

**SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS
ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES
INFRACTORES
- SNAI -**



**POLÍTICAS DE USO, SERVICIOS, CONECTIVIDAD Y EQUIPOS
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIÓN**

Diciembre 2020

**Versión
2.0**

Elaborado por: Juan Carlos Muñoz Mejía



Tabla de Contenido

Capítulo I.- POLÍTICAS DE SEGURIDAD 5

Capítulo II.-ESTRUCTURA DEL ÁREA DE SISTEMAS27

Capítulo III.-SERVICIO EXTENDIDO “ON CALL” 35

Capítulo IV.-PROPUESTA “GREEN IT”37

Capítulo V.- PROCESOS.....43

Capítulo VI.- MANUAL DE PROCEDIMIENTOS 53

Capítulo VII.- FORMULARIOS..... 61

Capítulo VIII.- SLA..... 66

Capítulo IX.-PLAN DE CONTINGENCIA 76

Capítulo X.- CATÁLOGO DE SERVICIOS 119

CAPÍTULO 1.- POLÍTICAS DE SEGURIDAD



ÍNDICE

CAPÍTULO 1.- POLÍTICAS DE SEGURIDAD

CAPÍTULO 2.- ESTRUCTURA DEL ÁREA DE SISTEMAS

CAPÍTULO 3.-SERVICIO EXTENDIDO “ON CALL”

CAPÍTULO 4.-PROPUESTA “GREEN IT”

CAPÍTULO 5.- PROCESOS

CAPÍTULO 6.- MANUAL DE PROCEDIMIENTOS

CAPÍTULO 7.- FORMULARIOS

CAPÍTULO 8.- SLA

CAPÍTULO 9.- PORTAFOLIO DE SERVICIOS

CAPÍTULO 10.- PLAN DE CONTINGENCIA



I. POLÍTICAS DE SEGURIDAD

Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Institución. Sin ellos nos quedaríamos rápidamente limitados en ejecución de procesos y compromisos gubernamentales y por tal razón la Coordinación General Administrativa Financiera y la Área de Tecnologías de la Información y Comunicación, tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Institución debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), cómo se procesa (PC, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas coordinaciones de la Institución están en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. En todo caso cada año el área de TIC llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará cada año un informe para la Coordinación General Administrativa Financiera que muestre el estado actual de la Institución en cuanto a seguridad informática y los progresos que se han logrado.

A todos los servidores públicos, consultores y contratistas debe proporcionárseles adiestramiento, información y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Institución. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la Institución como lo son la contabilidad y la nómina.

La finalidad de las políticas de seguridad que se describen más adelante es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la Institución (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

Responsabilidades

Los siguientes entes son responsables, en distintos grados, de la seguridad en la Institución:

- **El área de TIC** es responsable de implantar y velar por el cumplimiento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización. También es responsable de evaluar, adquirir e implantar productos

de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

- **El Director de TIC** es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.
- **El Administrador de Sistemas** es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto o de un ente como el CERT (Computer Emergency Response Team). El Administrador de Sistemas también es responsable de informar al Director de TIC y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.
- **Los servidores públicos** son responsables de cumplir con todas las políticas de la Institución relativas a la seguridad informática y en particular:
 - a. Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
 - b. No divulgar información confidencial de la Institución a personas no autorizadas.
 - c. No permitir y no facilitar el uso de los sistemas informáticos de la Institución a personas no autorizadas.
 - d. No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax, email, internet) para otras actividades que no estén directamente relacionadas con el trabajo en la Institución.
 - e. Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
 - f. Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
 - g. Reportar inmediatamente a su jefe inmediato y/o a un funcionario de TIC evento que pueda comprometer la seguridad de la Institución y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

I.1.- Políticas de seguridad para computadores

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de los equipos de cómputo de la Institución.

Alcance

Esta política se aplica a todos los servidores públicos, contratistas, consultores y personal temporal de la Institución.

1. Los computadores de la Institución sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
2. Los equipos de la Institución sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos, pasatiempos o asuntos personales.
3. Debe respetarse y no modificar la configuración de hardware y software establecida por el área de Gestión de TIC.
4. No se permite fumar, comer o beber mientras se está usando un PC.
5. Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
6. Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder interrumpibles (UPS).
7. Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
8. Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.
9. No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Institución se requiere una autorización escrita.
10. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
11. Si un PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

12. Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.
13. Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
14. Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PC que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Institución.
15. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
16. Los usuarios no deben copiar a un medio removible (como un dispositivo de almacenamiento USB) el software o los datos residentes en las computadoras de la Institución sin la aprobación previa de la Coordinación respectiva.
17. No pueden extraerse datos fuera de la sede de la Institución sin la aprobación previa de la Coordinación respectiva. Esta política es particularmente pertinente a aquellos que usan computadoras portátiles o están conectados a redes como Internet.
18. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al área de Gestión de TIC y poner la PC en cuarentena hasta que el problema sea resuelto.
19. Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Institución.
20. No debe utilizarse software bajado de 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 el área de Gestión de TIC.
21. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el área de Gestión de TIC.

22. No deben usarse medios de almacenamiento en cualquier computadora de la Institución a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
23. La información de la Institución clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por el área de Gestión de TIC.
24. No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.
25. El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.
26. Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de enviarlas a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la Institución.
27. No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la Institución.
28. La información generada en los equipos de la Institución sean portátiles o de escritorio, son exclusivamente **propiedad intelectual del SNAI** por tanto, mientras permanezca laborando o al cesar funciones, el funcionario está en la OBLIGACIÓN de presentar los respaldos de su trabajo o de la información que mantiene en el procesador de trabajo ya sea que, sea requerido por la DTIC, por la Dirección de Administración de Talento Humano o por la Máxima autoridad.
29. El personal que utiliza un computador portátil que contenga información confidencial de la Institución, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

I.2.- Políticas de Seguridad para las Comunicaciones

Propiedad de la información

Con el fin de mejorar la productividad, la Institución promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono y el correo electrónico. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Institución y no propiedad de los usuarios de los servicios de comunicación.

Uso de los sistemas de comunicación

1. Los sistemas de comunicación de la Institución generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del funcionario ni con las actividades de la Institución.
2. Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
3. La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Institución y en tal sentido deben usarse las horas no laborables.

Confidencialidad y privacidad

1. Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que esté cifrada. Para tal fin debe utilizarse PGP (Pretty Good Privacy), Outlook, Spark, Outlook Express u otros productos previamente aprobados por el área de Gestión de TIC.
2. Los funcionarios y servidores públicos de la Institución no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Institución se compromete a respetar los derechos de sus funcionarios, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.
3. Es política de la Institución no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones pueden ocasionalmente ser supervisados, de ser necesario, para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un funcionario individual durante el curso de resolución de un problema.



- De manera consistente con prácticas generalmente aceptadas, la Institución procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

Reenvío de mensajes

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Institución, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la Institución sin la debida aprobación.

Borrado de mensajes

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.



I.3.- Políticas de seguridad para redes

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Institución al estar conectada a redes de computadoras.

Alcance

Esta política se aplica a todos los servidores públicos, contratistas, consultores y personal temporal de la Institución.

Aspectos generales

Es política de la Institución prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

Modificaciones

Todos los cambios en los servidores y equipos de red de la Institución, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de Routers y Switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Cuentas de los usuarios

1. La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.
2. No debe concederse una cuenta a personas que no sean funcionarios de la Institución a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
3. Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
4. No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más

largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

5. Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.
6. Ningún equipo ajeno a esta Cartera de Estado gozará de los servicios de red como son IP, Wireless, configuración especial, adhesión a los dominios *atencionintegral.gob.ec* y/o *seguridadpenitenciaria.gob.ec*
7. Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
8. Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un funcionario cesa en sus funciones.
9. Cuando un funcionario es despedido o renuncia a la Institución, debe desactivarse su cuenta antes de que deje el cargo.

Contraseñas y el Control de Acceso

1. El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
2. Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
3. Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
4. La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
5. Las contraseñas predefinidas que traen los equipos nuevos tales como Routers, Switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

6. Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número consecutivos de intentos consecutivos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.
7. Para el acceso remoto a los recursos informáticos de la Institución, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.
8. Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).
9. Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
10. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Institución, pudiendo ser causal de despido.
11. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
12. Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.
13. Los servidores de red y los equipos de comunicación (PBX, Routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

I.4.- Políticas de Uso de Internet

Propósito

El propósito de esta política es establecer directrices adecuadas para el acceso y la utilización de Internet a través de la red de la Institución.

Alcance

Esta política se aplica a todos los servidores públicos, contratistas, consultores y personal temporal de la Institución.

Aspectos generales

Servicios de Internet están autorizados a funcionarios designados por su manager para mejorar la responsabilidad de su trabajo. Internet es una herramienta excelente sino que también crea las implicaciones de seguridad que debe protegerse de la Institución. Por esa razón, los funcionarios tengan acceso sólo como un medio de proporcionar apoyo en el cumplimiento de sus responsabilidades de trabajo.

Modificaciones

Todos los cambios en los servidores y equipos de red de la Institución, incluyendo la instalación del nuevo software, el cambio de direcciones IP, la reconfiguración de Routers y Switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

General:

1. El acceso a internet está autorizado por el jefe inmediato si considera al internet como herramientas que ayuden a su trabajo.
2. Cada persona es responsable de respectivo uso.
3. El uso de servicios de Internet debe reflejar la misión de la Institución y apoyar las metas y los objetivos fijados.
4. Estos servicios deben apoyar actividades conexas legítimas, misión de la Institución y ser coherentes con prudentes consideraciones operacionales, de seguridad y de privacidad.

5. La Institución tendrá la responsabilidad de todo el contenido del sitio web (www.atencionintegral.gob.ec) y del formato de presentación para reflejar la misión de la Institución y los objetivos departamentales.
6. La Institución no tiene control sobre la información o contenido que se accede desde Internet y no se hace responsable por el contenido.
7. Cualquier software o archivos descargados a través de Internet en la red de la Institución son propiedad de la Institución. Dichos archivos o software puede utilizarse sólo en formas que sean coherentes con sus licencias o derechos de autor.

