1. OBJETIVO

Establecer medidas de control y vigilancia con el fin de garantizar la seguridad, confidencialidad y buen manejo de las tecnologías de información (Equipos de cómputo, sistemas de información y redes), dirigida a todos los usuarios de cómputo de la fundación de lucha contra el cáncer Unicancer.

2. ALCANCE

Estas políticas son aplicables a todos los empleados, contratistas, voluntariado, consultores, estudiantes en formación y otros empleados de las empresas en convenio, incluyendo a todo el personal externo que soliciten que sus equipos sean conectados a la Red de dominio de UNICANCER, esta política es también aplicable a los entes externos que de alguna manera tengan que utilizar local o remotamente el uso de la red o recursos tecnológicos como VPN de La fundación así como de los servicios e intercambio de información digital.

3. DEFINICIONES

- **ATI:** Administradores de Tecnología de Información, responsables de la administración de los equipos de cómputo, sistemas de información y redes de la empresa. Vela por todo lo relacionado con la utilización de equipos de cómputo, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

- **POLÍTICA:** son instrucciones mandatorias que indican la intención de la alta dirección respecto a la operación de la institución.

- **RECURSO INFORMÁTICO:** Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

- **INFORMACIÓN:** Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

- **USUARIOS TERCEROS:** Todas aquellas personas naturales o jurídicas, que no son funcionarios de la Fundación, pero que por las actividades que realizan en la institución, deban tener acceso a recursos informáticos.

- **ATAQUE CIBERNÉTICO:** Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

- **BRECHA DE SEGURIDAD:** Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

- **HARDWARE:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

- **SOFTWARE:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

- **VPN:** En ingles Virtual Private Network o red privada virtual (RPV), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

- **WAN:** es la sigla de Wide Área Network ("red de área amplia"). El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial. Un ejemplo de red WAN es la propia Internet.

- **LAN:** son las siglas de Local Area Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios). Las redes LAN se pueden conectar entre ellas a través de líneas telefónicas y ondas de radio.

- **MALWARE:** es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

- **PHISHING:** es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.
- **SPAM:** Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

- **FIREWALL:** Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

4. CONDICIONES GENERALES

La coordinación de sistemas está integrada por el ATI -Coordinadora Administrativa y T.I de soporte, los cuales son responsables de:

- La administración de la red de dominio de unicancer iniciando con la planeación topológica, y el monitoreo de las redes WAN y LAN.
- El uso del internet, directorio activo, servidores y equipos activos de red, velando por la conectividad de los servicios y usuarios del dominio.
- La instalación, adecuación, monitorización, ampliación, operación y actualización de las redes de cómputo de unicancer para agilizar los procesos administrativos y misionales de la entidad.
- El soporte y mantenimiento de la plataforma tecnológica, administración de bases de datos, correo en hosting y dominio unicancercali.com y demás servicios asociados a este.
- Velar por el funcionamiento y seguridad de la tecnología informática que se utilice en las diferentes áreas con el fin de evitar ataques cibernéticos o brechas de seguridad.

- Realizar el mantenimiento a los equipos de cómputo y todos los recursos informáticos manteniendo su inventario actualizado.
- Velar por el cumplimiento de las Políticas de Seguridad y Procedimientos establecidos.
- Realizar la copia de seguridad o backup de la información de la empresa que reposa en el servidor.
- Administrar y configurar la solución de antivirus ESET endpoint security con que cuenta la fundación.
- Solucionar contingencias presentadas ante el surgimiento de virus que la solución no se haya detectado automáticamente.
- Desarrollar, someter a revisión y divulgar (intranet, email, sitio web oficial) las Políticas de Seguridad.

5. DESCRIPCIÓN DE LAS POLITICAS

5.1 ACCESO A LA INFORMACIÓN

Todos los empleados que laboran para la Fundación Unión de Lucha contra el Cáncer UNICANCER deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. Para que un empleado tenga acceso a otros servicios y recursos informáticos, se requiere autorización por parte del ATI o Gerencia mediante solicitud previa hecha por correo electrónico describiendo detalladamente el perfil de la solicitud.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la institución, con el objeto de minimizar el riesgo de pérdida o fuga de esta.
Ningún empleado podrá extraer, difundir o compartir información exclusiva de la fundación sin previo aviso, solicitud por escrito o correo electrónico a la Gerencia o ATI.

