INJUPEMP
SOLIDEZ • FUTURO • PROTECCIÓN

POLÍTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

SEPTIEMBRE, 2013

INDICE

I. INTRODUCCIÓN

La información y los recursos informáticos son activos importantes y vitales del INJUPEMP, por lo que las máximas autoridades y todos los empleados en cualquier nivel jerárquico, tienen el deber de custodiarlos, preservarlos, utilizarlos y mejorarlos. Esto implica que se deben tomar las acciones pertinentes para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos contra muchas clases de amenazas y riesgos, por lo que deben adoptarse y aplicarse medidas de seguridad, sin importar los medios en los cuales la información se genera y/o guarde: (en papel o en forma electrónica); como se procesa (computadoras personales, servidores, correo de voz, etc.) y cómo se transmite (en físico, correo electrónico, conversación telefónica, chat corporativo, etc.).

Cualquier imprudencia, violación o incumplimiento en materia de seguridad puede ocasionar al INSTITUTO perjuicios de diversa índole y consideración. Es por ello que los Usuarios deben estar conscientes que la seguridad es asunto de todos y por tanto, debe conocer y respetar las políticas que el INSTITUTO adopte en esta materia.

II. OBJETIVOS

OBJETIVO GENERAL: Definir las Políticas de Seguridad de las Tecnologías de la Información y las Comunicaciones en el INJUPEMP, las cuales son el fundamento para obtener un control efectivo sobre la información, su resguardo y las actividades de los funcionarios y empleados del Instituto que son realizadas a través de operaciones de cómputo o del uso de equipos y recursos informáticos, proveyendo la información necesaria que permita a todos los funcionarios, ejecutivos, empleados, participantes, beneficiarios del sistema y otros actores asociados al instituto, crear una "**Cultura de Seguridad y Control de la Información**", para que tomen conciencia de la necesidad imperativa de proteger la Información, el Hardware, el Software y las redes de datos y comunicaciones del INJUPEMP.

OBJETIVOS ESPECIFICOS

- Consolidación de la seguridad como tema estratégico y concientización global sobre la importancia de la seguridad de la información.
- Planeamiento y manejo de la seguridad más efectivos.
- Mayor seguridad en el ambiente informático, minimizar los riesgos inherentes a la seguridad de la información y generar una mejor y oportuna reacción a incidentes de seguridad.
- Orden en el trabajo bajo un marco normativo que evita la duplicidad de tareas y facilita el intercambio de información.
- Incremento de la cooperación entre las Unidades Organizacionales, por ser la seguridad el interés común.
- Mayor facilidad para la toma de decisiones.
- Mejora de la imagen institucional.

- Mayor control de la información recibida y/o proporcionada a terceros y aumento de la confianza de los mismos.

III. ALCANCE

Las presentes Políticas de Seguridad**,** son aplicables a la administración de:

LA INFORMACIÓN: **D**atos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, usb, etc.).

EL SOFTWARE: **C**onjunto de Sistemas Operacionales, programas, productos y aplicaciones que utiliza el INSTITUTO**.**

EL HARDWARE: **C**onjunto de equipos de cómputo, telecomunicaciones y redes que utiliza el INSTITUTO.

IV. DEFINICIONES

Para los efectos de la aplicación de las presentes disposiciones y bajo la perspectiva de la tecnología de información, deberán considerarse las siguientes definiciones:

Archivos: Conjunto de datos o instrucciones que se almacenan en el Disco Duro y/o cualquier otro medio de almacenamiento con un nombre que los identifica. Ejemplo: PLANILLAS.xlsx, donde PLANILLAS es el nombre y xlsx es la extensión del archivo.

Aplicaciones de Software: Es el conjunto de instrucciones mediante las cuales el Hardware puede realizar las tareas ordenadas por el usuario. Está integrado por los programas, sistemas operativos y utilidades.

Autorización: Proceso o procedimiento oficial del INJUPEMP por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información.

CPU: (Unidad Central de Proceso): Es una parte del Hardware o equipo de cómputo que realiza el procesamiento de datos.

Contraseña: Password o clave para obtener acceso a un programa o partes de un programa determinado, una terminal u ordenador personal (computadora portátil o de escritorio), un punto en la red (fijo o inalámbrico), etc.

Contraseña Robusta: Password o clave que cumplen con las condiciones específicas de acuerdo a la normativa internacional para la seguridad de la información.

Cuenta de Usuario: Es el identificador único que utiliza un Sistema de Información en la autenticación de los usuarios autorizados.

Correo Corporativo: Servicio en línea que provee un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico por medio de Internet a través del dominio corporativo del INJUPEMP (@injupemp.gob.hn)

Cuenta de Correo Corporativo: Asignación única para un usuario del correo corporativo.

Encriptado: Cifrado o codificación de la información sensible que puede ser recibida o enviada desde o para los sistemas de información del Injupemp.

Disco duro: Medio utilizado para el almacenamiento de información. Cuando se almacena información en un disco, ésta se conserva incluso después de apagar el computador y se encuentra guardada de forma permanente en el interior del Hardware.

Disponibilidad: Característica relacionada con la facilidad y oportunidad de acceso a la información cuando sea requerida por los procesos del INSTITUTO para realizar sus negocios ahora y en el futuro.

Disquetes, CD-ROM, DVD, USB: Medios utilizados para el almacenamiento de información, que puede introducirse y retirarse del drive del Hardware o de los puertos de comunicación de la computadora.

Equipos de cómputo: Son los dispositivos eléctricos, electrónicos y mecánicos que se emplean para procesar o consultar, transmitir, almacenar datos. (Hardware)

Hacker: Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo. Popularmente se le conoce como piratas informáticos a aquellos hackers que realizan acciones malignas con sus conocimientos.

Hardware: Partes físicas de un sistema de procesamiento de datos, por ejemplo, la CPU, el monitor, la impresora, teclado, ratón, módems, teléfonos, enrutador, switches, etc.

Incidente: Es todo evento que surge a raíz de una definición inadecuada del alcance de un producto, mala práctica en el sistema, operación o una violación a las Políticas de Seguridad de la Información y que conlleva a una falla en la operatividad normal dentro del INJUPEMP.

Información: conjunto de datos sobre un suceso o fenómeno en particular que al ser ordenados en un contexto sirven para disminuir la incertidumbre y aumentar el conocimiento sobre

un tema específico**.** Es todo lo que puede ser expresado a través de un lenguaje y es utilizada por el INSTITUTO durante el desarrollo de sus operaciones.

Información Sensible: Información que por su naturaleza debe mantenerse bajo estrictas medidas de seguridad que garanticen el acceso sólo al personal autorizado y para un propósito previamente definido.

Información Interna: Es aquella información de uso interno que utilizan los empleados del INJUPEMP con el propósito de realizar las operaciones normales del INSTITUTO. Son ejemplos de información interna: los registros o datos obtenidos o generados de los participantes.