Uso inapropiado

1. Los siguientes usos del internet proporcionado por la Institución no están permitidas:
 - Para acceder, cargar, descargar o distribuir material pornográfico o sexualmente explícito.
 - Violar la ley nacional, estatal o local.
 - Vandalismo o daños a la propiedad de cualquier otro individuo u organización.
 - Invadir o abusar la privacidad de los demás.
 - Violar Copyright o utilizar material intelectual sin permiso.
 - Utilizar la red para obtener ganancias financieras o comerciales.
 - Degradar o alterar el rendimiento de la red
2. Ningún funcionario puede utilizar instalaciones de la Institución conscientemente para descargar o distribuir software pirateado o datos. Está prohibido el uso del archivo de intercambio de software en equipos de la Institución y las redes de Institución.
3. Ningún funcionario puede utilizar servicios de Internet de la institución para propagar deliberadamente cualquier código de programa de virus, gusanos, caballos de Troya o trap-door.

Solicitud de servicios y/o accesos a páginas web específicas.

Para solicitar acceso a cualquier servicio de Internet, el funcionario interesado debe presentar el formulario detallado en *Anexo C 1.1.- Formulario para solicitar servicios de Internet*.

Es importante detallar nombre y firmas de las personas que autorizan.

I.5.- Políticas de Uso de Correo Electrónico

Propósito

El propósito de esta política es establecer directrices adecuadas para el correcto uso de la herramienta institucional denominada **correo electrónico**.

Alcance

Esta política se aplica a todos los servidores públicos, contratistas, consultores y personal temporal de la Institución.

Normas y Disposiciones Generales

El servicio de correo electrónico institucional y los recursos tecnológicos asociados al mismo, forman parte de los activos de información estratégicos del SNAI, razón por la cual es necesario establecer medidas de protección, y control de su uso legal, profesional y ético.

Toda la información contenida en los mensajes de datos y sus archivos adjuntos recibidos y/o transmitidos a través del correo electrónico institucional, por los servidores del SNAI o por personal externo, en cumplimiento de sus funciones laborales o contractuales, son de propiedad del SNAI

Normas de Uso, Protección y Control

1. El servicio y las cuentas de correo institucional que se encuentran bajo los dominios “@atencionintegral.gob.ec” y “@seguridadpenitenciaria.gob.ec”, son de propiedad del Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y a Adolescentes Infractores, y tienen como finalidad facilitar la gestión laboral de los servidores o personal externo, a quienes se les haya autorizado y habilitado este servicio.
2. El SNAI se reserva el derecho de habilitar o deshabilitar, ampliar o restringir el servicio de correo electrónico institucional, a los servidores o al personal externo, como medidas para asegurar el uso aceptable del servicio y la seguridad de la información institucional.
3. Para salvaguardar la información institucional contenida en el correo electrónico corporativo, el SNAI respaldará automáticamente todo correo electrónico entrante y saliente, así como sus archivos adjuntos.
4. La cuenta de correo electrónico institucional asignada a un servidor o personal externo, es personal e intransferible, en consecuencia, el usuario titular de la cuenta es responsable del uso que se le dé a la misma.

5. Las cuentas de correo electrónico asignadas a grupos, tienen el carácter de impersonal, sin embargo, el servidor o personal externo, a cuyo cargo se haya creado dicha cuenta, es responsable del uso que se le dé a la misma.
6. Cada cuenta de correo tendrá asociada una clave de acceso o contraseña para acceder al contenido de la misma. El usuario de la cuenta de correo será el responsable de la administración y custodia de dicha contraseña, garantizando la confidencialidad y privacidad de la misma; así como de tomar las acciones necesarias para evitar su difusión o conocimiento por parte de otros servidores o personas externas a la organización.
7. La contraseña usada para acceder al buzón de correo electrónico deberá seguir los estándares y normas de seguridad que determina la política de contraseñas a aplicar.
8. Los servidores o personal externo que hagan uso autorizado del correo electrónico institucional, están en la obligación de observar los compromisos y disposiciones establecidas en este documento.
9. Todo mensaje que sea enviado fuera de la Institución a través del servicio de correo electrónico institucional, deberá incluir una cláusula de confidencialidad que será configurada de forma automática; ésta permitirá advertir respecto a la confidencialidad de la información transmitida. El servidor o personal externo que emita un correo electrónico fuera de la institución, está en la obligación de mantener dicha cláusula en el texto del mensaje de datos.
10. El servidor o tercero podrá recibir o transmitir mensajes de datos no relacionados con el desempeño de sus funciones laborales, utilizando los recursos tecnológicos que el SNAI pone a su disposición, siempre y cuando los mensajes que se transmitan o reenvíen no contravengan las normas, políticas institucionales e indicaciones detalladas en este documento.
11. El contenido de los mensajes de datos personales transmitidos o reenviados, a través del correo electrónico institucional, es responsabilidad exclusiva del servidor o personal externo, en consecuencia asume los efectos legales que pudieran derivarse de dicha acción, sin perjuicio de las responsabilidades administrativas a que hubiere lugar

Autorización del Servicio

1. Todo funcionario cuyas funciones requieran la utilización de un computador y la correspondiente integración a la red informática institucional, se le habilitará por defecto el servicio de correo electrónico interno. El personal externo deberá solicitarlo expresamente para acceder a este servicio, en cumplimiento al procedimiento respectivo.

2. El reenvío de mensajes de datos a dispositivos móviles como un Smartphone, PDA's, Palm, etc., se autoriza por defecto a Coordinadores Generales, Directores y Asesores.

Para el acceso a este servicio por parte de los Jefes Departamentales y de Área, se seguirá el procedimiento de autorización por excepción respectivo.

3. El envío masivo de mensajes a través de la lista de distribución SNAI-TODOS u otras similares, se autoriza únicamente a través de las cuentas de correo asignadas al Ministro, Vice Ministros, Director de Secretaría Nacional, Casa Adentro, Cultura Organizacional, Personal de TIC encargado de notificar incidentes.
4. Para obtener acceso a este servicio por parte de los servidores del SNAI, se debe seguir el procedimiento de autorización por excepción respectivo, solamente en el caso de necesidad de comunicación con entidades públicas o privadas para tratar temas asociados a las funciones del cargo que desempeña el servidor solicitante

Uso Aceptable del Correo Electrónico Institucional

1. El uso del servicio de correo electrónico institucional, de manera general, está orientado para su utilización en los fines institucionales, en consecuencia, los servidores y personal externo deberán utilizarlo para el cumplimiento de sus funciones y responsabilidades asociadas a sus cargos, convenios o contratos relacionados con el SNAI.
2. Es aceptable el envío y recepción de mensajes de datos personales, siempre y cuando el contenido de los mismos no contravengan los compromisos, las políticas de seguridad, uso de computadores y demás disposiciones contempladas en este documento.

Usos no Permitidos

1. Almacenar, transmitir o reenviar mensajes de datos, incompatibles con los estándares éticos de los servidores del SNAI, y con las normas legales o reglamentarias aplicables.
2. Utilizar el servicio de correo electrónico institucional para divulgar o transmitir información institucional de propiedad del SNAI, a terceras personas u organizaciones no autorizadas para recibirla, salvo en los casos que exista una disposición expresa por escrito, por parte de las autoridades competentes de la Institución.
3. Transmitir información institucional considerada como confidencial, a través de mensajes de datos identificados como personales.
4. Enviar correos masivos por parte de todas aquellas personas que no estén explícitamente autorizadas para dicha actividad.

5. Adjuntar archivos con un tamaño mayor a 5120 KB (Kilobytes) en los mensajes de datos masivos o dirigidos a grupos de más de 20 usuarios.
6. Acceder a una cuenta de correo electrónico que pertenezca a otro servidor tercero, sin su autorización expresa o la de autoridad competente.
7. Ver y/o copiar los mensajes de datos de una cuenta de correo que pertenezca a otro servidor o tercero sin su autorización expresa o la de autoridad competente.
8. Alterar el contenido de los mensajes de datos recibidos de las cuentas de correo de otros servidores o terceros, para a su vez reenviar el correo alterado.
9. Enviar mensajes alterando la dirección electrónica del remitente para suplantar a terceros, identificarse como una persona ficticia o no identificarse.
10. Intentar vulnerar las seguridades del servicio de correo electrónico.
11. Usar frases o palabras obscenas, peyorativas, ofensivas o denigrantes en los mensajes de correo electrónico.
12. Utilizar el correo electrónico institucional para almacenar y, o transmitir la siguiente información y, o material:
 - Textos o imágenes pornográficas;
 - Material que promueva cualquier forma la explotación sexual, racismo o violencia;
 - Información que promueva el uso ilegal de drogas y/o armas;
 - Mensajes discriminatorios con relación a preferencias sexuales, raza, religión, nacionalidad, ideología o militancia política;
 - Material con contenido violento;
 - Material que promueva o posibilite juegos o apuestas;
 - Códigos destructivos (virus, programas que se auto replican, etc.) o material que facilite el cometimiento de delitos informáticos;
 - Cadenas de correos;
 - Propaganda partidista o política;
 - Propaganda comercial o gremial;
 - Material difamatorio, ofensivo o injurioso contra la honra de las personas;
 - Material intimidatorio;
 - Material ilegal como software sin licencia o violación de los derechos de autor.

Restricciones y Prohibiciones

1. La suspensión del servicio es una medida de prevención contra la repetición de acciones que puedan afectar los niveles de servicio o atentar contra los principios y valores plasmados en este documento.
2. La suspensión del servicio se aplicará para aquellos funcionarios o personal externo que hayan incurrido en mal uso del servicio, sin perjuicio de las sanciones administrativas, civiles o penales a las que hubiere lugar, si fuere el caso.
3. El área de Tecnologías de información y Comunicación, luego de verificar el mal uso del servicio de correo electrónico institucional, de ser el caso, podrá requerir la suspensión temporal del servicio de hasta 30 días calendario, al (los) usuario (s) incurso(s) en esta práctica. La suspensión por un tiempo mayor, estará a lo dispuesto por el Ministro.

