PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR

ICULTUR

2020 - 2023

Contenido

1. OBJETIVOS

Establecer un Plan de Seguridad y Privacidad de la Información que apoye la construcción e implementación en un futuro de un Modelo de Seguridad y Privacidad de la Información, acorde a los lineamientos de la política de gobierno digital, el cual será impulsado por los miembros del comités de gestión y desempeño institucional del ICULTUR, El presente documento tiene como finalidad dar a conocer las Política de Seguridad Informática del ICULTUR que deberán observar los administradores de servicios de tecnologías de información y usuarios, para proteger adecuadamente los activos tecnológicos y la información resguardada en el Centro de Cómputo del Instituto de cultura y Turismo de Bolivar y en cada una de las Estaciones de Trabajo con el objetivo de asegurar su disponibilidad y mitigar los riesgos en caso de desastres.

2. DISPOSICIONES GENERALES

2.1. Definiciones

i. Oficina de Sistemas y Tecnologías OTS

La Oficina de Sistemas y Tecnologías del ICULTUR es responsable de proveer y mantener la infraestructura de Tecnología y ha desarrollado las siguientes Políticas de Seguridad Informática que, a su vez, son un conjunto de normas enmarcadas en el ámbito jurídico y administrativo del ICULTUR. Estas normas inciden en la adquisición y el uso de los bienes y servicios informáticos, las cuales se deberán acatar por aquellas instancias que intervengan directa o indirectamente en ello.

ii. ABD

Administrador de Base de Datos.

iii. ATI

Administradores de Tecnología de Información de OTS. Responsables de la administración de los equipos de cómputo, sistemas de información y redes del ICULTUR. 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.

El Área de Tecnología de OTS actualmente está conformado por 3 funcionarios los cuales tienen a su cargo distintas funciones referentes a el soporte y mantenimiento de la plataforma tecnológica, soporte de sistemas de información, administración de bases de datos, gestión de recursos de tecnología y administración de redes; dado a esta razón ha sido necesario emitir políticas particulares para el conjunto de recursos y facilidades

informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos, provistos por OTS.

La Administración de Tecnología de OTS está integrada por la Gerencia de Tecnología, el Jefe de Soluciones IT y el Jefe de Infraestructura, los cuales son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes áreas.
- Definir estrategias y objetivos a corto, mediano y largo plazo.
- Mantener la arquitectura tecnológica.
- Controlar la calidad del servicio brindado.
- Mantener el Inventario actualizado de los recursos informáticos.
- Velar por el cumplimiento de las Políticas y Procedimientos establecidos.
- Desarrollar, someter a revisión y divulgar (intranet, email, sitio web oficial) las Políticas de Seguridad.

iv. Centro de Comunicaciones:

Cualquier oficina dentro de los inmuebles del ICULTUR que cuenten con equipamiento de cómputo, telecomunicaciones o servidores.

v. Comité

Equipo integrado por La Gerencia, el Gestor de Seguridad, los Jefes de área y el personal administrativo del ICULTUR (ocasionalmente) convocados para fines específicos como:

- Adquisiciones de Hardware y software.
- Establecimiento de estándares de Las Empresas tanto de hardware como de software.
- Establecimiento de la Arquitectura tecnológica de grupo.
- Capacitar a los empleados en lo relacionado con las Políticas de Seguridad.

vi. Contraseña

Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

vii. DataCenter (Centro de Datos)

Oficina con equipos de cómputo, telecomunicaciones y servidores que prestan servicios con las características físicas y ambientales adecuadas para que los equipos alojados funcionen sin problema.

viii. Dirección

Representante de nivel superior del ICULTUR que a su vez integra el comité de seguridad. Bajo su administración están la aceptación y seguimiento de las Políticas de Seguridad.

ix. Gestor de Seguridad

Persona dotada de conocimientos técnicos, encargada de velar por la seguridad de la información, realizar auditorías de seguridad, elaborar documentos de seguridad como, políticas, normas; y de llevar un estricto control con la ayuda de los ATI referente a los servicios prestados y niveles de seguridad aceptados para tales servicios. Este rol es asumido por la Gerencia de Tecnología de OTS.

x. Red

Equipos de cómputo, sistemas de información y redes de telemática del ICULTUR.

xi. Responsable de Activos

Personal del área administrativa del ICULTUR, que velará por la seguridad y correcto funcionamiento de los activos informáticos, así como de la información procesada en éstos, dentro de sus respectivas

áreas. Esta persona debe mantener el inventario físico al día, velar por que todos los activos tengan sus respectivas pólizas de seguros bajo los parámetros entregados por La Dirección.

xii. Solución Antivirus

Recurso informático empleado para solucionar problemas causados por virus informáticos.

xiii. Usuario

Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por el ICULTUR tales como equipos de cómputo, sistemas de información, redes de telemática.

xiv. Virus informático

Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

2.2. Alcance

Este manual de políticas de seguridad es elaborado de acuerdo con el análisis de riesgos y de vulnerabilidades en las dependencias del ICULTUR, por consiguiente, el alcance de estas políticas se encuentra sujeto al ICULTUR.

