



CISIDAT

MANUAL DE SEGURIDAD
INFORMÁTICA DEL CONSORCIO
DE INVESTIGACIÓN SOBRE VIH
SIDA TB CISIDAT, A.C.



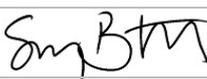
MANUAL DE SEGURIDAD
INFORMÁTICA DEL CONSORCIO
DE INVESTIGACIÓN SOBRE VIH
SIDA TB CISIDAT, A.C.

Código:
CISIDAT - 003
ABRIL - 2020
Hoja: 2 de 11

ÍNDICE

1. INTRODUCCIÓN
2. TÉRMINOS DEFINIDOS
3. LINEAMIENTOS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA
 - 3.1. ASAMBLEA GENERAL
 - 3.1.1. Del buen uso
 - 3.1.1.1. Del internet
 - 3.1.1.2. Del correo electrónico
 - 3.1.2. De las medidas de seguridad
 - 3.1.2.1. Del correo electrónico
 - 3.1.2.2. De las impresoras y escáneres
 - 3.1.2.3. De los servicios en la nube
 - 3.1.2.4. Del servidor
 - 3.1.2.5. Del sitio web

ANEXOS

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020



MANUAL DE SEGURIDAD INFORMÁTICA

INTRODUCCIÓN

El presente documento tiene como propósito dar a conocer los Lineamientos y Estándares de Seguridad Informática realizadas por el Consorcio de Investigación sobre VIH SIDA TB CISIDAT, A.C., para proteger adecuadamente los activos tecnológicos y de información asignados a todo el personal del Consorcio.

El seguimiento del presente manual por parte del personal, permitirá disminuir las amenazas a la seguridad de la información y datos, así como de los recursos informáticos asignados.

TÉRMINOS DEFINIDOS

CISIDAT, al Consorcio de Investigación sobre VIH SIDA TB CISIDAT, A.C.

SOPORTE TÉCNICO DE INFORMÁTICA DE CISIDAT, al rango de servicios de asistencia a usuarios para solución de problemas relacionadas con hardware o software, servicios de internet, periféricos o cualquier otro dispositivo.

SOFTWARE, al conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

HARDWARE, al conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

FIREWALL (CORTAFUEGOS), a la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas

WIFI, a la tecnología de conexión inalámbrica que permite conectar a internet a los equipos de cómputo.

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020



MANUAL DE SEGURIDAD
INFORMÁTICA DEL CONSORCIO
DE INVESTIGACIÓN SOBRE VIH
SIDA TB CISIDAT, A.C.

Código:
CISIDAT - 003
ABRIL - 2020
Hoja: 4 de 11

NAVEGADOR WEB, a la aplicación que permite el acceso a internet, a través de la interpretación de la información de distintos tipos de archivos y sitios web para que estos puedan ser vistos.

CORREO ELECTRÓNICO, al servicio de red que permite a los usuarios enviar y recibir mensajes mediante redes de comunicación electrónica.

ANTIVIRUS, al software que detecta la presencia de un virus informático en una computadora y lo elimina.

MALWARE (SOFTWARE MALICIOSO), a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

PHISING (SUPLANTACIÓN DE IDENTIDAD), al conjunto de técnicas que tienen como propósito, engañar y manipular a una víctima haciéndose pasar por una persona, empresa o servicio de confianza, para que realice acciones que no debería realizar.

LINEAMIENTOS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de CISIDAT, así como el estricto apego al Manual de Seguridad Informática.

1.1. Del buen uso

1.1.1. De los activos tecnológicos

a) Los activos tecnológicos definidos por CISIDAT son:

- Computadora de escritorio
- Servidor
- Impresoras
- Escáneres

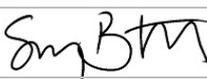
	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLGUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020



MANUAL DE SEGURIDAD
INFORMÁTICA DEL CONSORCIO
DE INVESTIGACIÓN SOBRE VIH
SIDA TB CISIDAT, A.C.