Recomendaciones

1. El usuario tomará las medidas necesarias para proteger la información institucional adjunta al mensaje de datos, tales como contraseñas y, o encriptación que permitan abrir los archivos solamente a la persona autorizada.
2. En caso de requerir compartir archivos de forma masiva, con tamaño mayor a 500 KB, se recomienda abrir una carpeta compartida con acceso a los usuarios que se considere necesario.

Mecanismos De Control

El SNAI con el objetivo de preservar la integridad y el buen uso del correo electrónico institucional tienen y hará uso de la facultad de definir e implementar los mecanismos de control que considere necesarios, sin que éstos violen el Acuerdo de Confidencialidad de la Información, firmado entre los funcionarios y la Institución.

I.6.- Políticas de Uso de Software

Propósito

El propósito de esta política es establecer directrices adecuadas para el correcto uso del software terminal.

Alcance

Esta política se aplica a todos los servidores públicos, contratistas, consultores y personal temporal de la Institución, que utilicen equipos desktop o laptops asignados por la unidad de Bienes.

Normas y disposiciones generales

El decreto ejecutivo 1014 con fecha 10 de abril del 2008, dispone que:

Artículo 1.- *Establecer como política pública para las Entidades de la Administración Publica Central la utilización de Software Libre en sus sistemas y equipamientos Informáticos*

Artículo 2.- *Se entiende por Software Libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.*

Estos programas de computación tienen las siguientes libertades:

- a) Utilización del programa con cualquier propósito de uso común*
- b) Distribución de copias sin restricción alguna.*
- c) Estudio y modificación del programa (Requisito: código fuente disponible)*
- d) Publicación del programa mejorado (Requisito: código fuente disponible).*

Artículo 3.- *Las entidades de la Administración Publica Central previa a la Instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de este tipo de software*

Artículo 4.- *Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de Software Libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.*

Para efectos de este decreta se comprende como seguridad nacional, supervivencia de la colectividad y la defensa del patrimonio nacional.

Para efectos de este decreto se entiende por un punto de no retorno, cuando el sistema o proyecto informático se encuentre en cualquiera de estas condiciones:

- Sistema en producción funcionando satisfactoriamente y que un análisis de costo beneficio muestre que no es razonable ni conveniente una migración a Software Libre.*
- b) Proyecto en estado de desarrollo y que un análisis de costo - beneficio muestre que no es conveniente modificar el proyecto y utilizar Software Libre.*

Periódicamente se evaluarán los sistemas Informáticos que utilizan software propietario con la finalidad de migrarlos a Software Libre.

Artículo 5.- *Tanto para software libre como software propietario, siempre y cuando se satisfagan los requerimientos, se debe preferir las soluciones en este orden:*

- a) Nacionales que permitan autonomía y soberanía tecnológica.*
- b) Regionales con componente nacional.*
- c) Regionales con proveedores nacionales.*
- d) Internacionales con componente nacional.*
- e) Internacionales con proveedores nacionales.*
- f) Internacionales.*

Artículo 6.- *La Subsecretaría de Informática como órgano regulador y ejecutor de las políticas y proyectos Informáticos en las entidades del Gobierno Central deberá realizar el control y seguimiento de este Decreto.*

Para todas las evaluaciones constantes en este decreto la Subsecretaría de Informática establecerá los parámetros y metodología obligatorios

Artículo 7.- *Encárguese de la ejecución de este decreto los señores Ministros Coordinadores y el señor Secretario General de la Administración Pública y Comunicación.*

Normas de Uso, Protección y Control

1. Es obligatorio el uso de software libre.
2. El SNAI se reserva el derecho de habilitar o deshabilitar, desinstalar y/o modificar software al personal, como medidas para asegurar el uso aceptable del servicio y la seguridad de la información institucional.

3. Para salvaguardar la información institucional contenida en el equipo, el SNAI garantiza la implementación, actualización e instalación de software ANTIVIRUS.
4. Ningún funcionario está autorizado a instalar software en cualquier equipo de la Institución, salvo personal de TIC.
5. Para la instalación de cualquier software licenciado, el funcionario a través de su jefe inmediato solicitará al Director de TIC la factibilidad de dicho software o su equivalente en código abierto.
6. La Dirección de Tecnologías es la única entidad encargada de instalar software en cualquier equipo perteneciente al SNAI.

Mecanismos de Control

El SNAI con el objetivo de preservar la integridad y el buen uso del software institucional tienen y hará uso de la facultad de definir e implementar los mecanismos de control que considere necesarios, sin que éstos violen el Acuerdo de Confidencialidad de la Información, firmado entre los funcionarios y la Institución.

I.7.- Políticas de Respaldos y Entrega de Información para Salida de la Institución

Propósito

El propósito de esta política es establecer directrices adecuadas para el correcto manejo de respaldos de la información de los funcionarios que salen de la Institución.

Alcance

Esta política se aplica a todos los servidores públicos, contratistas, consultores y personal temporal de la Institución, que utilicen equipos desktop o laptops asignados por la unidad de Bienes y que se prestan a salir de la Institución.

Aspectos generales

Al ingresar al SNAI, cada funcionario cuenta obligatoriamente con un usuario y una contraseña tanto para correo electrónico como para el sistema de gestión documental Quipux, el respaldo de información se refiere a la información, productos, informes, memorandos, ayuda memorias, hojas de cálculo, bases de datos, alcances y todo documento generado por el funcionario.

Esta información será revisada por la persona encargada de firmar y aceptar los respaldos.

Normas de Uso, Protección y Control

1. Es obligatoria la entrega de respaldos de todo funcionario que termina su relación de dependencia con el SNAI.
2. Dicha información será entregada en un medio magnético, sea este CD, DVD o pendrive; si éstos están vacíos o no grabados, se informará inmediatamente para su correctivo.
3. Si la persona que solicita no utilizó en ningún momento un equipo de cómputo, se receptorá la hoja respectiva denominada “CUMPLIMIENTO DE OBLIGACIONES” y se detallara esta novedad en el campo “Observaciones”.
4. Para el respaldo de Quipux, el funcionario debe administrar sus propios respaldos en el sistema y solo en caso de inconvenientes coordinará con el responsable Institucional de dicho sistema, para generar los respaldos respectivos.
5. Esta información reposará en el área de la Dirección de Tecnologías quienes son los custodios de la información.
6. Para solicitar una “copia” de los respaldos de algún funcionario, ésta debe ser formal y enviada a la Dirección Administrativa para su aprobación.

7. UNA VEZ QUE EL FUNCIONARIO DE LA DIRECCIÓN DE TECNOLOGÍAS RECIBA Y FIRME EL DOCUMENTO DE SALIDA, SE DESACTIVAN LOS TRES USUARIOS (CUENTA DE INICIO DE SESION, CUENTA DE CORREO ELECTRÓNICO Y QUIPUX)
8. La cuenta de correo electrónico estará disponible para respaldos por un máximo de 30 días calendario.

Solicitud de Respaldos de Funcionarios que han Salido de la Institución

Para facilitar el respaldo de información de cualquier funcionario que ha salido de la institución, la persona solicitante presentará el formulario detallado en el *Anexo C 1.2.- Solicitud de Respaldos*.

Cualquier persona representante de empresa, consultora u otra Institución Pública que solicite acceso a información por cualquier razón, firmarán el acuerdo de confidencialidad detallado en el *Anexo C 1.3.- Acuerdo de Confidencialidad*.

Mecanismos De Control

El SNAI con el objetivo de preservar la integridad y el buen uso de la información institucional tienen y hará uso de la facultad de definir e implementar los mecanismos de control que considere necesarios, sin que éstos violen el Acuerdo de Confidencialidad de la Información, firmado entre los funcionarios y la Institución.

Archivos a Respaldar

El SNAI, a través de la Dirección de Tecnologías, respalda la información considerada “necesaria” y que están en las siguientes carpetas:

1. **Documentos**
2. **Imágenes**
3. **Descargas**
4. **Música**
5. **Video**
6. **Escritorio**
7. **Cualquier otra carpeta creada en particiones C:, D:, etc.**

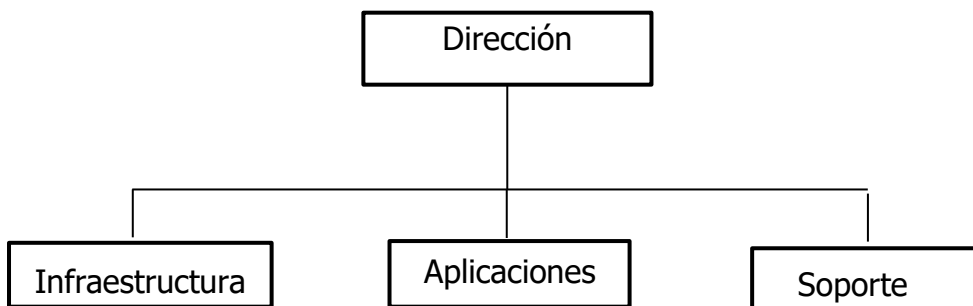
No se respaldará información personal considerada innecesaria:

- **Fotos personales**
- **Audio personales**
- **Videos personales**
- **Documentos personales**

CAPÍTULO 2.- ESTRUCTURA DEL ÁREA DE SISTEMAS



II. ESTRUCTURA DEL ÁREA DE SISTEMAS



II.1.- INFRAESTRUCTURA

Requerimientos de Usuarios

Define la necesidad técnica para la conectividad y comunicaciones, dentro de las cuales se encuentra:

1. Cableado estructurado.
2. Habilitación de áreas y redes.
3. Habilitación de Wireless.
4. Creación de puntos de red.
5. Conectividad y servicios continuos.
6. Restricción de navegación.
7. Creación de cuentas.
8. Cámaras web.

Responsable.- Coordinador de Infraestructura.