Este plan que además contiene la política de seguridad y privacidad es aplicable a todos los empleados, contratistas, consultores, eventuales y otros empleados del ICULTUR, incluyendo a todo el personal externo que cuenten con un equipo conectado a la Red. Esta política es aplicable también a todo el equipo y servicios propietarios o arrendados que de alguna manera tengan que utilizar local o remotamente el uso de la Red o recursos tecnológicos del ICULTUR, así como de los servicios e intercambio de archivos y programas.

La elaboración de las Políticas de Seguridad está fundamentadas bajo la norma ISO/IEC 27001, han sido planteadas, analizadas y revisadas con el fin de no contravenir con las garantías básicas de los usuarios, y no pretende ser una camisa de fuerza, y más bien muestra una buena forma de operar los sistemas con seguridad, respetando en todo momento, estatutos y reglamentos internos del ICULTUR.

- Control de acceso (aplicaciones, base de datos, área del Centro de Cómputo, sedes o dependientes del ICULTUR).
- Resguardo de la Información.
- Clasificación y control de activos.
- Gestión de las redes.
- Gestión de la continuidad del negocio.
- Seguridad de la Información en los puestos de trabajo.
- Controles de Cambios.
- Protección contra intrusión en software en los sistemas de información.
- Monitoreo de la seguridad.
- Identificación y autenticación.

- Utilización de recursos de seguridad.
- Comunicaciones.
- Privacidad.

2.3. Objetivos

Dotar de la información necesaria a los usuarios, empleados y director, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la Red, así como la información que es procesada y almacenada en estos.

Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos del ICULTUR.

Los objetivos que se desean alcanzar luego de implantar el plan de seguridad y privacidad de la información son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de los ATI en la administración del riesgo.
- Compromiso de todo el personal del ICULTUR con el proceso de seguridad, agilizando la aplicación de los controles.
- Que la prestación del servicio de seguridad gane en calidad.
- Todos los empleados se convierten en interventores del sistema de seguridad.

2.4. Vigencia

Todas estas amenazas están en continuo proceso de expansión, lo que, unido al progresivo aumento de los sistemas de información y dependencia del negocio, hace que todos los sistemas y aplicaciones estén expuestos a riesgos cada vez mayores, que, sin una adecuada gestión de los mismos, pueden ocasionar que su vulnerabilidad se incremente y consiguientemente los activos se vean afectados. Todo empleado es responsable del cumplimiento de los estándares, directrices y procedimientos de control de acceso, así como también notificar a su nivel jerárquico superior, cuando por algún motivo no pueda cumplir con las Políticas de Seguridad indicando el motivo por el cual no le es posible apegarse a la normativa de seguridad. Cabe destacar que este nivel de responsabilidad va a ser conocido por las diferentes áreas del ICULTUR quienes serán las garantes de que esta información sea conocida por cada integrante de área.

La documentación presentada como Políticas de Seguridad entrará en vigencia desde el momento en que sean aprobadas por la Dirección. Esta normativa deberá ser revisada y actualizada conforme a las exigencias del ICULTUR o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

2.5. Notificaciones de violaciones de seguridad

Es de carácter obligatorio para todo el personal (Fijo, 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 Dirección y/o a los ATI y/o a la Jefatura de Control Interno, 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.

Es responsabilidad de todo empleado que maneje datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, puesto que estas descansan en el establecimiento de responsabilidades donde se incurra en alguna violación en materia de seguridad acarreando sanciones a quien las haya causado, puesto que esto ocasionaría perjuicios económicos a Las Empresas de diversa consideración. Es por ello que las personas relacionadas de cualquier forma con los procesos tecnológicos deben ser conscientes y asumir que la seguridad es asunto de todos y, por tanto, se debe conocer y respetar las Políticas de Seguridad.

Está fundamentado como una exigencia que el personal de la organización conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación o falta, escrita en las Políticas de Seguridad firmado por el empleado o proveedor o cualquier entidad dependiente del Instituto. Por esta razón se entenderá que sólo una adecuada política de seguridad tecnológica apoyará la concientización para obtener la colaboración de los empleados, haciéndoles conscientes de los riesgos que podemos correr y de la importancia del cumplimiento de las normas.