Información Pública: Todo archivo, registro, dato o comunicación contenida en cualquier medio, documento, registro impreso, óptico o electrónico u otro que no haya sido clasificado como reservado y que está disponible para la distribución pública por medio de los canales autorizados, en congruencia con las disposiciones que establece la Ley de Transparencia y Acceso a la Información Pública.

Integridad: Es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados, así como su validez de acuerdo con los requerimientos del INSTITUTO.

Log o Bitácora: Archivo que registra movimientos y actividades de un determinado programa, utilizado como mecanismo de control y estadística.

Monitor: (pantalla): Permite visualizar electrónicamente la salida de datos de un computador.

Parche de Seguridad: Conjunto de instrucciones de corrección para un software en especial, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento, en el Código original de este.

Periféricos: Corresponde a cualquier dispositivo o equipo, tales como: impresoras, unidad ininterrumpida de poder (UPS), unidades de cinta, estabilizadores y reguladores de voltaje, mouse (ratón óptico o manual) teclado, unidades de CD y de DVD, teléfonos, enrutadores, switches, antenas de comunicación, controles de acceso, toquen, cámaras, grabadoras de video, parlantes, monitor, escáner, equipos biométricos, etc.

Programas (software): Conjunto de instrucciones que permiten manejar una tarea en procesamiento electrónico de datos, por ejemplo: office, módulo financiero, módulo de planillas, registro de afiliación, correo corporativo, chat corporativo, etc.

Protector de pantalla: Imagen o diseño móvil que aparece en la pantalla cuando transcurre un determinado período de tiempo durante el que no se mueve el ratón (Mouse) o se presiona una tecla. Los protectores de pantalla evitan que la pantalla resulte dañada como consecuencia de la presentación de áreas oscuras y luminosas en la misma posición durante largo tiempo.

Recursos informáticos: Software, hardware y redes que posee y/o utiliza el INJUPEMP.

Riesgo de la Información: Es una combinación de la posibilidad de que una amenaza contra un activo de información ocurra aprovechando una vulnerabilidad y/o falla en un control interno, y la severidad del impacto adverso resultante.

Sistema: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso, generados para cubrir una necesidad u objetivo.

Sistemas Operativos: Es un programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación ejecutándose en modo privilegiado respecto de los restantes.

Software ilegal: Es el Software que se adquiere y se instala sin el consentimiento de la persona o empresa que lo desarrolla (propietario). Es también llamado Software Pirata, en donde su fabricante no obtiene ninguna contraprestación económica por su uso y sus derechos de autoría intelectual son violados. También se considera ilegal todo el software que no ha sido autorizado por la autoridad competente para ser utilizado en el equipo y/o las instalaciones del INJUPEMP aun cuando el usuario haya comprado una licencia de uso del mismo.

Terceros: Personas que no son empleados del INJUPEMP o empresas diferentes al mismo. Ejemplo: Participantes, beneficiarios, proveedores regulares o potenciales de bienes y servicios, empresas candidatas a prestar servicios al Instituto, entes reguladores, consultores, etc.

Vulnerabilidad: Debilidad de un sistema, que da posibilidad de realizar alguna acción que afecte negativamente a éste.

V. NORMATIVA APLICABLE RELACIONADA

Las presentes Políticas de Seguridad están enmarcadas en la Ley del INJUPEMP y demás disposiciones vigentes que le son aplicables, tales como:

i. Resolución No.1301/22-11-2005 "**Normas Para Regular La Administración de las Tecnologías de Información y Comunicaciones en las Instituciones del Sistema Financiero"** emitida por la Comisión Nacional de Bancos y Seguros.
ii. Ley de Transparencia y Acceso a la Información Pública
iii. Código De Comercio; Artículo 956.
iv. Ley Del Sistema Financiero; Articulo 34.-
v. Normas contables, contraloras, nacionales e internacionales vigentes en lo que aplique a los sistemas de información, Ejemplo: NIIF, NICS, Resoluciones de la CNBS, BCH, SEFIN, ONADICI, TSC, etc.
vi. Normas Generales de Control Interno emitidas por el TSC y ONADICI

Otros Documentos Relacionados

a. Manual de Administración de Usuarios Perfiles/ Aplicaciones
   - ✓ UTI-Ps001 Uso de Carpetas Compartidas
   - ✓ UTI -Ps002 Instalación de Software Legal No Oficial de INJUPEMP
   - ✓ UTI -Ps003 Codificación de Activos, Mobiliario y Equipo
   - ✓ UTI -Ps004 Uso de Equipo Electrónico Propiedad de Empleados o Externos
   - ✓ UTI -Ps005 Creación de Accesos a Programas Adicionales
   - ✓ UTI -Ps006 Eliminación de Software Legal No Oficial de INJUPEMP
   - ✓ UTI -Ps007 Formato de Vigencia de Uso de Máquina

b. Manual de operaciones del centro de datos

VI. RESPONSABLES

Las presentes Normas y Políticas de Seguridad de la Información son aplicables a todas las áreas, departamentos, secciones o entidades de INJUPEMP y son de cumplimiento obligatorio por parte de todos los funcionarios y empleados del Instituto en cualquier nivel jerárquico, sean temporales o permanentes, definidos como los usuarios y administradores de la información y equipos informáticos, así como por otros usuarios que utilicen de una u otra forma los sistemas de información o las redes tecnológicas del INJUPEMP.

En ese contexto, existen distintos niveles de responsabilidad en el manejo y uso de la información:

ADMINISTRADOR DE SISTEMAS: Es el responsable técnicamente de la administración, disponibilidad, seguridad y operación de un determinado sistema de información, en función de su responsabilidad institucional.

CUSTODIOS: Se denomina así a las personas o áreas que proporcionan servicios, sin que necesariamente conozcan la información que custodian, solamente la procesan, gestionan su almacenamiento y la hacen accesible.

DUEÑO: Es generalmente el titular del área funcional de un sistema específico en particular, con la potestad para definir el alcance, la operatividad y las limitantes del mismo y de autorizar el acceso a la información.

USUARIO: Es aquella persona, empleada del INSTITUTO, que crea, lee, introduce, cambia o actualiza la información almacenada en los Sistemas Informáticos de acuerdo con los privilegios que le son asignados. Para adquirir un perfil de usuario es necesaria la justificación y autorización por escrito previa del Dueño de la información o de la autoridad competente.

El incumplimiento de las presentes Políticas de Seguridad dará lugar a la aplicación de las sanciones laborales establecidas de conformidad al Código de Trabajo, el Reglamento Interno de Trabajo del INJUPEMP y demás disposiciones internas relacionadas, sin perjuicio de las acciones civiles o penales que, en su caso, puedan resultar aplicables.