II.2.- DESARROLLO

Requerimientos de Usuarios

Mejoras continuas a los sistemas internos del SNAI, por ejemplo:

9. SGP (e-SIGPEN).
10. Mejora de conectividad.
11. Creación de nuevos módulos.
12. Soluciones integrales con otras instituciones.
13. Administración de Base de Datos.
14. Creación de usuarios de sistemas propios.
15. Nuevos sistemas dependiendo la necesidad institucional.

Responsable.- Coordinador de Aplicaciones.



II.3.- SOPORTE TÉCNICO

Requerimientos de Usuarios

Con la finalidad de administrar y supervisar la atención de solicitudes de soporte técnico, de tal forma que se proporcione a los funcionarios el apoyo informático (operación de los equipos, sistemas operativos o paquetes de software residentes en los mismos) para elevar la productividad de las áreas corporativas, se implementa el Soporte Tecnológico o la mesa de ayuda.

Estos requerimientos deberán ser solicitados de la siguiente manera:

1. **Herramienta “Soporte TICs” (GLPI).**- Para generar un ticket o dar seguimiento a uno ya generado, el funcionario deberá ingresar al siguiente link:

<http://soporte.atencionintegral.gob.ec/>

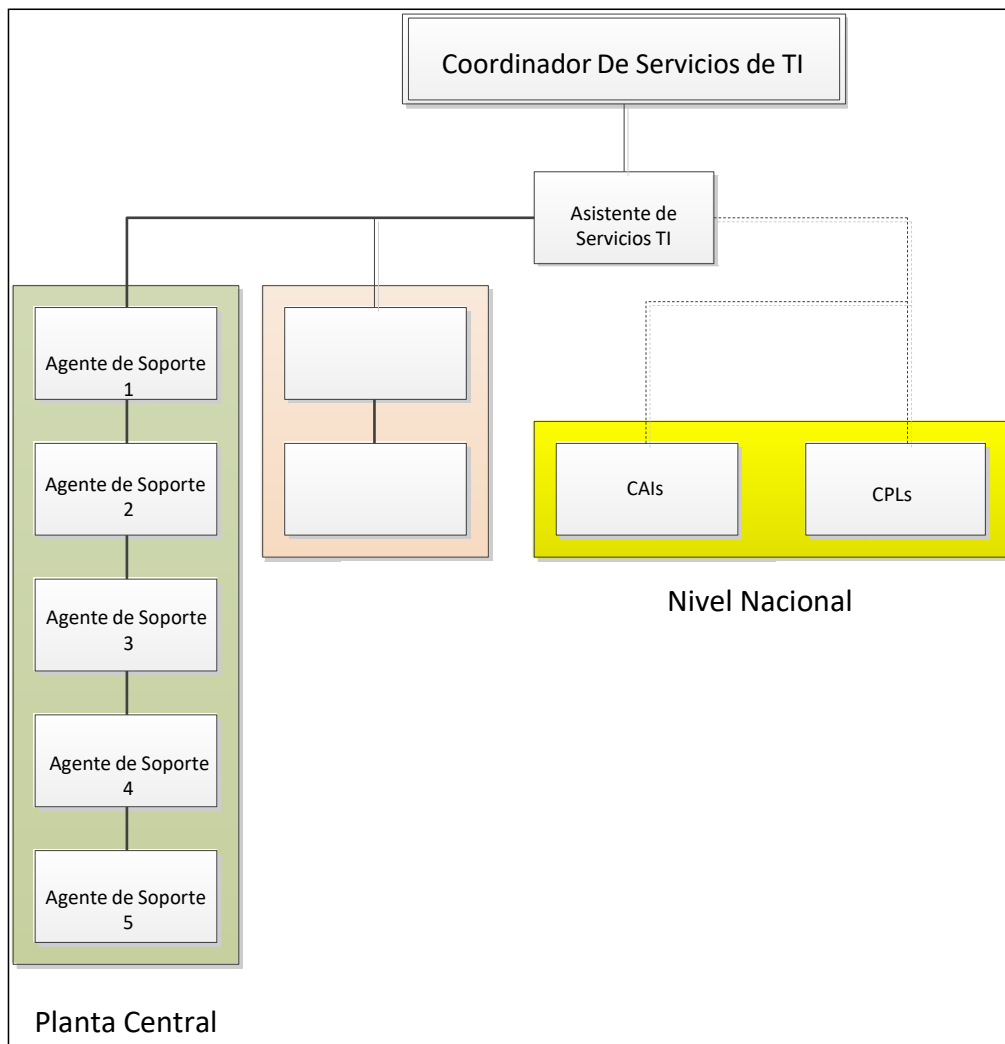
Para el ingreso el funcionario utilizará las mismas credenciales (usuario y clave) del computador asignado.

2. **eMail (Correo Electrónico).**- El funcionario que requiera un soporte técnico y no ha podido acceder a la Intranet a “Soporte TICs”, enviará un eMail a soporte@atencionintegral.gob.ec (en caso de la Regional Guayas #8: TIC.RGuayas@atencionintegral.gob.ec); automáticamente se generará un número de ticket con el cual puede dar seguimiento a su requerimiento en la página indicada anteriormente.

1. Se recomienda observar el video tutorial (<http://intranet.atencionintegral.gob.ec/snai/wp-content/uploads/2020/12/ExplicativoGLPI-1.wmv>) antes de “**Crear un Caso**” ya que el ticket debe contener información relevante para la resolución del mismo.
2. Si es posible, adjuntar una captura de pantalla como adjunto al ticket.
3. Detallar las acciones que se han realizado antes, durante y después del incidente.
4. Si el incidente es por factores externos, el agente de soporte técnico gestionará e informará a las áreas indicadas.

TODO REQUERIMIENTO SERÁ ATENDIDO OBLIGATORIAMENTE A TRAVÉS DE “SOPORTE TICS” (Aplicativo GLPI) o en caso necesario a través DEL CORREO ELECTRÓNICO: soporte@atencionintegral.gob.ec

Estructura:



Responsabilidades:

Del Coordinador de Servicios de TI:

1. Administrar la herramienta GLPI.
2. Generar informes mensuales de uso.
3. Generar informes mensuales de tickets atendidos, tiempos estimados, etc.
4. Generar informes mensuales y evaluación parcial.
5. Responder a través de la herramienta GLPI si se requiere una explicación sobre una incidencia.
6. Informar al funcionario que solicitó el soporte técnico, la razón del problema suscitado.
7. Informe mensual unificado.

Del Asistente de Servicios de TI:

8. Seguimiento a cada ticket generado a través de GLPI, su solución y cierre.

9. Recibir equipos necesarios.
10. Despachar equipos necesarios.
11. Receptar llamadas telefónicas y de ser el caso, generar el ticket respectivo.
12. Informe mensual de novedades.

De los agentes locales y zonales son responsables de:

13. Cerrar puntualmente los tickets indicando el proceso seguido para la solución del mismo.
14. Informar al funcionario que solicitó el soporte técnico, la razón del problema suscitado.
15. NO ATENDER NINGUN CASO SI NO ESTA REGISTRADO EN LA MESA DE AYUDA.
16. Informe mensualmente los casos atendidos.

Si bien en ciertos casos los agentes zonales no son parte de la Dirección de Tecnologías, se coordinará acciones con ellos para poder solventar incidencias que así lo requiera.

Ámbito de atención:

Rol	Nombre	Ámbito
Agente 1 PC	Martín Carlier	Local / Nacional
Agente 2 PC	<i>Vacante</i>	Local / Nacional
Agente 3 PC	<i>Vacante</i>	Local
Agente 4 PC	<i>Vacante</i>	Local
Agente 5 PC	<i>Vacante</i>	Local
Agente 1 12O	Stalin Morales	Local / Nacional
Agente 2 12O	<i>Vacante</i>	Local
Asistente	<i>Vacante</i>	Local
Coordinador	<i>Vacante</i>	Local / Nacional

PC: Planta Central.- Edificio Gral. Robles E3-33 entre Ulpiano Páez y 9 de Octubre

Tipos de Soporte – Soporte Técnico

17. **Problemas de Hardware** (Monitor, teclado, mouse, portátil, CPU, impresoras, equipos BlackBerry y Tablet pertenecientes a la Institución).
18. **Problemas de Software** (Windows, office, internet, virus, correo institucional, instalación de aplicaciones bajo autorización de ser el caso).
19. **Incidentes de primer orden** (Soporte in situ hardware y software, conectividad, internet).
20. **Requerimientos Puntuales** (Preparación de equipos informáticos, respaldos, generación de especificaciones técnicas, etc.).

Rol	Nombre
Principal	Agentes de Soporte
Back up	Coordinador de Servicios de TI

Tipos de Soporte – Aplicaciones de Gobierno

Sistema de Gestión Documental Quipux.

Rol	Nombre
Principal / Administración	Responsable Técnico Institucional
Back up / Administración	Coordinador de Servicios de TI
Soporte Técnico	Agente TI

- ✓ Problemas al ingresar al sistema.
- ✓ Problemas de usuario/clave.
- ✓ Apoyo cambio de contraseña.
- ✓ Problemas de funcionalidad, instalación de complementos.
- ✓ Instalación de firma electrónica.
- ✓ Apoyo solicitud de respaldos.
- ✓ Apoyo creación de ciudadanos.
- ✓ Apoyo visualización de borradores.

eSIGEF - SPRYN.

Rol	Nombre
Principal / Administración	Responsable Técnico Institucional
Back up / Administración	Coordinador de Servicios de TI
Soporte Técnico	Agente TI

- ✓ Problemas al ingresar al sistema.
- ✓ Problemas de usuario/clave.
- ✓ Apoyo cambio de contraseña.
- ✓ Problemas de funcionalidad, instalación de complementos.
- ✓ Impresión de documentos.



GPR.

Rol	Nombre
Principal / Administración	Responsable Técnico Institucional
Back up / Administración	Coordinador de Servicios de TI
Soporte Técnico	Líder GPR Institucional

- Problemas al ingresar al sistema.
- Problemas de usuario/clave.
- Apoyo cambio de contraseña.
- Problemas de funcionalidad, instalación de complementos.

S.G.P. (e-SIGPEN).