2.6. Lineamientos para la adquisición de bienes informáticos

Toda adquisición de tecnología informática se efectuará a través del Comité. Los ATI, al planear las operaciones relativas a la adquisición de bienes informáticos, establecerán prioridades y en su selección deberá tomar en cuenta:

2.6.1. Precio

Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.

2.6.2. Calidad

Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

2.6.3. Experiencia

Presencia en el mercado, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

2.6.4. Desarrollo Tecnológico

Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

2.6.5. Estándares

Toda adquisición se basa en los estándares, es decir la arquitectura de grupo empresarial establecida por el Comité. Esta arquitectura tiene una permanencia mínima de dos a cinco años.

2.6.6. Capacidades

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área. Para la adquisición de Hardware se tendrá en cuenta lo siguiente:

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares del ICULTUR.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
- Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por el Comité.
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local. Tratándose de microcomputadores, a fin de mantener actualizada la arquitectura informática del ICULTUR, el Comité emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.
- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y en el ICULTUR, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
- Los equipos adquiridos deben contar con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos al vencer su período de garantía.
- En lo que se refiere a los computadores personales, al vencer su garantía por adquisición, deberán de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de repuestos.
- Todo proyecto de adquisición de bienes de tecnología debe sujetarse al análisis, aprobación y autorización del Comité.

2.6.7. Alcances y Requerimientos Legales

Se deberá cumplir con todos los parámetros, requisitos y trámites legales vigentes a la fecha de cada proceso, garantizando los principios de transparencia y eficiencia.

2.6.8. Software

En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente.

Para la adquisición de Software base y utilitarios, el Comité dará a conocer periódicamente las tendencias con tecnología de punta vigente, siendo la principal lista de productos autorizados la siguiente:

2.6.8.1. Sistemas Operativos

- Microsoft Windows
- Mac OS-X

2.6.8.2. Bases de Datos

- Microsoft SQL Server
- MySQL / MariaDB

2.6.8.3. Lenguajes y herramientas de programación

- Microsoft .NET
- PHP / Apache
- Dreamweaver
- Fireworks

2.6.8.4. Utilitarios de oficina

- Microsoft Office
- Oppen Office
- iWork

2.6.8.5. Programas antivirus

- Kaspersky Internet Security

2.6.8.6. Correo electrónico

- Microsoft Outlook
- Web Mail

2.6.8.7. Navegadores de Internet

- Internet Explorer
- Mozilla Firefox
- Google Chrome

2.6.8.8. Diseño

- Adobe Creative Suite
- Cinema 4D

2.7. Licenciamiento

- Todos los productos de Software que se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.
- El área de Tecnología promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

2.8. Bases de datos

Para la operación del software de red en caso de manejar los datos institucionales mediante sistemas de información, se deberá tener en consideración lo siguiente:

- Toda la información del ICULTUR deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.
- El acceso a los sistemas de información deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información del ICULTUR. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
- Los datos de los sistemas de información deben ser respaldados de acuerdo con la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los CDs, DVDs, Blue Ray de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo (Google Drive) o en medios de almacenamiento alternos.
- Todos los sistemas de información que se tengan en operación deben contar con sus respectivos manuales actualizados. Un técnico que describa la estructura interna del sistema, así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema y los procedimientos para su utilización.
- Los sistemas de información deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoria y Control).
- Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.
-

2.9. Frecuencia de evaluación de las políticas.

Se evaluarán las políticas del presente documento, con una frecuencia anual por el Comité

Las políticas serán evaluadas por los ATI con una frecuencia semestral.

3.POLITICAS DE SEGURIDAD FISICA

3.1. Acceso Físico

El ICULTUR destinará un área que servirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y servidores.

Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso al edificio y a las oficinas del ICULTUR.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de tecnología o con permiso de los ATI.

Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el superior responsable o los ATI, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del Área Administrativa del ICULTUR y al personal de seguridad del edificio.

3.2. Protección Física

3.2.1. Data Center

El DataCenter deberá:

- Tener una puerta de acceso de vidrio templado transparente o malla en acero, para favorecer el control del uso de los recursos de cómputo.
- Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por los encargados de Tecnología.
- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado
- Aire acondicionado. Mantener la temperatura a 21 grados centígrados.
- Asignar un técnico para que realice un control diario temperatura y aires acondicionados y llevar un registro de estos controles.
- Respaldo de energía redundante.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Contar con algún esquema que asegure la continuidad del servicio.
- Control de humedad
- Prevención y/o detección de incendios
- Sistemas de extinción en caso de ser posible.
- Contar por lo menos con dos extintores de incendio adecuado y cercano al DataCenter.