Código:
CISIDAT - 003
ABRIL - 2020
Hoja: 5 de 11

- Sitio web
- b) CISIDAT asignará al personal de cada área los activos informáticos necesarios para el desempeño de sus funciones y éstos serán los únicos responsables de su utilización, así como de la información contenida en cada activo. En caso de préstamo del activo informático, no libera de la responsabilidad al usuario.
- c) Las computadoras de escritorio se encuentran con el hardware y software básicos, necesarios para la función de cada área en CISIDAT:
 - Windows 10 pro.
 - Microsoft Office (Excel, PowerPoints, Word, Outlook).
 - Microsoft Navision
 - Antivirus (Kaspersky)
 - Skype
- d) Toda movilización del activo informático dentro o fuera de las oficinas de CISIDAT, son responsabilidad del usuario que tenga asignado dicho activo.
- e) En caso de algún incidente como daño físico (hardware) o de software, robo o extravío del activo informático, éste deberá ser notificado a la Gerencia Administrativa, que informará las acciones a realizar.
- f) El Soporte Técnico de Informática de CISIDAT, será el único autorizado para realizar actualizaciones, reparaciones o desarmado de los activos informáticos.
- g) El Soporte Técnico de Informática de CISIDAT, será el único autorizado para instalar cualquier tipo de software en las Computadoras de escritorio.
- h) El Soporte Técnico de Informática de CISIDAT, realizará periódicamente actualizaciones de seguridad a todo el software instalado en todas las computadoras de escritorio.
- i) El personal de CISIDAT no podrá cambiar o eliminar las configuraciones del Antivirus ni Firewall definidos por el Soporte Técnico de Informática de CISIDAT, sólo podrán

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020

	MANUAL DE SEGURIDAD INFORMÁTICA DEL CONSORCIO DE INVESTIGACIÓN SOBRE VIH SIDA TB CISIDAT, A.C.	Código: CISIDAT - 003
		ABRIL - 2020
		Hoja: 6 de 11

realizar acciones de escaneo de virus cada que sea solicitado por el Soporte Técnico de Informática de CISIDAT.

1.1.2. Del Internet

- a) En CISIDAT se cuenta con conexión a Internet que deberá utilizarse exclusivamente para las funciones de cada área, utilizándose de manera austera y eficiente.
- b) Para personal de CISIDAT se aginará una red wifi o alámbrica exclusiva y para invitados se asignará una conexión "Guest" cuya contraseña es renovada cada mes por parte del Soporte Técnico de Informática de CISIDAT.
- c) El acceso a páginas web, no se encuentra restringido a ninguna de las áreas de CISIDAT, por lo que el personal deberá:
 - Abstenerse de publicar información relevante de CISIDAT, no importando el formato.
 - Abstenerse de descargar imágenes, videos, música, archivos o instalar software de cualquier tipo, proveniente de sitios web desconocidos o gratuitos.

1.1.3. Del correo electrónico

- a) El correo con extensión @cisidat.org.mx es para uso exclusivo de personal de CISIDAT, la Gerencia Administrativa es la única facultada para solicitar al Soporte Técnico de Informática de CISIDAT la asignación de una cuenta de correo electrónico a nuevos usuarios.
- b) CISIDAT usa la plataforma Gsuite de Google como servicio de correo electrónico, que cumple con estrictos estándares de privacidad y seguridad.

1.2. De las medidas de seguridad

1.2.1. En las computadoras de escritorio:

- a) Todas las computadoras de escritorio deberán tener una contraseña de acceso al sistema que el usuario de cada equipo podrá asignar, sin embargo, el Soporte Técnico de

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020



MANUAL DE SEGURIDAD
INFORMÁTICA DEL CONSORCIO
DE INVESTIGACIÓN SOBRE VIH
SIDA TB CISIDAT, A.C.

Código:
CISIDAT - 003
ABRIL - 2020
Hoja: 7 de 11

Informática de CISIDAT deberá resguardar todas las contraseñas en un lugar bajo llave, como respaldo o para atender acceso a la información en caso de emergencia.