Rol	Nombre
Principal / Administración	Responsable Técnico Institucional
Back up / Administración	Coordinador de Servicios de TI
Soporte Técnico	Agente TI

- Problemas al ingresar al sistema.
- Problemas de usuario/clave.
- Apoyo cambio de contraseña.
- Problemas de funcionalidad, instalación de complementos.



CAPÍTULO 3.- S ERVICIO EXTENDIDO “O N C A L L”

III. SERVICIO EXTENDIDO DENOMINADO “ON CALL”

Objetivo

Brindar un servicio de Soporte Técnico para cualquier eventualidad fuera del horario de trabajo habitual, es decir, desde las 17:30 hasta las 18:30.

Modalidad:

1. La modalidad de “ON CALL” se ejecutará semanalmente entre los agentes de Soporte, comenzando en orden alfabético por apellido.
2. El agente de soporte asignado y de turno, prestará servicio de soporte técnico dentro del horario establecido, siempre respaldado en un ticket que demuestre el requerimiento solicitado.
3. De no existir ningún requerimiento, es responsabilidad de cada agente completar el horario extendido.
4. Si un agente de soporte no cumple el horario extendido por efectos de “ON CALL” sin justificación o permiso alguno, automáticamente repetirá su turno la semana siguiente.
5. Se incluye fines de semana y feriados.
6. AL finalizar la semana, el agente de soporte generará un informe de actividades en relación al servicio “ON CALL” adjuntando los respaldos de tickets para el pago de horas extras.
7. Es importante que el agente de turno tenga contacto con los demás administradores tanto de infraestructura como de aplicaciones.
8. La única línea que atenderá dentro del servicio “ON CALL” será la extensión 750.

MODELO RACI

	<div> <div>Agente de Soporte - PC</div> <div>Agente de Soporte - 120</div> <div>Coordinador de Servicios de TI</div> <div>Desarrollador</div> <div>Coordinador de Desarrollo</div> <div>Agente de Infraestructura</div> <div>Coordinador de Infraestructura</div> <div>Asistente de Servicios de TI</div> <div>Director de Tecnologías</div> </div>							
Hardware	R	R	A					
Software	R	R	A					C
Internet	R	R				C		
Correo electrónico	R	R				C		I
Aplicaciones				R	A			I
Red						R	A	I
Informes Técnicos	R	R	A					I
Ap - Quipux	I	I				R	A	
Ap - e-SIGPEN	I	I		R	A			

R: RESPONSABLE

A: APROBADOR

C: CONSULTADO

I: INFORMADO

CAPÍTULO 4.- PROPUESTA “GREEN IT”

IV. PROPUESTA “GREEN IT”

Que es “Green IT”

Así como en todos los ámbitos se debe perseguir la finalidad de NO contaminación y preservación del medio ambiente, la informática y tecnología son un ámbito que deben trabajar fuertemente para evitar los daños que ocasiona.

Sumado a esta contaminación que el sector tecnológico produce, está la creciente y constante expansión que tiene, donde la demanda y uso de computadores aumentan a diario, incrementando el número de fabricación de estos, llevando, consecuentemente, a una mayor y peligrosa contaminación sino se comienzan a tomar medidas eficientes y ecológicas en este sector.

A raíz de esto nace “Green IT”, la cual procura investigaciones en Tecnologías de Información, TI, y el uso eficiente y ecológico de las mismas, en las diversas etapas del “ciclo de vida” de éstas; desarrollo, producción, uso y eliminación.

Así es como en el desarrollo se deben seguir lineamientos en pos del medio ambiente, en la producción se deben emplear métodos de producción ecológicos, el uso también debe ser ecológico, y los residuos, por ejemplo los computadores viejos, deben ser eliminados en forma correcta y ecológica.

Aplicación de “Green IT” en el Servicio Nacional de Atención Integral a Personas Adultas Privadas de la Libertad y a Adolescentes Infractores

El SNAI está ligada al 100% con el uso de tecnología y equipos de cómputo en cada uno de los ámbitos laborales y no es productora de componentes y/o partes de equipos, en ese sentido, la aplicación de “Green IT” se aplica en el ciclo de uso, adquisición y eliminación de las tecnologías.

El término de “Green IT” comenzó a utilizarse después de que la agencia de protección ambiental (EPA, por sus siglas en inglés) de los estados unidos desarrollara el programa de estrella de energía en el año de 1992, diseñado para promover y reconocer la eficiencia energética de diversas tecnologías como computadoras, monitores y aires acondicionados. La EPA cuenta con una herramienta que funciona en internet con la que se puede realizar una evaluación ambiental de productos electrónicos (EPAT) y que sirve para seleccionar y evaluar computadoras de escritorio, laptops y monitores en base a sus características ambientales. los productos EPEAT están diseñados para reducir el consumo de energía, disminuir las actividades de mantenimiento y permitir el reciclaje de materiales incrementando su eficiencia y tiempo de vida de los productos computacionales.

En la actualidad se utiliza una gran cantidad de energía eléctrica para que puedan operar los diferentes equipos de cómputo, desde estaciones de trabajo hasta grandes servidores y los diferentes suministros necesarios como los data centers que los alojan, el aire acondicionado, la iluminación, ups, racks, entre otros, esto con el fin de satisfacer las demandas de información de los usuarios.

De acuerdo a lo anterior se hace evidente la necesidad de implementar medidas para el ahorro de energía. Esto puede empezar desde la simple acción de apagar un equipo que no se está utilizando (ya que según Johna Till Johnson, presidente de Nemertes Research la simple acción del apagado puede resultar en un decremento en cerca del 50% del consumo energético por cada 100 servidores) hasta la implementación de procesadores ahorradores de energía que utilizan el algoritmo dvfs (dynamic voltage and frequency scaling).

Gran cantidad de energía eléctrica es necesaria para que puedan operar los diferentes equipos de cómputo, desde estaciones de trabajo hasta grandes servidores y los diferentes suministros necesarios como los data centers que los alojan, el aire acondicionado, la iluminación, UPS, racks, entre otros, esto con el fin de satisfacer las demandas de información de los usuarios. Hoy día las empresas consumidoras y productoras de equipos de cómputo, preocupadas por mejorar este aspecto, están tomando acciones para la reducción del consumo de energía, esta es una de las principales metas de las Tecnologías Verdes.

Datos a tomar en cuenta

1. La vida media de un ordenador se ha reducido de seis años en 1997 a dos años en el 2005.
2. 30% de la potencia que utiliza un ordenador convencional se desperdicia porque el equipo se deja encendido cuando no se utiliza.
3. La producción de un solo ordenador requiere 1,7 toneladas de materias primas y agua.
4. Cada vez que un empleado trabaja desde casa utilizando la TI, se ahorra transporte y por lo tanto, emisiones de CO2.
5. Cada vez que un regulador de energía inteligente controlado por TI apaga luces, baja la calefacción o desconecta el aire acondicionado, se ahorran emisiones de CO2.
6. Cada vez que una empresa o el sector público producen de forma más eficiente con la ayuda de la TI, se ahorran emisiones de CO2.
7. Cada vez que se sustituyen catálogos, anuncios impresos y cartas con sus equivalentes electrónicos, se ahorran emisiones de CO2.

Propuesta de la Dirección de Tecnologías de Información y Comunicaciones

- a. **Computación en Nube (Clouding).**- La computación en nube es una solución integral en la cual todos los recursos informáticos (hardware, software, sistemas de redes, almacenamiento, etc.) son brindados a los usuarios de manera rápida según lo que determina la demanda. Los recursos o servicios que se brindan son controlables a fin de asegurar cuestiones tales como la alta disponibilidad, la seguridad y la calidad. Permite tener acceso a servidores, espacio de almacenamiento y software, sin que se disponga de equipos sofisticados para soportarlos.

- b. **Computación GRID.-** Tecnología que permite utilizar de forma coordinada todo tipo de recurso (entre ellos cómputo, almacenamiento y aplicaciones específicas) que no están sujetos a un control centralizado. En este sentido es una forma de computación distribuida, en la cual los recursos pueden ser heterogéneos (diferentes arquitecturas, supercomputadores, clústeres....) y se encuentran conectados mediante redes de área extensa (por ejemplo Internet).

“La Grid” es una malla que enlaza recursos computacionales tales como PC, estaciones de trabajo, servidores, elementos de almacenamiento, y provee los mecanismos necesarios para acceder a ellos.

- c. **Virtualización.-** Tecnología que comparte los recursos de cómputo en distintos ambientes permitiendo que corran diferentes sistemas en la misma máquina física. Crea un recurso físico único para los servidores, el almacenamiento y las aplicaciones.

La virtualización de servidores permite el funcionamiento de múltiples servidores en un único servidor físico. Si un servidor se utiliza a un porcentaje de su capacidad, el hardware extra puede ser distribuido para la construcción de varios servidores y máquinas virtuales.

La virtualización ayuda a reducir la huella de carbono del centro de datos al disminuir el número de servidores físicos y consolidar múltiples aplicaciones en un único servidor con lo cual se consume menos energía y se requiere menos enfriamiento. Además se logra un mayor índice de utilización de recursos y ahorro de espacio.

- d. **SaaS.- (Software as a Service)** es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de la Institución, a los que se accede con un navegador web desde un cliente, a través de Internet.

La Dirección de TIC se ocupa del servicio de mantenimiento, de la operación diaria y del soporte del software usado por el usuario. Regularmente el software puede ser consultado en cualquier computador, se encuentre presente en la Institución o no. Se deduce que la información, el procesamiento, los insumos, y los resultados de la lógica de negocio del software, están hospedados en la Dirección de TIC.

- e. **Evaluación del Consumo de Energía del Parque Informático.-** Para reducir el consumo de energía se debe evaluar las necesidades del parque informático.

Cada componente de un ordenador debe ser tomado en cuenta.

1. El procesador: a mayor potencia mayor consumo de energía.
2. La tarjeta gráfica: Las tarjetas gráficas comunes son ideales para la ofimática. Sin embargo, otras actividades requerirán tarjetas más potentes.
3. El monitor: De preferencia pantallas LCD con bajo consumo de energía.