3.2.2. Infraestructura

Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

El resguardo de los equipos de cómputo deberá quedar bajo el área de Tecnología contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

3.3. Instalaciones de equipos de cómputo

La instalación del equipo de cómputo quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- El Área de Tecnología, así como las áreas operativas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
- La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

3.4. Control

- Los ATI deben llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.
- Los encargados del área de tecnología son los responsables de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.
- El Área de Recursos Humanos de OTS deberá reportar a los ATI cuando un usuario deje de laborar o de tener una relación con Las Empresas con el fin de retirarle las credenciales de ingreso a los recursos y supervisar la correcta devolución de los equipos y recursos asignados al usuario.
- El usuario, en caso de retiro, deberá tramitar ante el Área de Tecnología el paz y salvo correspondiente.

3.5. Respaldos

- Las Bases de Datos del ICULTUR serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro (Cloud) que permita tener contingencia y continuidad de negocio.
- Los servidores de contingencia de Bases de Datos y aplicaciones estarán alojados en un Operador Externo o por lo menos contar con Máquinas Virtuales en topología Activo-Pasivo dispuestas para operar.
- Los servidores de hosting estarán alojados en Bluehost.
- Los demás respaldos (una copia completa) deberán ser almacenados en un lugar seguro y distante del sitio de trabajo, en bodegas con los estándares de calidad para almacenamiento de medios magnéticos.
- La empresa prestadora para estos fines será SYNC.
- Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio; y en las unidades de almacenamiento asignadas por el ICULTUR en “La Nube” (SYNC), deberá realizar una sincronización continua de la información importante.
- Los respaldos serán responsabilidad absoluta de los usuarios.
- Los ATI no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

3.6. Recursos de los usuarios

3.6.1. Uso

- Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y Red del ICULTUR, de acuerdo con las políticas que en este documento se mencionan.
- Los usuarios deberán solicitar apoyo al área de Tecnología ante cualquier duda en el manejo de los recursos de cómputo del ICULTUR.
- El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno al ICULTUR, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera).

3.6.2. Derechos de Autor

Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los usuarios deberán firmar un documento donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor.

Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores del ICULTUR bajo ninguna circunstancia sin la autorización escrita de la Dirección o de los Encargados de Tecnología de OTS.

- No está permitido instalar ningún programa en su computadora sin dicha autorización o la clara verificación de que La Empresa posee una licencia que cubre dicha instalación.
- No está autorizada la descarga de Internet de programas informáticos no autorizados por La Dirección o los Encargados de Tecnología de OTS.
- No se tolerará que un empleado realice copias no autorizadas de programas informáticos.
- No se tolerará que un empleado cargue o descargue programas informáticos no autorizados de Internet, incluidos entre otros la descarga de programas informáticos para utilizar sistemas de peer-to-peer (P2P – Ej. Kazaa) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.
- No se tolerará un empleado realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.
- Si se descubre que un empleado ha copiado programas informáticos o música en forma ilegal, este puede ser sancionado, suspendido o despedido.
- Si se descubre que un empleado ha copiado programas informáticos en forma ilegal para dárselos a un tercero, también puede ser sancionado, suspendido o despedido.
- Si un usuario desea utilizar programas informáticos autorizados por Las Empresas en su hogar, debe consultar con los ATI para asegurarse de que ese uso esté permitido por la licencia del editor.
- El personal encargado de soporte de Tecnología revisará las computadoras constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si Las Empresas poseen licencias para cada una de las copias de los programas informáticos instalados.
- Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.
- El ICULTUR autoriza el uso de programas informáticos de diversas empresas externas. Las Empresas no son dueñas de estos programas informáticos o la documentación vinculada con ellos y, a menos que cuente con la autorización del creador de los programas informáticos, no tiene derecho a reproducirlos excepto con fines de respaldo.
- Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.
- Los usuarios no descargarán ni cargarán programas informáticos no autorizados a través de Internet.
- Los usuarios no realizarán intercambios o descargas de archivos digitales de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.
- Los usuarios que se enteren de cualquier uso inadecuado que se haga en la Entidad de los programas informáticos o la documentación vinculada a estos, deberán notificar a la Dirección o Director del área en la que trabajan o al asesor legal del ICULTUR.

- Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.
- Los empleados o contratistas que realicen adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo a las circunstancias. Dichas sanciones pueden incluir suspensiones y despidos justificados.