VII POLITICAS DE SEGURIDAD

A. ADMINISTRADOR DE SEGURIDAD INFORMÁTICA.

Con el propósito de homogenizar y centralizar todo lo relativo a la seguridad de la información, el instituto deberá contar con la plaza de **Administrador de Seguridad Informática**, quien será nombrado por la Junta Directiva y estará subordinado al Director Ejecutivo, comprendiendo entre sus responsabilidades las siguientes:

i. Promover y gestionar la implementación de una cultura de seguridad de la información por parte de todos los empleados del Instituto.

ii. Documentar y proponer ante el Director Ejecutivo las políticas, normas y procedimientos de seguridad de la información para su aprobación y presentación ante la Junta Directiva cuando corresponda y velar por su implementación y cumplimiento.

iii. Dirigir las investigaciones y auditorias sobre incidentes y problemas relacionados con la seguridad de la información, así como recomendar las medidas de control pertinentes.

iv. Promover e implementar la continuidad del negocio y recuperación de desastres

v. Velar por la protección de la propiedad intelectual

vi. Proponer y gestionar la implementación de medidas de prevención del fraude electrónico

B. POLÍTICAS DE SEGURIDAD DE APLICACIÓN GENERAL

1. **DE LOS USUARIOS**.

Los Usuarios son responsables de cumplir con todas las políticas del INJUPEMP relativas a la Seguridad de la Información y las telecomunicaciones, y en particular de:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la Información, Hardware y Software del INJUPEMP.
- No divulgar por cualquier medio, información confidencial del INJUPEMP a personas no autorizadas.
- Responder por todas y cada una de las transacciones efectuadas en el software con su usuario y contraseña asignada.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros usuarios en forma inadvertida.
- No compartir o revelar su contraseña a otras personas empleados o ajenos al INJUPEMP.
- Seleccionar una contraseña segura que no tenga relación obvia con el usuario, sus familiares, el Instituto de trabajo y otras relaciones parecidas.
- Reportar inmediatamente a su jefe inmediato, al Administrador de Seguridad Informática cualquier evento que pueda comprometer la seguridad del INJUPEMP y sus recursos informáticos, como por ejemplo: contagio de virus informáticos, intrusos, modificación o pérdida de datos y otras actividades poco usuales.
- Proponer medidas de Seguridad de la Información que hagan que el INJUPEMP tenga una operación cada vez más segura.

2. SEGURIDAD DE INFORMACIÓN SENSIBLE

i. Es responsabilidad de los usuarios velar por la integridad, confidencialidad, y disponibilidad de la información que acceda o maneje directamente, especialmente si dicha información ha sido clasificada como sensible.

ii. Los usuarios son responsables de utilizar la información a la que tengan acceso, exclusivamente para el desempeño de su actividad profesional y laboral en el INJUPEMP, no podrán facilitarla más que a aquellos otros empleados que necesiten conocerla para la misma finalidad y se abstendrá de usarla en beneficio propio o de terceros.

iii. La información relativa a aportaciones, números de cuenta de banco, beneficiarios, estados financieros institucionales y de los participantes, y en general datos de los participantes, debe ser tratada como información confidencial, así como, aquella información clasificada como reservada de acuerdo a los preceptos establecidos en la Ley de Transparencia y Acceso a la Información Pública.

iv. Los usuarios no podrán dar noticias de los saldo de aportaciones, préstamos personales e hipotecarios y demás operaciones sino al participante, deudor o beneficiario, a sus representantes legales o a quien tenga poder para disponer de la cuenta personal del participante o para intervenir en la operación, salvo cuando la información la pidiere la autoridad judicial en virtud de providencia dictada en juicio en que el participante sea parte, y las autoridades bancarias o entres reguladores. Los usuarios, empleados del INJUPEMP serán responsables en los términos de la Ley del Sistema Financiero por la violación del secreto que se establece y estarán obligados, en caso de revelación de secreto, a reparar los daños y perjuicios que se causen, imputables al INJUPEMP por vía Judicial y por comprobada negligencia al respecto.

v. La información relativa a los empleados, funcionarios y miembros de Junta Directiva, incluida, en su caso, la relativa a remuneraciones, evaluaciones y revisiones médicas debe ser tratada con especial cuidado como información confidencial sensible del recurso humano.

vi. Es responsabilidad de los usuarios garantizar que toda documentación en formato impreso, electrónico, etc., que contenga información sensitiva de los participantes, una vez utilizada, o que no pueda ser entregada al propietario, sea archivada de manera segura.

vii. Es responsabilidad de los encargados de la gestión de archivos físicos, velar por la integridad de la información almacenada físicamente y que refleja las transacciones e información del participante o de la institución afiliada.

viii. Cuando se traslade documentación física que contenga información sensible, por parte de cualquier empleado del INJUPEMP, ya sea que ingrese o salga de las oficinas principales/regionales o transite entre las áreas funcionales, debe portar los expedientes y demás documentos dentro de un fólder o bolsa cerrada que no permita ver el contenido de los mismos (impedir la visión de la información).

3. USO DE LAS ESTACIONES DE TRABAJO

i. El Usuario es responsable de mantener el Hardware que le ha sido asignado debidamente identificado para efectos de control de inventario. El Área responsable (Departamento de

Bienes) deberá mantener los registros de inventario debidamente actualizados.

ii. Se prohíbe utilizar la Información, Hardware y Software, para realizar actividades diferentes a las estrictamente laborales.

iii. Se prohíbe mover el Hardware, reubicarlo o llevarlo fuera del INJUPEMP sin el Visto Bueno del titular de la Oficina que lo tiene asignado y la debida autorización escrita extendida por el departamento de Bienes y el traslado debe estar motivado por los intereses y objetivos del INJUPEMP.

iv. Se prohíbe instalar y utilizar en el hardware asignado para sus actividades laborales, software no autorizado o software ilegal. En los equipos del INJUPEMP sólo podrá utilizarse software legal y oficial y su instalación será exclusiva de la Unidad Técnica de Informática.

v. Está prohibido modificar la configuración de hardware y software establecida por la Unidad Técnica de Informática. Tampoco está permitido hacer copias del software para fines personales.

vi. Se prohíbe instalar en el Hardware del INJUPEMP, software propiedad del usuario, a menos que haya sido comprobado en forma rigurosa y que esté aprobado y autorizado su uso por la Jefatura de mayor jerarquía del usuario solicitante y la Jefatura de la Unidad Técnica de Informática.

vii. El Usuario es responsable de salvar periódicamente la información de su equipo personal cuando esté utilizando el hardware para evitar que un corte de energía u otra falla del equipo, le haga perder la información de manera permanente.

viii. El Usuario debe realizar su debido respaldo (Backup) de la información que generar o utiliza en su equipo, en forma periódica.

ix. El Usuario es responsable de utilizar un protector de pantalla con contraseña para evitar que otras personas ingresen a sus archivos o en su defecto de bloquear la maquina mientras se mueva de su sitio de trabajo. Asimismo, siempre que sea posible el hardware deberá estar instalado de tal forma que no permita que visitantes o personas extrañas al INJUPEMP puedan tener acceso a ningún tipo de información, ya sea en pantalla, impresora o cualquier otro dispositivo.

x. El Usuario es responsable de apagar el hardware que tenga asignado cuando tenga que abandonar su estación de trabajo por períodos de tiempo superiores a una (1) hora. Deberá además bloquear su estación de trabajo durante cualquier ausencia temporal de su puesto de trabajo.