- f. **Programación de Puesta en Reposo de los Computadores.-** Configurar la puesta en reposo de los computadores en función de un periodo preciso de inactividad:
1. Puesta en reposo después de 10 minutos de inactividad
 1. Puesta en reposo prolongada después de 30 minutos de inactividad.
 2. Permite poner en reposo el sistema operativo del PC guardando los datos en el disco rígido, como política de seguridad.
- g. **ECO Responsabilidad con el Uso de Impresiones.-** Según un estudio de IPSOS (Empresa Española Líder en Investigación de Mercado a Través de Encuestas) del año 2008, el 16% de las páginas impresas nunca son leídas!

Ante este indicador, la Dirección de Tecnologías propone implementar las siguientes soluciones:

2. Prohibir el uso sistemático de la impresora, implementar sistemas de auditoría de impresión.
 3. Configurar el modo blanco/negro y anverso/reverso por defecto de la impresora.
 4. Deshabilitar la impresión a color, salva ciertas excepciones.
 5. Utilizar la vista previa antes de imprimir.
 6. Preferir un sistema de impresoras colectivas en lugar de impresoras individuales.
 7. Reutilizar el papel impreso en una cara como borrador.
 8. De preferencia utilizar papel reciclado.
 9. Implantar una verdadera política de colecta del papel para su posterior reciclaje.
- h. **Adquirir Equipos ECO lógicos.-** Cuando se adquiera equipos informáticos (computadoras, escáner, impresoras...), opte por fabricantes que cuenten con un sello ecológico. Estos fabricantes se comprometen a respetar ciertas normas de respeto del medio ambiente en la fabricación de sus productos.
- Algunos fabricantes de equipo informático cumplen con las normas de logotipos ecológicos. El más conocido de estos logotipos es **Energystar**, que garantiza que los equipos han sido diseñados para ahorrar energía
- i. **Establecer Políticas de Reciclaje de Equipos.-** En la mayoría de casos, la distribución de equipos a nivel interno no se la realiza con la opinión técnica de la Dirección de TIC, esto es que, en ciertos casos, a tareas de carga liviana asignan equipos de poca capacidad y viceversa. Se debe analizar muy bien el trabajo al cual van a ser utilizados los equipos a fin de priorizar y administrar los recursos de manera sistemática.

Así mismo, si un equipo es dado de baja porque tiene algún componente dañado, esto no significa que todos los componentes no funcionen, se debe aplicar políticas de reutilización de componentes como monitores, memorias RAM, discos internos, fuentes de poder, drives, etc.

Si el equipo es inutilizable, se debe contactar con empresas especializadas en el reciclaje de desechos electrónicos, a veces, considerados tóxicos a causa de sus componentes.

Todo esto, dentro del marco legal que rige en el **REGLAMENTO GENERAL DE BIENES DEL SECTOR PUBLICO, Art 79, Capítulo VIII, DE LAS BAJAS.**

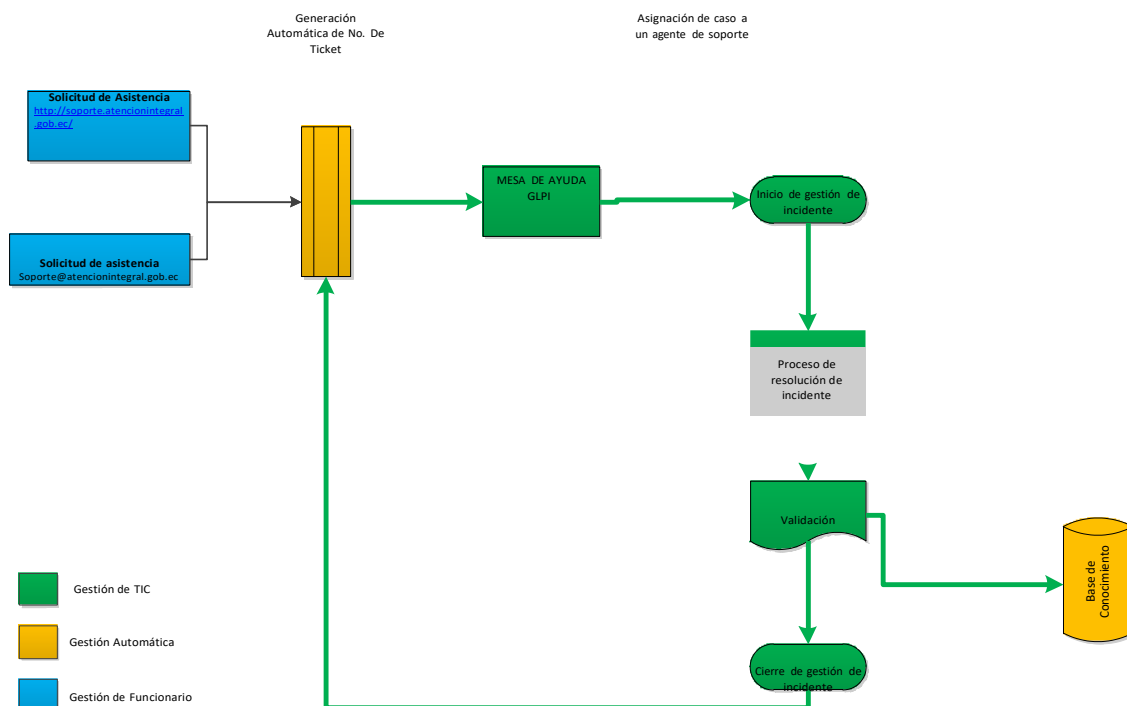
CAPÍTULO 5.- PROCESOS

V. PROCESOS

A.1: Soporte Técnico

Responsable: Agente de Soporte
BackUp: Coordinador de Servicios de TI

1. Cualquier dependencia, funcionario o unidad administrativa para reportar un incidente o solicitar soporte técnico, debe “Crear un Caso” dentro de “Soporte TICs” de la Intranet (<http://soporte.atencionintegral.gob.ec/>) o enviar a soporte@atencionintegral.gob.ec un correo explicando con lujo de detalles todos los factores, acciones y/o resultados que han ocasionado dicha incidencia y las tareas realizadas hasta ese momento.
2. La herramienta GLPI genera automáticamente un No. de ticket y se asigna a un agente el caso dependiendo su naturaleza.
3. El agente de soporte realiza el soporte técnico, dependiendo de la naturaleza de la misma, gestiona los correctivos necesarios para solventar el incidente.
4. El agente de soporte documenta el incidente y alimenta la Base de Conocimiento, verifica resultado y cierra el caso.



A.2: Creación de Usuario y Correo Electrónico

Responsable: Administrador de servidores

BackUp: Coordinador de Servicios de TI

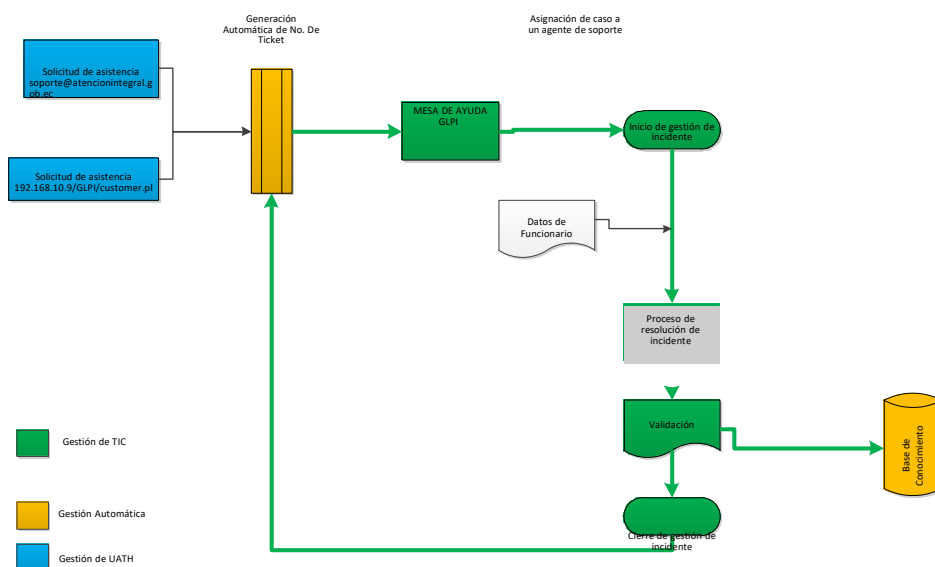
a) La Dirección de Administración de Talento Humano DATH, envía a soporte@atencionintegral.gob.ec con copia al eMail del administrador de servidores y administrador de Quipux un correo solicitando la creación del funcionario con los siguientes datos:

- Cédula de ciudadanía.
- Apellidos.
- Nombres.
- Título profesional.
- Abreviatura de Título profesional.
- Área a la que pertenece.
- Grupo Ocupacional.
- Puesto.
- eMail.
- Nombre del jefe inmediato.

Esta información es enviada en un archivo de hoja de cálculo.

b) Una vez creado el usuario, se direcciona la creación en Quipux.

c) Una vez creado el usuario en Quipux, se notifica a la DATH.