4. POLITICAS DE SEGURIDAD LOGICA

4.1. Red

- Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro del ICULTUR entre usuarios, departamentos, oficinas y hacia afuera a través de conexiones con otras redes.
- El Área de Tecnología no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.
- No se permite el uso de los servicios de la red cuando no cumplan con las labores propias del ICULTUR.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad del ICULTUR y se usarán exclusivamente para actividades relacionadas con la labor asignada.
- Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
- El uso de analizadores de red es permitido única y exclusivamente por los ATI para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las Políticas de Seguridad.
- No se permitirá el uso de analizadores para monitorear o censar redes ajenas al ICULTUR y no se deberán realizar análisis de la Red desde equipos externos a la entidad.
- Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

4.2. Servidores

4.2.1. Configuración e instalación

- Los ATI tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.
- La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de los ATI.
- Durante la configuración de los servidores los ATI deben genera las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.
- Los servidores que proporcionen servicios a través de la red e Internet deberán:
  - Funcionar 24 horas del día los 365 días del año.

- Recibir mantenimiento preventivo mínimo dos veces al año
- Recibir mantenimiento semestral que incluya depuración de logs.
- Recibir mantenimiento anual que incluya la revisión de su configuración.
- Ser monitoreados por los ATI.

- La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:
  - Diariamente, información crítica.
  - Semanalmente, los documentos web.
  - Mensualmente, configuración del servidor y logs.

- Los servicios hacia Internet sólo podrán proveerse a través de los servidores autorizados por los ATI.

4.2.2. Correo Electrónico

- Los ATI se encargarán de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
- Para efecto de asignarle su cuenta de correo al usuario, el área de Recursos Humanos deberá llenar una solicitud en formato establecido para tal fin y entregarlo al área de Tecnología, con su firma y la del Director del área.
- La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres.

4.2.3. Bases de Datos

- El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.
- El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso.
- Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.
- En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

4.3. Recursos de Cómputo

4.3.1. Seguridad de cómputo

- Los ATI son los encargados de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.
- Los ATI deben mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.
- Los ATI son los únicos autorizados para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

4.3.2. Ingenieros de Soporte

Los Ingenieros de Soporte tendrán las siguientes atribuciones y/o responsabilidades:

- Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.
- Deberán utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.
- Deberán realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.
- Deben actualizar la información de los recursos de cómputo del ICULTUR, cada vez que adquiera e instale equipos o software.
- Deben registrar cada máquina en el inventario de control de equipos de cómputo y red del ICULTUR.
- Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
- Reportar a la Dirección los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

4.3.3. Renovación de equipos

- Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.
- Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al área de Tecnología a fin de que se seleccione el equipo adecuado. Sin el visto bueno de Tecnología no podrá liberarse una orden de compra.

4.4. Uso de Servicios de Red

4.4.1. Dirección y Sedes

- La Dirección definirá los servicios de Internet a ofrecer a los usuarios y se coordinará con los ATI para su otorgamiento y configuración.
- La Dirección puede utilizar la infraestructura de la Red para proveer servicios a los usuarios externos y/o visitas previa autorización los ATI.
- Los ATI son los responsables de la administración de contraseñas y deberán guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.
- No se darán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en el ICULTUR, excepto por orden expresa de La Dirección.
- Los ATI realizarán las siguientes actividades en los servidores del ICULTUR.
- Respaldo de información conforme a los procedimientos establecidos.
- Revisión de logs y reporte de cualquier eventualidad.
- Implementar de forma inmediata las recomendaciones de seguridad y reportar posibles faltas a las políticas de seguridad en cómputo.
- Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
- Organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.
- Los ATI son los únicos autorizado para asignar las cuentas a los usuarios.
- Los ATI podrán aislar cualquier servidor de red, notificando a las Direcciones y áreas de la entidad, en las condiciones siguientes:
    - Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.
    - Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
    - Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
    - Si se detectan accesos no autorizados que comprometan la integridad de la información.
    - Si se viola las políticas de uso de los servidores.
    - Si se reporta un tráfico adicional que comprometa a la red del ICULTUR.

4.4.2. Usuarios

4.4.2.1. Identificación de Usuarios y contraseñas

- Todos los usuarios con acceso a un sistema de información o a la Red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Ningún usuario recibirá un identificador de acceso a la Red, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.
- El usuario deberá definir su contraseña de acuerdo con el procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recurso que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por La Gerencia.

- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud de los ATI, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:
  - Cuando ésta sea una contraseña débil o de fácil acceso.
  - Cuando crea que ha sido violada la contraseña de alguna manera.
- El usuario deberá notificar a los ATI en los siguientes casos:
  - Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
  - Si tiene problemas en el acceso a los servicios proporcionados por el servidor.
- Si un usuario viola las políticas de uso de los servidores, los ATI podrán cancelar totalmente su cuenta de acceso a los servidores, notificando a La Gerencia correspondiente.