xi. Es responsabilidad de la División de Recursos Humanos notificar a la Unidad Técnica de Informática tan pronto un empleado termine su relación laboral con el INJUPEMP y trabaje en un Hardware propio, para que proceda a eliminar la información propiedad del INJUPEMP

contenida en el equipo y realizar la desinstalación del software Institucional.

xii. El Usuario es responsable de mantener organizada la información en el disco duro y conservar en el mismo únicamente los archivos que necesita para llevar a cabo sus labores. Los archivos de uso personal como música, fotografías, videos, juegos, etc. están prohibidos y estarán bajo la responsabilidad del usuario los daños que causaren al equipo o información del INJUPEMP por no acatar esta disposición.

xiii. El área de Soporte Técnico, eliminará bajo la instrucción y responsabilidad del usuario, la información confidencial contenida en el hardware que el usuario tenga asignado, antes de que dicho Hardware sea reparado o enviado fuera del INJUPEMP. Si esto no es posible, el usuario debe asegurarse de que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un acuerdo de confidencialidad.

xiv. Se prohíbe el uso del hardware y software del INJUPEMP a terceros o personas extrañas al mismo, salvo autorización escrita del Director Ejecutivo.

xv. Es responsabilidad de los usuarios identificar y reportar a su Jefe inmediato, hardware y software no autorizado, así como la pérdida o robo de los mismos.

xvi. No debe dejarse desatendido en ningún momento el hardware, sobre todo si se está imprimiendo o se va a imprimir Información confidencial o si la misma se está enviando oficialmente a través del correo electrónico corporativo o a través de fax.

xvii. Es responsabilidad del Usuario evitar el deterioro del Hardware, para lo cual deberá cumplir las siguientes reglas básicas:

- No ingerir ni dejar alimentos y/o bebidas cerca y/o encima del Hardware.
- No colocar objetos pesados encima del Hardware.
- Mantener alejado del Hardware cualquier elemento electromagnético como imanes, teléfonos, radios, etc.
- No colocar el Hardware en lugares inestables y/o expuestos a ser golpeados involuntariamente o que estén en riesgo de caer y dañarse parcial o totalmente.
- No abrir el Hardware. De ser necesaria dicha labor será llevada a cabo por el Área de Soporte Técnico de la Unidad Técnica de Informática.
- Es responsabilidad de los Usuarios conservar siempre limpio su lugar de trabajo, así como su Hardware.
- Conservar los cables en buen estado, ordenados y correctamente conectados. No debe existir ningún tipo de tensión, evitando siempre el doblado de los mismos.

4. USUARIOS Y CONTRASEÑAS

i. Es responsabilidad del área encargada de la administración de usuarios de la Unidad Técnica de Informática (UTI), asignar un nombre único de usuario y es responsabilidad del usuario tener una contraseña robusta reservada en cada sistema informático, los cuales deberán ser confidenciales e intransferibles para garantizar su óptima identificación.

ii. Se prohíbe asignar códigos de identificación de usuario genérico o universal, tales como: Injupemp1, Injupemp2, etc. Su utilización está restringida a procesos automáticos que se realicen en los sistemas y que no puedan cambiarse por usuarios personalizados, tales como el proceso de cierre diario o mensual, en cuyo caso, se tendrá un listado oficial de todos estos usuarios, indicando su función y operación asignada.

iii. Se prohíbe asignar códigos de identificación de usuario a personas que no sean empleados del INJUPEMP, a menos que estén debidamente autorizados, por el Director Ejecutivo o Jefe de mayor jerarquía del área que corresponda, en este caso el Jefe de la Unidad Técnica de Informática deberá dar su visto bueno y determinará los medios de control requeridos para evaluar el riesgo y que estos códigos se definan por tiempo limitado.

iv. Ningún usuario o programa debe utilizar las contraseñas de administrador de sistemas, salvo personal autorizado.

v. La UTI desactivará los Códigos de Identificación de Usuario que no sean usados por un período de un (1) mes.

vi. Los Códigos de Usuario que cumplan un período de tres (3) meses en estado de inactivos, deben pasar al estado de Cancelado en el sistema.

vii. Es responsabilidad del Usuario no guardar su contraseña en una forma legible en archivos en disco; tampoco debe escribirla en papel, dejarla en sitios donde pueda ser encontrada o compartirla o revelarla a cualquier otra persona. El usuario que viole esta normativa será responsable directo por todos los daños y perjuicios que resulten de tal violación.

viii. Es responsabilidad del Usuario cambiar inmediatamente su contraseña cuando tenga indicio o razón suficiente para creer que ha sido comprometida, o de acuerdo a la política establecida por el INJUPEMP (cada 30 días calendarios).

ix. Es responsabilidad del Usuario no usar contraseñas que sean idénticas o sustancialmente similares a contraseñas previamente empleadas.

x. La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. Es responsabilidad del Usuario cambiar en esta primera sesión su contraseña inicial por otra

contraseña robusta, el mismo día que se le entregue por parte de la Unidad Técnica de Informática.

xi. Es responsabilidad del Usuario cambiar su contraseña por lo menos cada treinta (30) días calendario.

xii. Se limita a tres (3) el número consecutivo de intentos infructuosos para introducir la contraseña de Usuario; después del tercero y último intento la cuenta involucrada queda bloqueada y se deberá notificar a la Unidad Técnica de Informática, así como de llenar el formulario respectivo, documentando cual ha sido el problema para tal evento y firmado por su Jefe inmediato.

xiii. Es responsabilidad del Usuario evitar que su contraseña esté visible en pantalla en cualquiera de los procesos en que la utilice (conexión, utilización, etc.).

xiv. Todo aplicativo debe ser auditable, es decir, debe permitir dejar rastro de todas las transacciones críticas generadas: bitácora (log) de transacciones y registro de entradas y salidas de usuarios.

xv. Se prohíbe tener múltiples sesiones de usuario en diferente Hardware. Por ejemplo su usuario en computadoras del Departamento de Prestamos Personales y otra sesión en el Departamento de Cartera y Cobro.

xvi. Ningún usuario puede tener más de un código de identificación de usuario para el acceso a una misma aplicación.

xvii. Es responsabilidad de Recursos Humanos que tan pronto un empleado termine su relación laboral con el INJUPEMP, se proceda a realizar la cancelación de sus códigos de identificación de usuario y Contraseña, notificando a la Unidad Técnica de Informática de tal cambio por escrito para hacer las gestiones necesarias de seguridad y de resguardo de la información propiedad del INJUPEMP.

xviii. Es responsabilidad del Usuario crear siempre contraseñas robustas, para ello deberá cumplir las siguientes reglas:

- No utilizar solamente letras o números, sino una combinación de ambos.
- No utilizar palabras reconocibles como nombres propios, palabras del diccionario o términos de programas de televisión, novelas y artistas, entre otros.
- No utilizar palabras en idiomas extranjeros.
- No utilizar información personal.
- No invertir palabras reconocibles.
- No utilizar la misma contraseña para todas las máquinas.
- Mezclar letras mayúsculas y minúsculas.
- Seleccionar una contraseña que pueda recordar.

viii. Es responsabilidad del encargado del área que administra la seguridad de los usuarios, realizar una revisión periódica de al menos cuatro veces al año, de los accesos asignados a los usuarios.