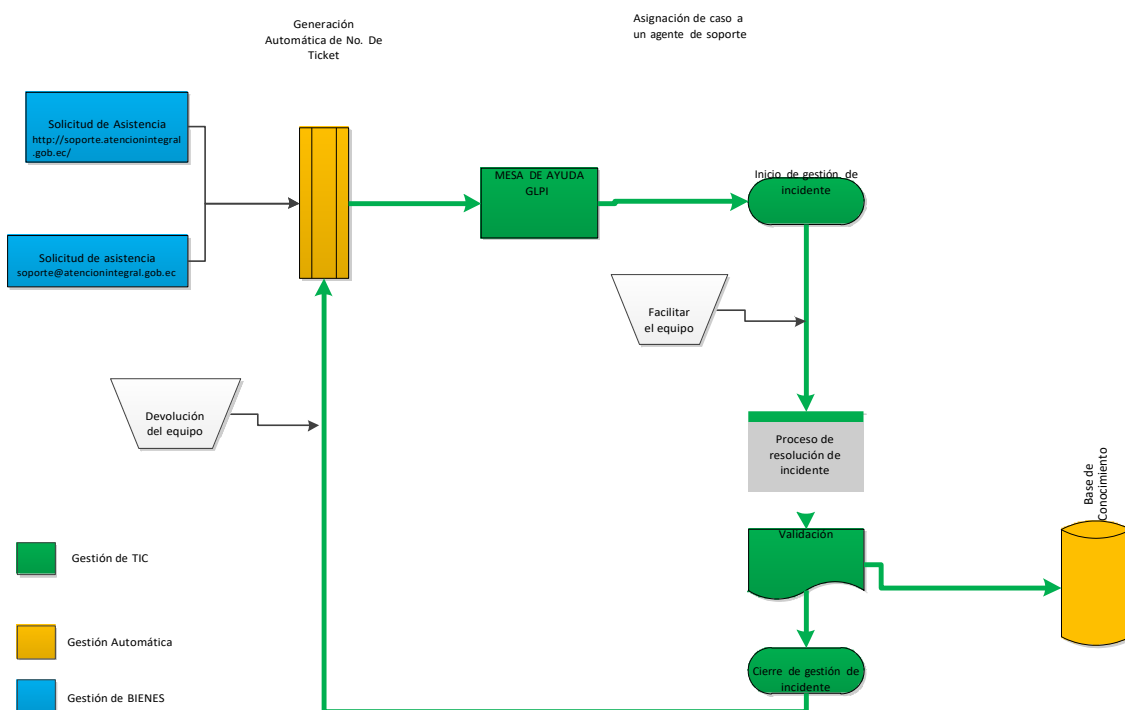


A.3: Preparación y Asignación de Equipos Informáticos

Responsable: Coordinador de Servicios de TI

BackUp: Agente de Soporte

- La Unidad de Administración de Bienes, “Crea un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI envía a soporte@atencionintegral.gob.ec un correo solicitando la adecuación del equipo, así mismo, facilita el mismo al área de TIC.
- La herramienta GLPI genera automáticamente un No. de ticket y se asigna a un agente el caso dependiendo su naturaleza.
- El personal procede a realizar la revisión del equipo y si el usuario ya ha sido creado, lo configura en el equipo caso contrario, el equipo queda preparado pero no configurado.
- Una vez configurado el equipo, el área de TIC lo devuelve al área de Bienes para su asignación, esta acción cierra el ticket.

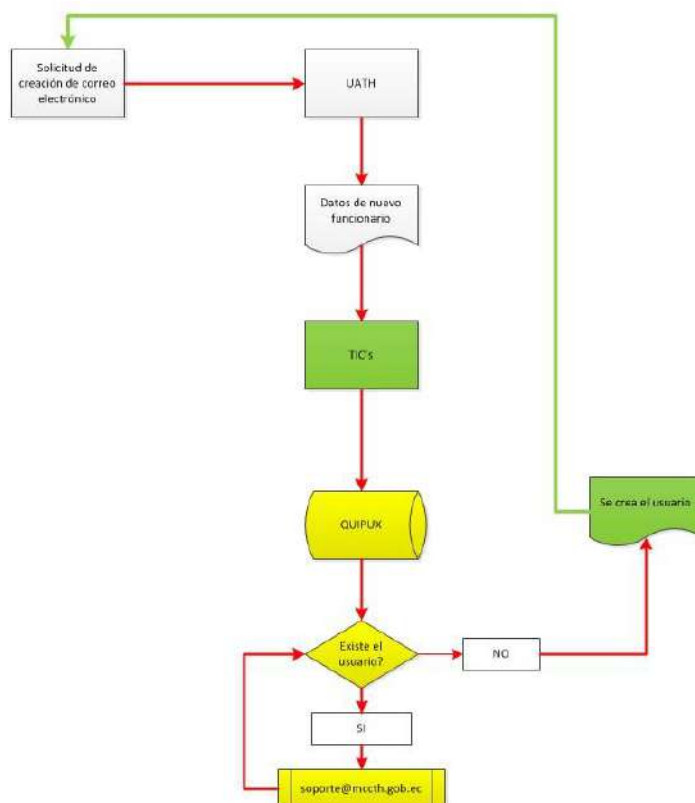


A4: Sistema de Gestión Documental OUIPUX

A.4.1: Creación de Usuario

Responsable: Administrador Quipux
BackUp: Coordinador de Servicios de TI

1. Cuando ya se ha creado el usuario y correo electrónico, se envía los datos al administrador Quipux quien procede a crear al funcionario.
2. Se valida que el usuario no este creado en otra institución gubernamental, si da el caso, “Crear un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI se envía un eMail a soporte@gobiernoelectronico.gob.ec solicitando la deshabilitación del mismo.
3. Una vez creado el usuario Quipux, le llegará al funcionario que solicito la creación de la cuenta un eMail para cambio de contraseña.
4. Es responsabilidad de cada funcionario el manejo del sistema Quipux, manejo de sus claves y manejo de sus funcionalidades.

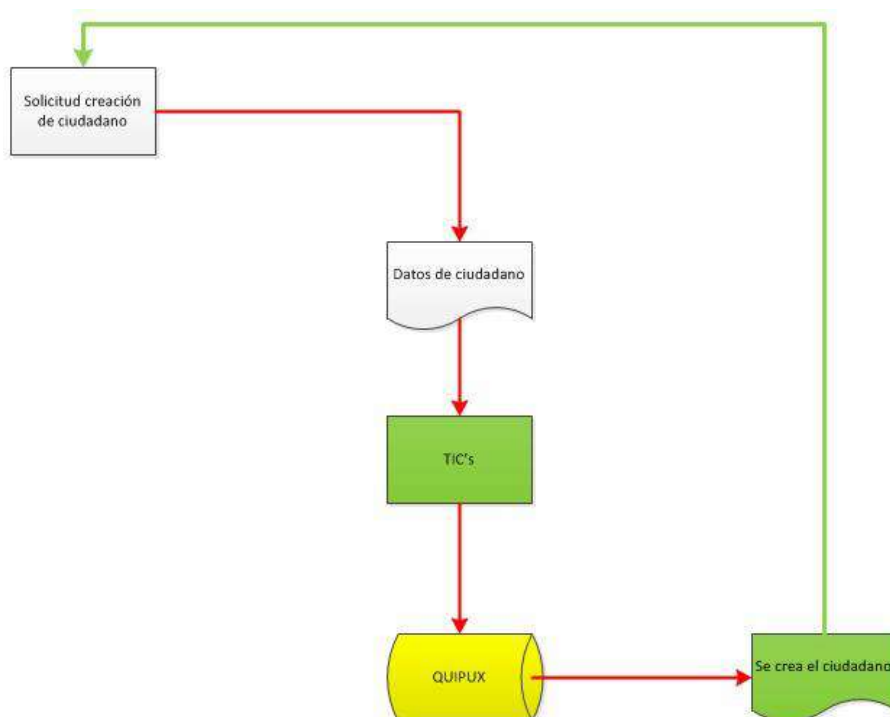


A4: Sistema de Gestión Documental OUIPUX

A.4.2: Creación de Ciudadanos

Responsable: Administrador Quipux
BackUp: Coordinador de Servicios de TI

1. El usuario interesado “Crea un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI envía un correo a soporte@atencionintegral.gob.ec con por lo menos los siguientes datos del ciudadano a crear, una vez validado que no existe en Quipux:
 - a. Nombres completos.
 - b. Institución a la que pertenece.
 - c. Cargo.
 - d. Ciudad.
2. El área de Gestión de TIC genera el requerimiento en el orden en que estos lleguen, tomándolos a todos por igual como “urgentes”.
3. Se crea el ciudadano siguiendo los pasos destinados para este objeto.
4. Una vez creado el ciudadano en Quipux, se notifica al funcionario el resultado del proceso.
5. Es responsabilidad de cada funcionario verificar que el ciudadano a ser creado no este creado anteriormente.

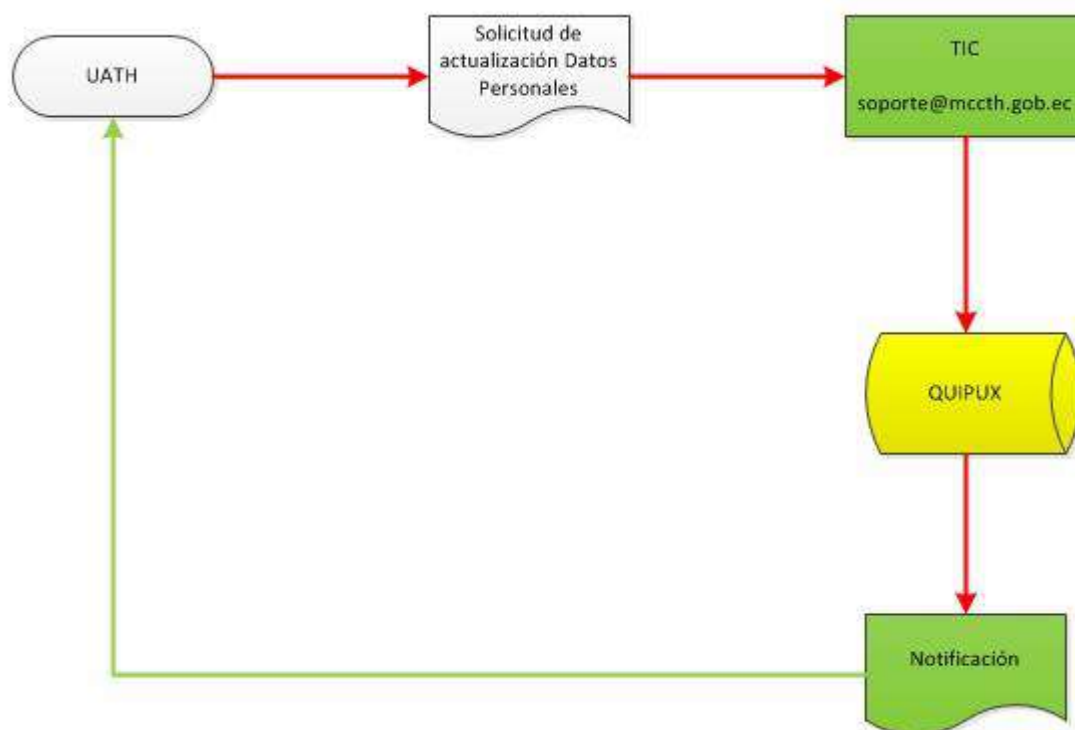


A4: Sistema de gestión documental OUIPUX

A.4.3: Cambio de datos personales/profesionales

Responsable: Administrador Quipux
BackUp: Coordinador de Servicios de TI

1. La Dirección de Administración de Talento Humano (DATH) “Crea un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI envía un correo a soporte@atencionintegral.gob.ec detallando los datos del usuario al cual se realizará la actualización
2. El área de Gestión de TIC genera el requerimiento en el orden en que estos lleguen, tomándolos a todos por igual como “urgentes”.
3. Se actualizan los datos solicitados en el usuario indicado.
4. Se notifica al funcionario el resultado del proceso.