4.4.2.2. 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 a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.
- El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.
- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.
- En caso de que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.
- Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.
- Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.
- Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.
- Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

- Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán 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.

4.4.2.3. Uso Apropiado de los Recursos

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

4.4.2.3.1. Queda Prohibido

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios del ICULTUR.
- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

4.5. Antivirus

4.5.1. Antivirus de la Red

- Todos los equipos de cómputo del ICULTUR deberán tener instalada una solución Antivirus.
- Periódicamente se hará el rastreo en los equipos de cómputo del ICULTUR, 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.

4.5.2. Responsabilidad de los ATI

Los ATI serán responsables de:

- Implementar la Solución Antivirus en las computadoras del ICULTUR.
- Solucionar contingencias presentadas ante el surgimiento de virus que la solución no se haya detectado automáticamente.
- Configurar el analizador de red para la detección de virus.
- Los ATI aislarán el equipo o red, notificando a la Dirección correspondiente, en las condiciones siguientes:
  - Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación del virus a otros equipos y redes.
  - Si el usuario viola las políticas antivirus.
  - Cada vez que los usuarios requieran hacer uso de discos, USB's, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de cómputo de las dependencias.
- En caso de contingencia con virus los ATI deberán seguir el procedimiento establecido.

La solución corporativa de seguridad de antivirus es Kaspersky Internet Security (KIS), Esta solución integra herramientas Antivirus, antispyware, firewall y prevención contra intrusiones, además de control de dispositivos y aplicaciones usando un único agente multiplataforma (Windows, Mac, Linux) para todos los clientes y gestionado mediante una consola central con motor de base de datos Microsoft SQL.

Complementando el servicio antivirus se implementará el servicio LiveUpdate Administrator (LUA), como repositorio central de actualización para toda la plataforma antivirus, facilitando la gestión de descarga y distribución actualizaciones permitiendo que todos los equipos del ICULTUR tengan las últimas versiones y parches emitidos por el fabricante.

4.5.3. Cobertura

Con KIS se da cobertura a los siguientes sistemas operativos:

4.5.3.1. Clientes

- Microsoft: Windows XP / VISTA / 7/8/10 en versiones 32 y 64 bits.
- Apple: Mac OS X 10.4 / 10.5 / 10.6 / 10.7 / 10.8

4.5.3.2. Servidores

- Microsoft: Windows 2008 Standard /Enterprise Edition, Windows 2012 R2 / Standard / Enterprise Edition en distribution 32 y 64 Bits.
- Apple: Mac OS X Server 10.7 64 Bits

Para simplificar la instalación del agente KIS, se pondrá a disposición del equipo de soporte los agentes de instalación clasificados como "Desktop, Portátiles y Servers" en versiones:

- Windows: Instalador interactivo y Silencioso en versiones 32 y 64 bits.
- Mac OS X (instalador único válido para Mac OSX 10.5 o superior)

Y un instalador especifico “Mac 104” el cual corresponde al paquete de instalación KIS última versión disponible y Agente para conexión a consola KIS.

4.5.4. Políticas Antivirus

Todos los equipos de cómputo conectados a la red corporativa deben tener instalado y debidamente actualizado KIS, con el fin de que esto sea cumplido, cualquier proceso interno de asignación y/o rotación de equipos de cómputo le corresponde una lista de chequeo para su alistamiento, lista dentro de la cual se encuentra debidamente registrado la instalación y/o validación de KIS. La desinstalación de KIS se encuentra restringida a la validación de clave de desinstalación, la cual se encuentra a disposición únicamente del equipo de soporte interno.

Utilizando la consola de administración de KIS se implementan las siguientes políticas:

4.5.4.1. Virus y Spyware

SERVICIO	PROGRAMACION	
	Desktop / Laptops	**Servidores**
Escaneo	Periodicidad: Semanal Tipo: Completo Dia y Hora: Jueves 12:00 M	Periodicidad: Diaria Tipo: Completo Dia y Hora: L-D 12:00 AM
Actualizaciones	Cada Ocho (8) Horas	Cada Cuatro (4) Horas

4.5.4.2. Autoprotect

DESCRIPCION	ACCIONES		
	TIPO DETECCION	**PRIMERA**	**SEGUNDA**
Revisión Automática de todos los archivos, Riegos de Seguridad, Equipos remotos cuando se ejecutan archivos.	Malware/Virus	Limpiar	Borrar
	Riesgos de Seguridad	Sugerir	Cuarentena