Para que un funcionario externo o contratista tenga acceso a los servicios y recursos informáticos dispuestos por la fundación (Incluido uso de Wifi), se requiere que el jefe inmediato o coordinador solicite al grupo de sistemas ATI mediante correo electrónico, la activación de dichos servicios con el perfil requerido y las restricciones de algunos servicios.

El grupo ATI exigirá en los equipos a conectar, incluidos teléfonos inteligentes en la red el uso de una solución legal de antivirus.

Los contratistas, voluntarios, consultores, estudiantes en formación y otros empleados de las empresas en convenio que hayan recibido aprobación para tener acceso a Internet a través de las estaciones de trabajo institucionales o computadoras portátiles personales, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet implantadas por el grupo ATI y Gerencia.

5.2 SEGURIDAD DE LA INFORMACIÓN

Todos los empleados, contratistas, voluntariado, consultores, estudiantes en formación y otros empleados de las empresas en convenio que utilicen los equipos de cómputo y los servicios informáticos disponibles, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información

que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Después de que un empleado o estudiante en formación deja de prestar sus servicios a la Fundación, éste se debe comprometer a entregar toda la información respectiva de su trabajo, realizando entrega al coordinador o jefe inmediato según sea el caso, quien avala e informa al ATI sobre lo recibido para elaborar el paz y salvo del funcionario retirado.

Una vez retirado el empleado o estudiante deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, así mismo, los empleados de la fundación que detecten el mal uso de la información están en la obligación de reportar el hecho al grupo de sistemas ATI. Para esto todo el personal de la fundación se debe tener firmado el acuerdo de confidencialidad.

Es de carácter obligatorio para todo el personal (Fijo, y/o Contratado), la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse por escrito vía correo electrónico a La Gerencia y/o al grupo ATI, quienes están en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente.

5.3 ADMINISTRACIÓN DE HARDWARE Y SOFTWARE

- Todo cambio en el hardware o software que afecte los recursos informáticos, debe ser requerido por los usuarios responsables de la información y aprobado por el grupo ATI de sistemas, con el visto bueno y supervisión del jefe inmediato.
- Bajo ninguna circunstancia ningún empleado podrá modificar o instalar hardware o software sin previo consentimiento del ATI o Gerencia.
- Para la administración de cambios en hardware y software se efectuará el procedimiento correspondiente definido por unicancer, de acuerdo con el tipo de cambio solicitado en los recursos tecnológicos.
- Cualquier tipo de cambio en el recurso tecnológico debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos en la fundación.

5.4 USO DEL WIFI

La Fundación de Lucha Contra el Cáncer- Unicancer restringirá el servicio de Internet en la red de comunicaciones WIFI a los dispositivos inalámbricos diferentes de de la Fundación y que no cuentan con soluciones propias legales de antivirus, tales como tabletas, celulares inteligentes, Smart tv (Televisores inteligentes), bafles con wifi y smartwatch (Relojes Inteligentes) Con el fin de minimizar el riesgo a la integridad de la información como son brechas de seguridad y ataques cibernéticos a la seguridad de los sistemas de información institucionales.

Unicancer utilizará mecanismos de bloqueo y firewall para controlar el acceso de una computadora o dispositivos inteligentes como celulares a la red, por motivos de seguridad.

5.5 DISPOSITIVOS DE ENTRADA Y SALIDA

- Ningún empleado, contratista, voluntario, consultor, estudiante en formación y otros empleados en convenio con la Fundación, podrá usar memorias USB en los equipos, salvo las memorias de la misma que solo comparten información de forma interna.
- La Fundación de Lucha Lontra el Cáncer -Unicancer no permitirá modificar o manipular la configuración de las impresoras en red o periférico con que cuenta la fundación.
- La Fundación de Lucha Contra el Cáncer-Unicancer - no permite conectar celulares inteligentes a los equipos de cómputo y más aún cuando no poseen soluciones legales de antivirus.