- b) Todas las computadoras de escritorio están conectadas a un disco duro de respaldo en red, siendo el Soporte Técnico de Informática de CISIDAT el único autorizado para realizar cambios o descargar respaldos.
- c) El uso de medios removibles de almacenamiento como memorias USB, discos CD, DVD o Discos duros externos, es responsabilidad de los usuarios asignados a cada computadora de escritorio por lo que el usuario deberá:
 - Escanear con el Antivirus todos los medios removibles de almacenamiento conectados a la computadora de escritorio.
 - No utilizar medios removibles de almacenamiento de los cuales no se conozca el origen o no sea de confianza.
- d) El Soporte Técnico de Informática de CISIDAT es el único autorizado a modificar el Estado y la Lista de aplicaciones permitidas, configuradas en el Firewall de Windows.
- e) Todas las computadoras de escritorio cuentan con un equipo No break para la protección de éstas y su información contenida.

1.2.2. De las Impresoras y Escáneres

- a) Las Impresoras y Escáneres dentro de CISIDAT que se encuentran en red, cuentan con un pin asignado a cada una para evitar mal uso de este activo por parte de usuarios no autorizados.
- b) La Impresión de documentos por parte de Invitados, sólo podrá realizarse enviando el documento que se desea imprimir, a cualquiera del personal de CISIDAT, ya que no existe una impresora para invitados. El personal de CISIDAT deberá seguir lo establecido en el apartado 1.2.3 de este manual.

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020

	MANUAL DE SEGURIDAD INFORMÁTICA DEL CONSORCIO DE INVESTIGACIÓN SOBRE VIH SIDA TB CISIDAT, A.C.	Código: CISIDAT - 003
		ABRIL - 2020
		Hoja: 8 de 11

1.2.3. Del correo electrónico

- a) Se recomienda a todos los usuarios con cuenta de correo electrónico de CISIDAT, incluir en su firma programada el Aviso de confidencialidad (Anexo 1) en español e inglés.
- b) Todos los usuarios de un correo electrónico de CISIDAT, deberán asignar una contraseña de al menos ocho caracteres en las que deberán incluir: mayúsculas, minúsculas, símbolos y números. Sólo el usuario de cada cuenta conocerá esta contraseña, sin embargo, en caso de emergencia o si se detectara mal uso de la cuenta de correo, la Gerencia Administrativa podrá solicitar al Soporte Técnico de Informática de CISIDAT, la revocación y asignación de una nueva contraseña para el correo electrónico en cuestión, sin previo aviso ni autorización por parte del usuario.
- c) Los usuarios de una cuenta de correo electrónico de CISIDAT que agreguen su cuenta a un dispositivo móvil, deberán tener activada una contraseña o pin de seguridad en dicho dispositivo, de otro modo, Gsuite no permite la autenticación del correo electrónico en dicho dispositivo.
- d) Todos los correos electrónicos recibidos son responsabilidad de los usuarios, por lo que se recomienda tomar las siguientes acciones para evitar ser víctima de Phising:
 - Revisar atentamente los remitentes de cada correo electrónico y sólo abrir aquellos de remitentes confiables o cuyo contenido en el tema del correo tenga sentido de acuerdo a las funciones de CISIDAT.
 - Antes de descargar un archivo adjunto, es necesario que cada usuario permita que el antivirus de Gmail (si se utiliza el navegador web) o el Antivirus (si se utiliza Outlook) escanee el archivo.
 - Antes de dar clic a un enlace, posicionarse sobre el texto del enlace y revisarlo.

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020

	MANUAL DE SEGURIDAD INFORMÁTICA DEL CONSORCIO DE INVESTIGACIÓN SOBRE VIH SIDA TB CISIDAT, A.C.	Código: CISIDAT - 003
		ABRIL - 2020
		Hoja: 9 de 11

- No enviar ninguna información de carácter personal o profesional si no es parte de una solicitud formal por parte de la Gerencia Administrativa de CISIDAT.