5. POLÍTICA ANTIVIRUS

Responsabilidades de los Usuarios:

i. Utilizar el Antivirus autorizado por el INJUPEMP, el cual tendrá disponible automáticamente cada vez que se conecte al dominio de la red.

ii. Mantener el Antivirus permanentemente activo para que vigile constantemente todas las operaciones realizadas en el Sistema. Está terminantemente prohibido al Usuario desactivar el Antivirus.

iii. Dar aviso inmediato a la Unidad Técnica de Informática y apagar el Hardware asignado inmediatamente que detecte la presencia de un virus electrónico que no es eliminado por el Antivirus.

Por motivo de seguridad, los mensajes o archivos adjuntos que contengan virus serán inmediatamente eliminados sin posibilidad de recuperación.

iv. Revisar con el Antivirus sus unidades de disco flexible, discos removibles o memorias USB (flash) antes de usarlas.

Prohibiciones:

v. Está terminantemente prohibido al Usuario ejecutar los archivos anexos a su correo electrónico si no provienen de una fuente reconocida y segura.

vi. Queda terminantemente prohibido al Usuario compartir el disco duro del Hardware que tenga asignado, si necesita compartir alguna carpeta debe obtener la autorización correspondiente y sólo hacerlo al usuario destino.

6. CORREO ELECTRÓNICO

i. Queda terminantemente prohibido a los usuarios el envío de mensajes masivos a través de correo electrónico; excepto en el caso de correos oficiales los que podrán ser enviado por

usuarios debidamente autorizados por la Dirección Ejecutiva, como ser los miembros de la Junta Directiva, el Director Ejecutivo, Asistente del Director Ejecutivo, Administrador de la Seguridad de la Información, Jefes de División, Jefes de Unidades, Asistente de la Jefatura de la Unidad Técnica de Informática y el Operador del Centro de Datos (Datacenter) u otros debidamente autorizados

ii. Es responsabilidad del Usuario enmarcar todos los mensajes que envíe a través de correo electrónico dentro de las normas mínimas de respeto y protocolo electrónico, siempre deberá incluir el tema o referencia del correo que remite (Asunto) pero sin incluir contenidos hostiles que molesten a los receptores del mismo, tales como: comentarios sobre sexo, raza, religión o preferencias sexuales; asimismo, es responsabilidad del Usuario reportar a su Jefe Inmediato la recepción de este tipo de mensajes, quien a su vez deberá reportarla al Jefe de la División de Recursos Humanos, Jefe de Relaciones Laborales, Jefe de la Unidad Técnica de Informática y al Administrador de Seguridad de la Información.

iii. Es responsabilidad del Usuario evitar que su cuenta de correo electrónico sea utilizada por terceros (clientes, proveedores, sindicatos, etc.).

iv. Es responsabilidad del Usuario evitar que la información confidencial sea transmitida por medio de su cuenta de correo electrónico, salvo autorización previa del Jefe de área en cuyo caso los archivos deben viajar en forma segura o cifrada.

v. Es responsabilidad del Usuario evitar el uso de una cuenta de correo electrónico que pertenezca a otro usuario, si hay necesidad de hacerlo en caso de ausencias o vacaciones se debe recurrir por medio de la UTI a mecanismos alternos como redirección de mensajes.

vi. Se prohíbe el uso de la cuenta de correo electrónico, para:

- Utilizar el correo corporativo para mensajes de carácter personal.
- Enviar mensajes desde la cuenta de correo electrónico de un usuario con firma de otro.
- Acceder sin autorización a otra cuenta de correo electrónico.
- Transmitir mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización.
- Participar en cadenas de mensajes que congestionen la red y que destruyen los equipos de comunicación de redes y que saturan los servidores de mensajería.

vii. Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

viii. Es responsabilidad del Usuario eliminar periódicamente de sus dispositivos de almacenamiento los mensajes que ya no necesite. Con esto se reducen los riesgos de que otros usuarios puedan acceder a esa información; y además, se libera espacio en disco.

ix. Ningún empleado del INJUPEMP está autorizado para monitorear los mensajes de correo

electrónico, excepto el área de Auditoría Interna o el área que previamente esté autorizada por la Dirección Ejecutiva. El monitoreo es realizado para cumplir con políticas internas en casos de sospechas de actividad no autorizada, investigaciones y otras razones de la Alta Gerencia; en estos casos el INJUPEMP no está obligado a solicitar autorización alguna al Usuario involucrado.

x. Todos los mensajes enviados por medio de correo electrónico pertenecen al INJUPEMP y éste se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.

xi. Queda terminantemente prohibido el uso de servicios de mensajería instantánea (Chat) no corporativo, utilizando el acceso de Internet del INJUPEMP, si para sus funciones necesita este servicio debe obtener la autorización correspondiente y utilizarlo sólo para asuntos laborales.

7. USO DE INTERNET

i. Es responsabilidad del Usuario utilizar Internet únicamente con propósitos laborales. Queda terminantemente prohibido a los Usuarios el acceso, la transmisión, distribución, reproducción o almacenamiento de cualquier tipo de información, dato o material que viole estas Políticas, la Ley o los protocolos electrónicos.

ii. Es responsabilidad del Usuario evitar la descarga de archivos desde el Internet. Antes de realizar una descarga desde Internet, el Usuario deberá solicitar por medio de la Unidad Técnica de Informática el software que requiere, y sólo en caso de que no esté disponible o no se cuente con uno similar, deberá solicitarle a su Jefe inmediato que lo solicite ante el área de compras, con la debida justificación avalada por la UTI.

iii. Queda terminantemente prohibido a los Usuarios el acceso a Internet por medio de dispositivos o servidores que no sean del INJUPEMP tales como Módems, USB, Accesos inalámbricos o redes externas o por medio de otros proveedores cuando esté haciendo uso de la red del INJUPEMP.

iv. Queda terminantemente prohibido a los Usuarios no autorizados interferir o tratar de interferir con los servicios Internet del INJUPEMP o de cualquier otro servidor de Internet, aun cuando no pertenezca al INJUPEMP.

v. Es responsabilidad de los Usuarios desconectarse inmediatamente de páginas de Internet que tengan contenido ofensivo, ya sea sexual, pornográfico, político, racista o de cualquier otro tipo. Los Usuarios que accidentalmente se conecten a estas páginas deberán informar a su superior

inmediato, quien deberá comunicarse con el Administrador de Seguridad para bloquear estos accesos.

vi. Es responsabilidad del Jefe de la Unidad Técnica de Informática, autorizar o denegar el acceso a Internet, de forma temporal o permanente y acorde al perfil del cargo del solicitante. Dicho acceso deberá ser solicitado por medio del procedimiento correspondiente y se otorgará (si procede) previa aprobación del Director Ejecutivo o su Asistente.

