servicio que se incluya en el catálogo de servicios de la GTIC-AD.

3. 3. Los activos de tecnologías de información incluidos en el inventario deben tener un funcionario responsable del mismo.

3. 4. Se deben definir reglas para el uso aceptable de los activos de tecnologías de información, las que deben estar identificadas, documentadas e implantadas, como por ejemplo reglas para el uso de internet, correo electrónico, acceso físico al centro de datos, respaldos, acceso remoto por VPN y adquisición de equipos TI.

3. 5. Los criterios bajo los cuales se clasificarán los activos de tecnologías de información deben estar establecidos.

3. 6. El tratamiento de la información dependerá de la clasificación asignada, considerando su administración, su transmisión y el medio en que reside.

3. 7. La actualización del inventario de activos de tecnología de información y la clasificación de los activos de tecnologías de información se revisará de forma anual, en el mes de junio por parte de la GTIC-AD en la Sede Central y es responsabilidad de la Administración en las Representaciones llevar este control.

3. 8. La salida o baja de los activos de tecnología de información se realizará bajo los siguientes criterios:

a. Los servidores se dan de baja cuando pasado el tiempo de garantía, presentan fallas críticas[5] en el *hardware* o cuando cumplen un período mayor a 5 años (caso de servidores críticos) y son sustituidos de acuerdo con el plan de reposición de equipos.

b. Las impresoras que no se encuentren bajo el sistema de *leasing* se dan de baja una vez que fallan y el arreglo tenga un costo mayor que el valor de reemplazo de la impresora.

c. Las *desktop y laptop* se dan de baja cuando pasado el tiempo de garantía, presentan fallas críticas o irreparables en el *hardware* o en su defecto son sustituidas de acuerdo al plan de reposición de equipos.

d. Los equipos de red se dan de baja cuando pasado el tiempo de garantía, presentan fallas críticas o irreparables o en su defecto son sustituidos de acuerdo con el plan de reposición de equipos.

……..…..……última página anexo 21……..……

[5] Fallas críticas: son fallas en el *hardware* cuyo costo de reparación es mayor o igual al valor del equipo.

Anexo 20. Procedimiento de adquisición de equipos de tecnologías de información y comunicación

TIPO DE DOCUMENTO		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento de adquisición de equipos de tecnologías de información y comunicación
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	3
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Aplicar el mecanismo y los procedimientos adecuados para agilizar y maximizar los recursos institucionales asignados a la adquisición de equipo tecnológico y de comunicación, como *software*, *hardware* u otras herramientas que contribuyan con el desarrollo tecnológico del Instituto.

2. Alcance

Este procedimiento aplica a los funcionarios que entre sus responsabilidades se encuentre la gestión de compras de los equipos tecnológicos en las diferentes unidades del Instituto Interamericano de Cooperación para la Agricultura (IICA).

3. Procedimiento para la adquisición de equipos de tecnologías de información y comunicación

3. 1. Tiene la responsabilidad de planificar la actualización oportuna y la reposición del equipo tecnológico propio de la unidad y del centro de datos para evitar la obsolescencia, mediante la revisión periódica de dichos activos.

3. 2. Debe preparar anualmente un **plan de reposición de los equipos a su cargo**, el cual debe:

a. Asegurar la debida disponibilidad de los equipos y prestación del servicio. Este plan debe estar listo en el mes de octubre de cada año.

b. Establecer los objetivos, planes y tareas específicas, entendidas y aceptadas por la GTIC-AD y la Representación correspondiente, alineada con la planificación estratégica de la institución.

c. Determinar las necesidades y objetivos específicos que se requieren alcanzar, igualmente, se debe determinar si la necesidad que se pretende satisfacer está contemplada en el presupuesto aprobado.

d. Tomar en cuenta los siguientes criterios para el desarrollo del plan de reposición: responsable, producto o entregable, requerimientos de acuerdo con el producto o entregable y justificación.