1.2.4. De los servicios en la nube

- Todos los proyectos de CISIDAT cuentan con servicio Drive de Gsuite, por lo que se recomienda utilizar este servicio a través del servicio de Discos compartidos (Shared drives) que el Soporte Técnico de Informática de CISIDAT puede asignar a cada proyecto.
- En caso de utilizar un servicio distinto, deberá informarse a la Gerencia Administrativa y al Soporte Técnico de Informática de CISIDAT, el usuario y contraseña de dicho servicio, sin excepción.

1.2.5. Del servidor

- El servidor de CISIDAT, contiene el software COI y Microsoft Navision necesarios para los procesos administrativos y contables de CISIDAT, el Soporte Técnico de Informática de CISIDAT es el único autorizado para ingresar a dicho servidor.
- El servidor cuenta con Antivirus que es actualizado periódicamente por parte de Soporte Técnico de Informática de CISIDAT, así como un disco duro de respaldo automático.

1.2.6. Del sitio web

- El sitio web de CISIDAT (<https://www.cisidat.org.mx/>) no contiene ni almacena datos o información sensible de CISIDAT o de terceros.
- El servicio de hospedaje se subcontrata a la empresa SiteGround (<https://www.siteground.com/>), el Soporte Técnico de Informática de CISIDAT es el único autorizado para ponerse en contacto con el proveedor de hospedaje.

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020



MANUAL DE SEGURIDAD
INFORMÁTICA DEL CONSORCIO
DE INVESTIGACIÓN SOBRE VIH
SIDA TB CISIDAT, A.C.

Código:
CISIDAT - 003

ABRIL - 2020

Hoja: 10 de 11

- c) Los cambios al contenido del sitio web de CISIDAT, sólo podrán ser autorizados por la Gerencia Administrativa y el Soporte Técnico de Informática de CISIDAT es el único autorizado para realizar dichos cambios, así como actualizaciones y mantenimiento.

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020

	MANUAL DE SEGURIDAD INFORMÁTICA DEL CONSORCIO DE INVESTIGACIÓN SOBRE VIH SIDA TB CISIDAT, A.C.	Código: CISIDAT - 003
		ABRIL - 2020
		Hoja: 11 de 11

Anexos

Aviso de confidencialidad para correos electrónicos de CISIDAT

AVISO DE CONFIDENCIALIDAD: Este correo electrónico, incluyendo en su caso, los archivos adjuntos al mismo, pueden contener información de carácter confidencial y/o privilegiada y se envían a la atención única y exclusiva de la persona y/o entidad a quien va dirigido. La copia, revisión, uso, revelación y/o distribución de dicha información confidencial sin la autorización por escrito del Consorcio de Investigación sobre VIH SIDA TB CISIDAT, A.C., está prohibida. Si usted no es el destinatario a quien se dirige el presente correo, favor de contactar al remitente respondiendo al presente correo y eliminar el correo original incluyendo en su caso, los archivos adjuntos. Mediante la recepción del presente correo usted reconoce y acepta que en caso de incumplimiento de su parte y/o de sus representantes a los términos antes mencionados, Consorcio de Investigación sobre VIH SIDA TB CISIDAT, A.C., tendrá derecho a los daños y perjuicios que esto le cause.

NOTICE OF CONFIDENTIALITY: The contents of this e-mail message and any attachments are intended solely for the addressee(s) and may have confidential and/or privileged information. It is prohibited by Consorcio de Investigación sobre VIH SIDA TB CISIDAT, A.C., any copy, revision, usage, to revile and/or distribute confidential information. If you are not an intended recipient, please notify the sender by replying this message and delete this message and its attachments, if any. By the reception of this email, you agree and accept terms and conditions above, and in case of non-fulfillment from you and your partners, Consorcio de Investigación sobre VIH SIDA TB CISIDAT, A.C., has the right to act against damages caused by this situation.

	Revisó:	Autorizó:	Autorizó:
Nombre	MBA. ALEJANDRA OLCUÍN	DRA. LETICIA PÉREZ SALEME	MTRO. SERGIO BAUTISTA
Firma			
Fecha	Abril 2020	Abril 2020	Abril 2020