8. ADQUISICIÓN DE HARDWARE Y SOFTWARE

i. El proceso de adquisición de Hardware y Software de misión crítica o prioritaria a través de terceros debe cumplir la metodología de adquisición legal y formal del INJUPEMP e incluir la suscripción de un contrato pro forma con cláusulas básicas para la protección de la Información y del Software, así como para documentación y respaldo, con el propósito de proteger los intereses institucionales frente a las cláusulas propuestas por el fabricante, distribuidor o vendedor.

ii. La adquisición de Hardware y Software, o el desarrollo de programas, sólo se gestionará a través de la Jefatura de la Unidad Técnica de Informática, Jefe de la División de Presupuestos y Jefe de la División Administrativa.

iii. A menos que se indique lo contrario, los Usuarios deben asumir que todo el Software del INJUPEMP está protegido por la Legislación sobre Derechos de Autor y requiere Licencia de Uso. Por tal razón, es ilegal y queda terminantemente prohibido a los Usuarios hacer copias o usar el Software para fines personales.

iv. Queda terminantemente prohibido a los usuarios utilizar software descargado desde Internet; y en general, software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por la Jefatura de la Unidad Técnica de Informática, en los términos del numeral anterior “7. USO DE INTERNET”

8. DISPOSITIVOS MÓVILES (LAPTOP).

i. Se prohíbe tener como herramientas de trabajo, computadores portátiles (laptops), CPU’s, USB´s o cualquier otro equipo de propiedad del usuario, salvo autorización previa emitida por el jefe de mayor jerarquía del área que corresponda y el correspondiente registro en la UTI y en el departamento de Bienes.

ii. Es responsabilidad del Usuario utilizar los disquetes, discos compactos, USB´s, etcétera, de manera adecuada. Queda terminantemente prohibido al Usuario usar en los equipos del INJUPEMP disquetes, CD’s, USB u otros dispositivos de almacenamiento que previamente hayan sido utilizados en computadores de uso público o dudoso, como por ejemplo: centros educativos, café Internet, o incluso, su computador personal sin la debida revisión por parte del antivirus corporativo.

iii. Es responsabilidad del Usuario que usa una Laptop del INJUPEMP o personal proteger la información propiedad de INJUPEMP guardada o archivada en el mismo, para lo cual deberá cumplir las siguientes reglas básicas:

- No dejar la Laptop desatendida en lugares públicos para evitar que el equipo o la información sea sustraída.
- Cifrar el contenido de la Laptop para evitar el acceso a los datos en caso de que el equipo sea objeto de robo.
- Usar contraseñas robustas, en lo posible con encriptación para evitar el acceso no autorizado a datos importantes.
- Respaldar la información antes de viajar.
- No desensamblar la Laptop. Sólo un representante técnico autorizado por el fabricante podrá dar servicio y reparar la computadora.

iv. Toda laptop perteneciente al INJUPEMP debe tener instalado el software oficial de antivirus y de ser posible el cifrado del disco para evitar el acceso a los datos en caso de que sea objeto de pérdida o robo.

v. Es obligatorio para todo el personal que usa dispositivos inalámbricos, propiedad del INJUPEMP, para el desarrollo de sus funciones, como: teléfonos celulares, Ipad, Ipod, etc. que utilice como mecanismo de seguridad el bloqueo automático de los mismos y el uso de contraseña de acceso, caso contrario se aplicarán las sanciones correspondientes.

vi. Es responsabilidad del usuario, realizar un respaldo periódico de la información contenida en los dispositivos móviles o portátiles asignados, para evitar la pérdida de dicha información por robo, extravío, daño del aparato o cualquier otra circunstancia.

vii. Es responsabilidad del Usuario que usa una Laptop del INJUPEMP, proteger la información guardada o archivada en la misma, para lo cual deberá cumplir las siguientes normas:

- Utilizar un candado físico para anclar la Laptop cuando vaya a ausentarse temporalmente.
- Eliminar datos innecesarios que puedan estar almacenados en la Laptop.
- Guardar todos los detalles del computador, incluyendo fabricante, modelo y número serial para poder llenar formularios en caso de ser necesitados.
- Asegurarse de apagar la Laptop, no dejarla en modo hibernación ni suspenso (stand-by) antes de empacarla.
- No empacar la Laptop dentro de un portafolio o valija que se encuentre densamente cargada con otros objetos. La compresión podría ocasionar un daño interno a ésta.
- No rayar, flexionar, golpear, o presionar la superficie de la pantalla de cristal líquido (LCD) de la Laptop.

- No colocar ningún objeto entre la pantalla y el teclado. No levantar la computadora deteniéndola por la pantalla únicamente. Cuando se levante la Laptop abierta, detenerla a por la mitad inferior.
- No voltear la Laptop sobre si misma mientras el adaptador de corriente está conectado. Esto podría romper su conector.
- No fijar la Laptop dentro de un vehículo o en cualquier otro lugar que esté sujeto a vibraciones continuas.
- No tocar el lente dentro de la bandeja de la unidad de DVD/CD-ROM. El disco compacto deberá de sostenerse por las orillas y no deberá tocarse la superficie del mismo.

10. POLÍTICAS DE SEGURIDAD APLICABLES A LA CONTRATACIÓN DE CONSULTORES DE SERVICIOS TECNOLOGICOS

i. No se deberá contratar a consultores para servicios que puedan crear conflicto con sus obligaciones previas o vigentes con respecto a los intereses del INJUPEMP, o cuando el juicio profesional, objetividad, imparcialidad o la defensa del interés institucional se puedan ver afectados por consideraciones personales, de índole financiera u otra.

ii. El INJUPEMP exige a todos los Consultores, observar los más altos niveles éticos y cualquier empleado está obligado a denunciar ante las instancias correspondientes, todo acto sospechoso de fraude o corrupción del cual tenga conocimiento o sea informado durante el proceso de selección y las negociaciones o la ejecución de un contrato.

iii. Todo contrato celebrado con terceros deberá contener cláusulas de confidencialidad e incluir al menos los siguientes puntos: acuerdo de no divulgación total o parcial de la información, propiedad de la información y vigencia perenne del acuerdo, responsabilidades de las partes y límite de uso de la información, siendo responsable el titular del área ejecutora, de vigilar su estricto cumplimiento.

11. POLÍTICA APLICABLE A LA SEGURIDAD FÍSICA

i. Todos los sitios donde se encuentren sistemas de procesamiento informático o de almacenamiento, así como el acceso a las diferentes oficinas, deben de ser protegidos contra accesos no autorizados, utilizando procedimientos o tecnologías de autenticación, monitoreo y registro.
ii. En aquellas oficinas en donde existen empleados con acceso al lugar o los equipos de comunicación hacia las redes de datos o telefonía del INJUPEMP, el Jefe del área deberá tomar las medidas pertinentes para el resguardo y cuidados especiales del equipo.