5.6 SEGURIDAD DE LOS SERVICIOS INFORMÁTICOS Y CORREO CORPORATIVO.

El sistema de correo electrónico y servicios informáticos prestados por la Fundación Unión de lucha contra el cáncer Unicancer deben ser usados única y exclusivamente para el ejercicio de las funciones de competencia de cada empleado. la Fundación se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico corporativo para cualquier propósito y para lo cual podrá realizar las revisiones y/o auditorias respectivas directamente o a través del grupo ATI y Gerencia.

La propiedad intelectual desarrollada o concebida mientras el empleado se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Fundación de lucha contra el cáncer unicancer. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, investigaciones pagadas por la fundación, estudios ambientales y de otros propósitos, programas de computación, códigos fuentes, documentación y otros materiales.

En cualquier momento que un empleado publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la Fundación.

Unicancer no permite el uso de correos personales dentro de la red de dominio, esta se debe limitar única y exclusivamente al uso de correos institucionales o corporativos, salvo en casos excepcionales se deberá realizar solicitud escrita mediante correo al grupo ATI o Gerencia exponiendo los motivos para su uso.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente comunicarse con el grupo ATI de sistemas y no utilizar su equipo, desconectándolo inmediatamente de la red.

5.7 SOFTWARE UTILIZADO

Todo software que utilice la Fundación Unión de Lucha Contra el Cáncer Unicancer será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Fundación o reglamentos internos.

Debe existir una cultura tecnológica al interior de la Fundación que garantice el conocimiento por parte de los empleados de las implicaciones que tiene el instalar software ilegal en las computadoras de la Fundación.

La administración y control del software la ejecutará el grupo ATI con el fin de evitar posibles sanciones por instalación de software no licenciado.

5.8 COPIAS DE RESPALDO O BACKUP

La información que es soportada por la infraestructura de tecnología de la Fundación Unión de Lucha Contra el Cáncer Unicancer, es almacenada y respaldada en cintas y disco externos de acuerdo con las normas emitidas de tal forma que se garantiza su disponibilidad y custodia.

La Gerencia y Grupo de Contabilidad será directamente responsable de la copia externa que se genera por parte del grupo ATI esto de acuerdo con la importancia de la información para la operación de la institución.

5.9 SEGURIDAD FISICA

La Fundación Unión de Lucha Contra el Cáncer- Unicancer- deberá contar con los mecanismos de control de acceso al cuarto de telecomunicaciones e informática, tales como planilla de control y supervisión por parte del grupo ATI o un empleado designado para este fin durante su permanencia en este cuarto, dejando registrado por escrito el motivo de ingreso y labor a realizar.

La Fundación Unión de lucha Contra el Cáncer –Unicancer- cuenta con medios tecnológicos como son unidades digitales, discos duros y memorias USB las cuales deben ser registradas en planilla por quien solicite su uso.

Todas las computadoras portátiles, computadoras de escritorio y equipos de comunicación deben registrar su salida e ingreso y no deben abandonar la Fundación a menos que esté acompañado por la autorización respectiva por parte del ATI y la validación de supervisión del vigilante de turno. En caso de requerir el equipo para realizar trabajos por fuera de la Fundación, estos deberán estar avalados por la Direccion Ejecutiva, cumpliendo con los mismos requisitos de salida.

Los equipos de cómputo (Computadoras de escritorio, servidores y equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa por parte del ATI.

Las UPS y estabilizadores de energía no deben ser utilizadas para conectar equipos eléctricos diferentes a su equipo de cómputo (CPU, monitor, equipo Portátil scanner o impresoras),. No se permite el uso de estos elementos para la carga de celulares, grabadoras, electrodomésticos, fotocopiadoras, parlantes, secadores de cabello, aires acondicionados, ventiladores, taladros, cámaras fotográficas, de video y en general cualquier equipo que genere caídas de energía.