3. 3. En el caso de la Sede Central, toda reposición de equipo debe estar aprobada por la Jefatura de la Gerencia de Tecnología de Información, Comunicación y Agricultura Digital del IICA y la Gerencia de Programación y Presupuesto (GPP). En el caso de las Representaciones, por el Representante y la GPP.

3. 4. Cada vez que se compren equipos nuevos de red, se deben incluir dentro del plan de mantenimiento preventivo.

3. 5. Los cambios de equipos deben responder al plan de reposición de equipos o cuando los mismos ya no cumplan con la prestación del servicio para el cual brindan apoyo.

3. 6. La adquisición de equipo tecnológico, se deber realizar de acuerdo a los lineamientos establecidos en el Manual de Adquisición de Bienes y Contratación de Servicios.

3. 7. Los servidores más críticos de la unidad deben estar en garantía.

3. 8. La GTIC-AD y la Administración en las Representaciones, realizará una vez al año un estudio de necesidades tecnológicas, en cada una de las Unidades del IICA, con el fin de determinar, orientar y maximizar el proceso de adquisición de equipos tecnológicos en el IICA.

4. Procedimientos generales de las Unidades del IICA

4. 1. La GTIC-AD deberá proveer los requerimientos técnicos para toda compra de equipo tecnológico en el Instituto y por consiguiente deberá contar con el aval técnico de la Gerencia de Tecnología de Información y Comunicación y Agricultura Digital para la adquisición final.

4. 2. Es recomendable que las unidades del IICA sustituyan anualmente el 25% o 30% de sus equipos (PC's), de manera que los equipos siempre se encuentren en garantía. Este aspecto deberá ser considerado en el estudio de necesidades tecnológicas de la Sede Central y las Representaciones.

……..…..……última página anexo 21……..……

Anexo 23. Procedimiento solicitud de sistemas nuevos o cambios en sistemas de información

TIPO DE DOCUMENTO		
		Público (disponible en el Sitio Web del IICA)
	X	Privado (disponible en la intranet del IICA)

TÍTULO	Procedimiento solicitud de sistemas nuevos o cambios en sistemas de información
APLICACIÓN	Todas las Representaciones del IICA y las Unidades de la Sede Central
FORMATO	Electrónico – Word
PÁGINAS	2
REF. APROBACIÓN	SC/DG-405

VERSIÓN	FECHA	AUTOR
1.0	[24.set.2021]	Instituto Interamericano de Cooperación para la Agricultura

1. Objetivo

Informar sobre los lineamientos que deben seguirse para solicitar un nuevo sistema o cambios a un sistema de información existente.

2. Alcance

Unidades del Instituto que requieran el desarrollo o cambios en un sistema de información con recursos del Instituto, tanto financieros como humanos.

3. Procedimiento para el desarrollo o cambios en un sistema de información

3. 1. Estos lineamientos aplican para los sistemas desarrollados con recursos propios y aquellos externos cuyo mantenimiento sea responsabilidad de la GTIC-AD.

3. 2. No aplica para la actualización de programas, producto o desarrollos externos cuya responsabilidad esté a cargo de proveedores externos.

3. 3. El responsable de la Unidad interesada en modificar o desarrollar un nuevo sistema de información debe enviar la solicitud a la GTIC-AD, que analizará la solicitud y definirá si es viable la ejecución de lo solicitado de acuerdo con los lineamientos institucionales y su planificación anual.

3. 4. En caso del desarrollo de un nuevo sistema, el solicitante con el funcionario de la GTIC-AD designado para atender los requerimientos definirán un plan de trabajo.

3. 5. En caso de mantenimiento el funcionario responsable del sistema en GTIC-AD procede a priorizar la solicitud.

3. 6. Aplicará el mismo procedimiento, en el caso de Representaciones que cuenten con esa capacidad instalada.

……..…..……última página anexo 23……..……