12. POLÍTICA DE SEGURIDAD APLICABLE A LAS BITACORAS (LOGS)

i. Es responsabilidad del Jefe de la Unidad Técnica de Informática asegurar que se generen Logs o Bitácoras para los equipos y aplicaciones clasificadas como críticas, así como los solicitados por el área de Auditoría; dichos Logs deben ser custodiados en forma segura para evitar su modificación.

ii. Los Logs o bitácoras generados deben ser monitoreados periódicamente para detección temprana de posibles fallas en los equipos y aplicaciones o vulnerabilidades de seguridad. Esta supervisión será en primer lugar por la Unidad Técnica de Informática, Administrador de la Seguridad de la Información, Unidad de Auditoria Interna a través del Auditor de Sistemas de Información.

C. POLÍTICAS DE SEGURIDAD DE APLICACIÓN ESPECÍFICA

AREA DE SISTEMAS.

1. SEGURIDAD DE SERVIDORES

i. Es responsabilidad del Jefe de la Unidad Técnica de Informática del INJUPEMP, asignar a todos los servidores internos instalados en el Instituto, un responsable por la administración del sistema de cada uno y contar como mínimo con la siguiente información relacionada:

- Nombre del Servidor
- Localización del Servidor
- Nombre del administrador responsable y localización al igual que su suplente
- Detalle especifico del Hardware
- Sistema operativo y su versión
- Aplicaciones y bases de datos
- Función principal y/o uso
- Acuerdos de mantenimiento (Plan detallado – Cronograma)

ii. Es responsabilidad de cada administrador del sistema, que todos los servidores, así como su sistema operativo, tengan estándares de configuración de seguridad documentados y aplicados de acuerdo al rol del servidor en la organización.

iii. Es responsabilidad del Administrador de Sistemas de la UTI, que las actualizaciones más recientes de seguridad sean instaladas en los servidores tan pronto como sea posible, validando previamente en ambientes de prueba, considerando el menor impacto en la continuidad de los servicios de negocio y contando con la aprobación del Comité de Gestión Tecnológica.

Dicha actualización será producto de revisiones mensuales a las publicaciones de seguridad del

emisor del software.

iv. Es responsabilidad del Jefe de la Unidad Técnica de Informática, definir los procesos tecnológicos, mantenerlos actualizados y velar por su cumplimiento, para mantener los servidores protegidos físicamente en un ambiente con control de acceso y protección ambiental.

v. Es responsabilidad del Jefe de la Unidad Técnica de Informática del INJUPEMP, garantizar que los cambios que se hagan tanto a hardware como software en ambiente de producción, cuenten con la aprobación del Comité de Gestión Tecnológica. .

vi. Es responsabilidad del Jefe de la Unidad Técnica de Informática del INJUPEMP reportar a su Jefe Inmediato con copia al Administrador de Seguridad de la Información, violaciones a las configuraciones, hechas por los usuarios, de acuerdo con las políticas definidas para servidores y estaciones de trabajo.

2. SEGURIDAD DE EQUIPOS DE COMUNICACIÓN

i. Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación, video seguridad y cómputo deben ser tratadas como Información Confidencial.

ii. Es responsabilidad del Jefe de la Unidad Técnica de Informática del INJUPEMP, definir los procesos de su área, mantenerlos actualizados y velar por su cumplimiento, para que todos los recursos de red críticos como enlaces de comunicaciones, Firewalls, servidores, centrales de conexión o centros de cableado del Instituto, estén en áreas de acceso físico restringido.

iii. Queda terminantemente prohibido que los empleados y funcionarios del INJUPEMP lleven a cabo algún tipo de instalación de líneas telefónicas digitales o análogas, canales de transmisión de datos, módems o cambiar su configuración, esto es responsabilidad exclusiva del área de Informática o de cualquier empresa que se haya contratado para tal fin, en cuyo caso será supervisada por la Unidad Técnica de Informática.

iv. Es responsabilidad del Asistente del Jefe de la Unidad Técnica de Informática (Jefe de Producción y Data Center), llevar control estricto y actualizado de la topología, archivos y parámetros de configuración de la red; así como el inventario de equipos y software de la misma.

v. Es responsabilidad del responsable del Área de Desarrollo de la UTI, definir e implantar con aprobación del Comité de Gestión Tecnológica, procedimientos y controles para la realización de cambios sobre la red de datos y telecomunicaciones, teniendo en cuenta que los horarios no impacten negativamente la disponibilidad de los servicios de red críticos.

vi. Queda terminantemente prohibida la utilización de herramientas de monitoreo de red, esta actividad está restringida sólo al área de Producción y Data Center del INJUPEMP, encargados

de efectuar el diagnóstico y mantenimiento del funcionamiento de las redes.

vii. Para prevenir la intrusión de hackers a través de puertas traseras, está prohibido el uso de módems en PC´s que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado por el Jefe de la Unidad Técnica de Informática del INJUPEMP. Todas las comunicaciones de datos deben efectuarse a través de la Red Interna.

3. SEGURIDAD EN REDES CON TERCEROS

i. Es responsabilidad del Jefe de la Unidad Técnica de Informática, definir los procesos de conexión con terceros, mantenerlos actualizados y velar por su cumplimiento para que toda conexión entre las redes del INJUPEMP y redes con terceros cuenten como mínimo con mecanismos de control de acceso lógico, tales como: Firewall, Proxys y DNS.

ii. Es responsabilidad del responsable del Área de Operaciones de la UTI asegurar que los enlaces de comunicación establecidos con terceros estén controlados y contar como mínimo con la siguiente información relacionada:

- Servicios habilitados
- Origen y destino de la conexión.
- Propósito de la conexión.
- Datos del contacto del tercero como: Nombre, teléfono y correo electrónico.

iii. Es responsabilidad del titular del área de Operaciones de la UTI, que en los enlaces de comunicaciones establecidos con terceros, se depure el enrutamiento de tal manera que se publiquen únicamente las redes necesarias para el buen funcionamiento de las aplicaciones que utiliza este enlace.

iv. Es responsabilidad del titular del Área de Operaciones de la UTI, que los eventos que afecten la seguridad de la red privada del INJUPEMP queden registrados en una bitácora como documento indispensable para posteriores análisis de riesgos.

v. Es responsabilidad del titular del Área de Operaciones de la UTI, garantizar comunicaciones encriptadas o cifradas y seguras desde el punto donde se produce al punto donde se consume.

4. ACCESO Y CONFIGURACIÓN REMOTOS

i. Está prohibido otorgar cuentas o acceso remoto a la red del INJUPEMP a menos que sea autorizado por el Jefe de la Unidad Técnica de Informática o el Director Ejecutivo y sólo a través de VPN’s que cuenten con las medidas de seguridad adecuadas.