Unicancer no permite a los usuarios introducir e ingerir alimentos y/o bebidas, cerca o en el área de los computadores o cuarto de telecomunicaciones e informática. Si desea tener en su escritorio alguna bebida deberá hacerlo en un termo debidamente cerrado. En caso de un derrame de bebida o alimentos, el usuario deberá asumir en su totalidad la reparación y/o sustitución del equipo.

5.10 ADMINISTRACION DE SEGURIDAD EN INTERNET E INTRANET

- La Navegación y uso de internet estará regulado por el ATI con el fin de evitar y minimizar el riesgo a la integridad de la información como son virus informáticos, spam, malware, phishing, ramsoware, brechas de seguridad y ataques cibernéticos a la seguridad de los sistemas de información institucionales, restringiendo el uso de páginas con contenidos pornográficos y maliciosos, redes sociales, youtube, chat de whatsapp para pc, juegos, compras en línea, arte, humor, televisión y películas entre otras.

- Cualquier brecha de seguridad o sospecha en la mala utilización en la Internet, la red corporativa o Intranet, los servicios y recursos informáticos de cualquier nivel (local o institucional) deberá ser

comunicada por el funcionario que la detecta, en forma inmediata y confidencial al grupo de sistemas ATI.

- El Grupo de sistemas ATI divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a la Direccion Ejecutiva, los casos de incumplimiento con copia a los coordinadores de área.

5.11 RESPONSABILIDADES PERSONALES

- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña (especialmente aplicado al uso del programa GCI) a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- Cuando el usuario deba retirarse por algún motivo, deberá cerrar la sesión del aplicativo de GCI con el fin de evitar que este sea utilizado por otro usuario.
- Los usuarios no deben utilizar ningún acceso autorizado a las carpetas compartidas (exclusivo de los jefes de área) de otro usuario, aunque dispongan de la autorización del propietario.
- Si un usuario tiene sospechas de que su acceso autorizado (carpeta compartida en servidor de dominio) está siendo utilizado por otra persona, debe proceder a informar a su jefe inmediato y éste reportar al grupo ATI.
- Los usuarios sólo podrán crear ficheros o carpetas que contengan datos de carácter personal y para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales deberán ser ubicados en unidades locales de disco del equipo de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

5.12 ANTIVIRUS

Todos los equipos de cómputo de La Fundación deberán tener instalada una solución antivirus, como requisito para adherirse al dominio de red unicancer. La Fundación en este momento cuenta con la Licencia de antivirus eset endpoint security, el cual se renueva anualmente.

Periódicamente se hará el rastreo en los equipos de cómputo de La fundación, y se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

Unicancer no permite la manipulación, configuración, desinstalación o reemplazo de la solución de antivirus contratada por la Fundación ya que estas deben estar debidamente licenciadas.

6. ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, Unicancer se reserva el derecho a modificar estas políticas cuando sea necesario. Los cambios realizados serán divulgados a todos los usuarios de La fundación.

Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de la Política de Seguridad más reciente.

Las normas y políticas objeto de este documento podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo entre la Dirección Ejecutiva y el grupo ATI; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

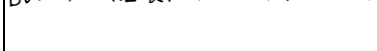
La falta de conocimiento de las normas aquí descritas por parte de los usuarios no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.

7. HISTÓRICO DE CAMBIOS

VERSION	FECHA DE EDICIÓN	DESCRIPCION DEL CAMBIO
01	2017-06-02	Creación del documento.
02	2018-08-28	Actualización del documento.

8. FIRMAS

ELABORÓ	REVISÓ	APROBÓ
Nombre: Zoraida Herrera **Cargo:** Coordinadora Administrativa. **Firma:**  **Fecha:** 2018-09-21	**Nombre:** Jennifer León **Cargo:** Coordinador de Calidad. **Firma:**  **Fecha:** 2018-09-26	**Nombre:** Diana Robayo. **Cargo:** Directora Ejecutiva. **Firma:**  **Fecha:** 2018-09-28