4.5.4.3. Descargas

DESCRIPCION	ACCIONES		
	TIPO DETECCION	**PRIMERA**	**SEGUNDA**
Análisis de Riegos potenciales basados en reputación con nivel de sensibilidad intermedia, que permite tener un numero bajo de falsos positivos sin comprometer el desempeño de los computadores	Archivos maliciosos	Borrar	Cuarentena
	No Probados	Sugerir	N/A

4.5.4.4. Sonar

DESCRIPCION	ACCIONES		
	TIPO DETECCION	**PRIMERA**	**SEGUNDA**
Inspector de Pquetes y Tráfico de Red de Kaspersky	Eventos de cambio: DNS, HOST FILE	Log	Log
	Comportamiento Sospechoso	Bloqueo	N/A

4.5.4.5. Autoprotect Mail

SERVICIO	DESCRIPCION	ACCIONES		
		TIPO DETECCIÓN	**PRIMERA**	**SEGUNDA**
INTERNET EMAIL	Scan de todos los archivos y hasta tres niveles de compresión	Malware/Antivirus	Limpiar	Borrar
		Riegos	de seguridad:	Borrar
MICROSOFT OUTLOOK	Se encuentran activadas estas opciones por no usar ninguna plataforma de correo orientado a la nube (Google Apps, Office 360, entre otros). Nuestro Servicio es un servicio Web basado en Web Mail con sus propias políticas de seguridad y control. Adicionalmente servicios de correo basados en POP e IMAP se encuentra restringidos en LAN			
LOTUS NOTES				

4.5.4.6. Firewall

- Desactiva el firewall de Windows y establece políticas de reglas centralizadas.
- Reglas preestablecidas en la instalación y que son recomendación de buenas prácticas por Kaspersky. Servicios como DHCP, DNS y WINS son controlados por tráfico desde la herramienta.

4.5.4.7. Intrusion Prevention

Detecta y bloquea automáticamente ataques de red y a navegadores de internet, debe permanecer activada globalmente.

4.5.5. Control de Aplicaciones y Dispositivos

- Conjunto de reglas que permiten controlar acceso de aplicaciones y/o dispositivos a los recursos del sistema, con el fin de prevenir riesgos de infección y/o seguridad; no se bloqueará el acceso a dispositivos como CD/DVD-ROM, USB o discos externos.
- Bloqueo a ejecución de aplicaciones desde CD-ROM/DVD-ROM y dispositivos de almacenamiento removibles incluyendo Autorun.inf.

4.5.6. Uso del Antivirus por los usuarios

- El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
- Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.
- El usuario deberá comunicarse con los ATI en caso de problemas de virus para buscar la solución.
- El usuario será notificado por los ATI en los siguientes casos:
  - Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.
  - Cuando sus archivos resulten con daños irreparables por causa de virus.
  - Cuando viole las políticas antivirus.

5. SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Los ATI implementarán soluciones lógicas y físicas que garanticen la protección de la información de las compañías de posibles ataques internos o externos.

- Rechazar conexiones a servicios comprometidos
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

5.1. Firewall

- La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.
- Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
- Los ATI establecerán las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- El firewall debe bloquear las “conexiones extrañas” y no dejarlas pasar para que no causen problemas.
- El firewall debe controlar los ataques de “Denegación de Servicio” y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
- Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

5.2. Sistemas de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un computador/servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

Los ATI implementarán soluciones lógicas y físicas que impidan el acceso no autorizado a los equipos del ICULTUR:

- Detección de ataques en el momento que están ocurriendo o poco después.
- Automatización de la búsqueda de nuevos patrones de ataque, con herramientas estadísticas de búsqueda y al análisis de tráfico anómalo.
- Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.
- Auditoría de configuraciones y vulnerabilidades de los sistemas de IDS.
- Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.
- Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto.
- Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos.
- La Red del ICULTUR sólo podrá acceder a los parámetros que el Firewall tenga permitido o posibilite mediante su configuración.

5.3. Redes Privadas Virtuales (VPN)

- Los usuarios móviles y remotos del ICULTUR podrán tener acceso al a red interna privada cuando se encuentren fuera de La Empresa alrededor del mundo en cualquier ubicación con acceso al Internet público, utilizando las redes privadas VPN IPSec habilitadas por el Área de Tecnología.
- Los ATI serán los encargados de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.