5. SEGURIDAD EN REDES INALÁMBRICAS

ii. Es responsabilidad del titular del Área de Operaciones, observar las siguientes prácticas en la administración de las redes inalámbricas:

- Cambiar la contraseña asignada por el fabricante o de instalación.
- Activar el filtro de direcciones MAC.
- Restringir de acuerdo con lo establecido el número máximo de dispositivos que pueden conectarse.
- Utilizar siempre protocolos de encriptación que estén de acuerdo con los estándares internacionales vigentes, los cuales serán verificados en conjunto con el Administrador de Seguridad de la Información.
- Proporcionar un entorno físicamente seguro a los puntos de acceso.
- Utilizar IPSec, VPN, Firewalls y monitorear los accesos a los puntos de acceso.
- Inhabilitar la emisión Broadcast del SSID.
- Cambiar el SSID (Server Set ID) por defecto de los puntos de acceso, conocidos por todos.

6. DESARROLLO DE SOFTWARE

i. Es Responsabilidad del Jefe de la Unidad Técnica de Informática del INJUPEMP y del Comité de Gestión Tecnológica, asegurar que todos los sistemas desarrollados por el INJUPEMP cumplan con las Políticas y Procedimientos de Seguridad de la Información, y que los contratos con terceros incluyan una cláusula para que éstos se obliguen también a cumplirlas.

ii. Con el propósito de garantizar la integridad y confidencialidad de la información que administrará el software desarrollado internamente o por terceros y antes del paso al ambiente de pruebas, es responsabilidad del titular del Área de Desarrollo de UTI, garantizar que existen evidencias de que se ejecutan pruebas intrínsecas al desarrollo y a la documentación técnica respectiva.

iii. Es Responsabilidad del titular del Área de Desarrollo, establecer los mecanismos para asegurar que solamente las funciones descritas en el documento de especificaciones de la solución tecnológica aprobado, sean desarrolladas.

iv. Se prohíbe que los Programadores de software conozcan las claves utilizadas en ambientes de producción (encriptores, claves, etc.) y es responsabilidad del Jefe de la Unidad Técnica de Informática del INJUPEMP asegurar el cumplimiento de dicha restricción.

v. Es Responsabilidad del Comité de Gestión Tecnológica, garantizar que los desarrollos y/o modificaciones hechos a los sistemas de aplicación, no se trasladen al ambiente de producción, si no se cuenta primero con todos los requerimientos documentados, pruebas de aceptación, manuales de usuario y técnico, Acta de Formalización y firma de aceptación de involucrados, programas fuentes, la documentación de entrenamiento, operación y de seguridad adecuados.

vi. Es Responsabilidad del titular del Área de Desarrollo, definir y mantener actualizados los procesos de desarrollo para que la nueva programación y/o modificaciones efectuadas a los

sistemas de información, cumplan un proceso estricto de pruebas que validen la calidad del Software, antes de ser validados en la etapa de pruebas de aceptación.

7. CENTROS DE CÓMPUTO Y TELECOMUNICACIONES

i. Los Centros de Cómputo y Área de Telecomunicaciones del INJUPEMP están clasificadas como áreas de acceso restringido.

ii. Es responsabilidad del Jefe de la Unidad Técnica de Informática del INJUPEMP, asegurar que todos los recursos de computación y Telecomunicaciones del Instituto, cuenten con planes de mantenimiento preventivo y/o correctivo debidamente contratados.

iii. Es responsabilidad del Jefe de la Unidad Técnica de Informática del INJUPEMP, que los Centros de Cómputo y las áreas de telecomunicaciones del Instituto cuenten con sistemas de control de acceso físico, que puedan ser auditados.

8. RESPALDOS

El Instituto deberá contar como mínimo con dos centros u oficinas diferentes, para el almacenamiento de respaldos. Para efecto de las Políticas de Respaldo, se referirá como centro alterno, el situado distante en la bóveda de un banco local contratado para tal efecto.

ii. Es responsabilidad del Administrador de Seguridad Informática definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los datos de producción independientemente del servidor en el Data Center donde se encuentre , el que debe cumplir con las siguientes reglas:

- Periodicidad: Diaria
- Tipo de Respaldo: Incremental/Total dependiendo de la viabilidad
- Retención: 5 años
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada seis meses

iii. Es responsabilidad del Administrador de Seguridad Informática definir, documentar, mantener y probar un proceso de respaldo y recuperación para a todos los archivos de aplicaciones de producción independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Semanal
- Tipo de Respaldo: Total
- Retención: 5 años
- Custodia: En centro alterno de almacenamiento

- Prueba de Recuperación: Cada seis meses

iv. Es responsabilidad del Administrador de Seguridad Informática definir, documentar, mantener y probar un proceso de respaldo y recuperación para todas las Configuraciones de los servidores incluyendo los elementos de comunicaciones y seguridad de producción, que estén en el Data Center y deben cumplir con las siguientes reglas:

- Periodicidad: Semanal
- Tipo de Respaldo: Total
- Retención: 1 año
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada seis meses

v. Es responsabilidad del Administrador de Seguridad Informática definir, documentar, mantener y probar un proceso de respaldo y recuperación para todas las imágenes y documentos digitalizados de producción independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Diaria
- Tipo de Respaldo: Incremental
- Retención: 10 años
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada seis meses

vi. Es responsabilidad del Administrador de Seguridad Informática definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los logs o bitácoras transaccionales del ambiente de producción independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Semanal
- Tipo de Respaldo: Incremental
- Retención: 5 años
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada un año
- Campos mínimos requeridos en el archivo de logs:
    a) Persona
    b) Lugar
    c) Tiempo
    d) Acción

vii. Es responsabilidad del Administrador de Seguridad Informática definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los logs de consulta de producción independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Semanal
- Tipo de Respaldo: Incremental
- Retención: 6 meses
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada un año

viii. Es responsabilidad del titular del Área de Desarrollo definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los archivos de programación del ambiente de Desarrollo independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Diaria
- Tipo de Respaldo: Total
- Retención: 1 año
- Custodia: En centro alterno de almacenamiento

ix. Es responsabilidad del Operador de Cierres ejecutar y monitorear la realización de los procesos de respaldo asociados con las políticas de respaldo de la i a la vii.

x. Es responsabilidad del Coordinador de Telecomunicaciones, custodiar los respaldos generados acorde con las políticas de respaldo de la i a la vii.

xi. Es responsabilidad del Coordinador de Telecomunicaciones, garantizar que el sitio alterno de almacenamiento cuente como mínimo con lo siguiente:

- Debe estar localizado en un lugar distante y distinto en donde se generó la copia de la información original.
- No debe estar en una zona con peligro de derrumbe o inundación.
- Control ambiental apropiado para el almacenamiento de los dispositivos utilizados para respaldar la información.
- Control de acceso físico
- Control de Inventario actualizado.
- Transporte seguro de la información respaldada
- Encripción del contenido de los dispositivos de almacenamiento a resguardar.

xii. Es responsabilidad del Coordinador de Telecomunicaciones, de la UTI, que los equipos de almacenamiento o respaldo de información que deban ser desechados, se destruyan físicamente o sean escritos de manera segura a través del uso de herramientas especiales que garanticen y verifiquen que no queda información remanente.