5.4. Conectividad a Internet

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores del ICULTUR tienen las mismas responsabilidades en cuanto al uso de Internet.
- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
- No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.
- Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

- Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

5.5. Red Inalámbrica (WIFI)

5.5.1. Acceso a funcionarios del ICULTUR:

- La red inalámbrica (ICULTUR-AP0X) es un servicio que permite conectarse a la red Las Empresas e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura del ICULTUR.
- Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
- Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Ipod, celulares, etc.) con capacidad de conexión Wireless.
- Los ATI, son los encargados de la administración, habilitación y/o bajas de usuarios en la red inalámbrica del ICULTUR.

5.5.1.1. Identificación y activación

- Para hacer uso de la red inalámbrica ICULTUR-AP0X, el solicitante necesariamente deberá ser miembro como Empleado o Contratista del ICULTUR.
- Como primer paso para hacer uso de este servicio, se deben de registrar los usuarios que deseen la prestación del servicio mediante el llenado de un formulario y presentando el dispositivo que se conectará a la red inalámbrica.
- Se debe registrar la dirección MAC de las tarjetas inalámbricas de todos y cada uno de los dispositivos de comunicación.
- La activación de la cuenta se realizará por un periodo semestral como máximo; salvo casos de fuerza mayor o anormalidades en el registro (usuarios inexistentes, apagones, fallas, etc.).
- Para conectarse a la red inalámbrica se deberá emplear autenticación tipo WPA2- AUTO-PSK para lo cual los nombres de usuarios y contraseñas cambiarán periódicamente (de 6 a 12 meses) con la finalidad de proporcionarles seguridad en el acceso a los usuarios.

5.5.1.2. Seguridad

- A pesar de que se han establecido sistemas de encriptación de datos mediante el uso de seguridad WPA2-AUTO-PSK, NO SE RECOMIENDA hacer uso de tarjetas de crédito para compras.
- Los ATI determinarán las medidas pertinentes de seguridad para usar las redes inalámbricas.
- Los ATI se reservan el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red.
- No se deben realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de ingreso no autorizado es una práctica ilegal y será.

- No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.
- Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar a los ATI para su respectiva baja del equipo de la red inalámbrica.

5.5.1.3. Tecnología

- La red inalámbrica del ICULTUR usa el estándar 802.11b/g/n con cifrado WPA2. Por lo tanto las tarjetas de red inalámbrica deben poseer la certificación Wi-Fi™ de este estándar y soportar los requerimientos descritos. Caso contrario se debe realizar algunas actualizaciones previas de tratarse de un computador portátil.
- A pesar de que se usan amplificadores de señal, la cobertura queda sujeta a diversos factores, por lo que NO SE GARANTIZA en ninguna forma el acceso desde cualquier punto fuera de cobertura del ICULTUR.
- Sólo será soportado el protocolo TCP/IPV.4 en la red inalámbrica.
- El área de Tecnología se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios del ICULTUR.
- No se permiten la operación ni instalación de “puntos de acceso” (access points) conectados a la red cableada del ICULTUR sin la debida autorización por parte los ATI.
- No se permite configurar las tarjetas inalámbricas como “puntos de acceso” o la configuración de equipos como servidores adicionales.

5.5.1.4. Restricciones/prohibiciones de acceso a Internet

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

- El uso de programas para compartir archivos (Peer to Peer).
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- El uso de sitios de videos en línea o en tiempo real.
- Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
- Uso de JUEGOS "on line" en la red.

5.5.1.5. Excepciones

- Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.
- En caso de eventos, cursos, talleres, conferencias, etc, se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.
- En el caso de estos eventos las restricciones para acceder podrán ser “anuladas” temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.

5.5.2. Acceso a Invitados

- La red inalámbrica (ICULTUR Invitado) es un servicio que permite conectarse única y exclusivamente a personal externo del ICULTUR (clientes, proveedores) a internet sin la necesidad de algún tipo de cableado. La Red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura del ICULTUR.
- Los usuarios invitados no tendrán acceso a la Red del ICULTUR ni a ningún recurso de uso privado del ICULTUR.
- La red inalámbrica es de tipo Portal Cautivo y cada Recepción tendrá una lista de voucher con contraseñas que se actualizarán cada dos meses.

6. PLAN DE CONTINGENCIA INFORMATICA

Los ATI crearán para los departamentos un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

7. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, La entidad se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los usuarios del ICULTUR.

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

8. DISPOSICIONES

- Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.
- Las normas y políticas objeto de este documento podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo del Comité; 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.

Elaborado por:	Revisado por:	Aprobado por:
Natacha Gonzalez **Direccion Financiera** **27/01/2022**	**Iván Sanes Pérez** **Director General** **xx/xx/xxxx**	**Comité Institucional de Gestión y Desempeño** **xx/xx/xxxx**