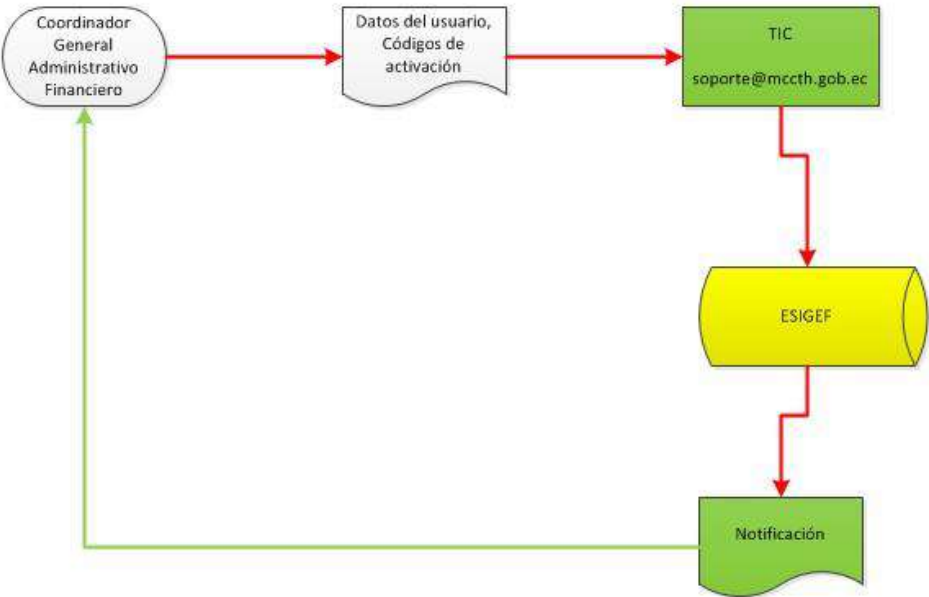
A.5: Sistema de Gestión Documental ESIGEF

A.5.1: Creación de Usuario / Activación de Códigos

Responsable: Administrador ESIGEF
BackUp: Coordinador de Servicios de TI

1. La Coordinación Administrativa Financiera a través de su Coordinador o de la Dirección Financiera “Crea un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI envía a soporte@atencionintegral.gob.ec un correo solicitando la creación del usuario en el sistema ESIGEF adjuntando los siguientes datos
 - a. Nombres completos.
 - b. No. de cédula de ciudadanía.
 - c. Título profesional.
 - d. Códigos de activación.
2. El área de Gestión de TIC genera el requerimiento en el orden en que estos lleguen, tomándolos a todos por igual como “urgentes”.
3. Se crea el usuario en el sistema ingresando los datos y códigos indicados.
4. Una vez creado el usuario ESIGEF, se notifica al Coordinador Administrativo a través de un correo indicando la creación satisfactoria para su posterior activación.
5. Es responsabilidad de cada funcionario el manejo del sistema ESIGEF, manejo de sus claves y manejo de sus funcionalidades.





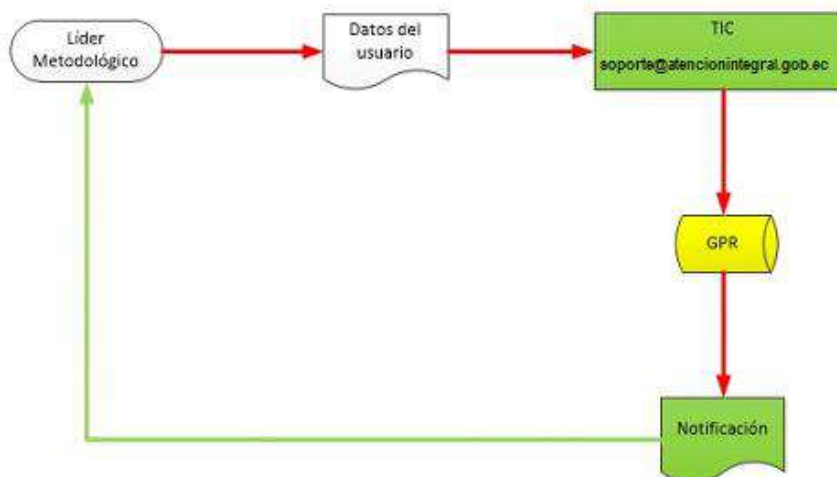
A.6: Sistema de Gestión por Resultados GPR

A.6.1: Creación de Usuario

Responsable: Administrador Técnico GPR

BackUp: Coordinador de Servicios de TI

- El líder metodológico “Crear un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI envía a soporte@atencionintegral.gob.ec un correo solicitando la creación del usuario en el sistema ESIGEF adjuntando los siguientes datos
 - Nombres completos.
 - No. de cédula de ciudadanía.
 - Título profesional.
- El área de Gestión de TIC genera el requerimiento en el orden en que estos lleguen, tomándolos a todos por igual como “urgentes”.
- Se crea el usuario en el sistema ingresando los datos y códigos indicados.
- Una vez creado el usuario GPR, se notifica al Líder Metodológico a través de un correo indicando la creación satisfactoria para su posterior activación.
- Es responsabilidad de cada funcionario el manejo del sistema GPR, manejo de sus claves y manejo de sus funcionalidades.



A.7: Sistema de Gestión Penitenciaria SGP

A.7.1: Creación de usuario

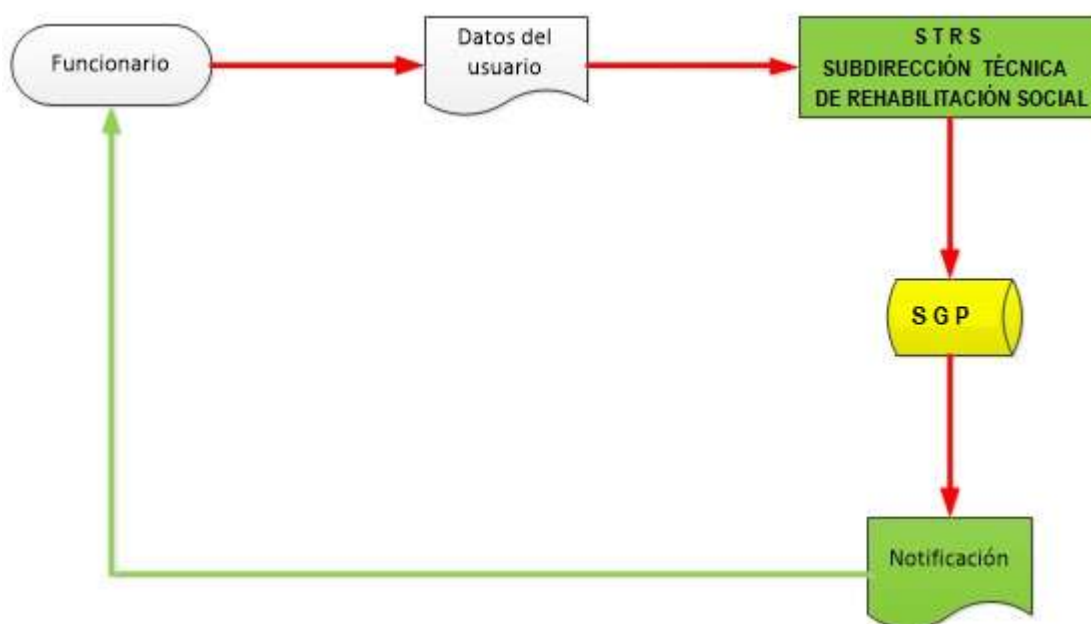
Responsable: Administrador SGP
BackUp: Coordinador de Servicios de TI

- El Funcionario envía vía Quipux a la Subdirección Técnica de Rehabilitación Social (STRS), solicitando la creación del usuario en el sistema SGP adjuntando la siguiente información:

- Acuerdo de Confidencialidad SGP
- Permisos SGP

Formularios que se pueden encontrar en
http://intranet.atencionintegral.gob.ec/snai/?page_id=1358

- El área de Gestión de TIC genera el requerimiento en el orden en que estos lleguen, tomándolos a todos por igual como “urgentes”.
- Se crea el usuario en el sistema ingresando los datos y códigos indicados.
- Una vez creado el usuario en el SGP, se notifica al Funcionario a través de un correo indicando la creación satisfactoria para su posterior activación.
- Es responsabilidad de cada funcionario el manejo del Sistema SGP, manejo de sus claves y manejo de sus funcionalidades.



A.8 Sistema Oficial de Contratación Pública

A.8.1: Creación de Usuario como Entidad Contratante

Responsable: Funcionarios Área Compras Públicas

1. Aceptación de Términos de Uso y Condiciones de Privacidad en el Portal (www.compraspublicas.gob.ec)
2. Registro de Información General:
 - Usuario
 - Contraseña
 - Confirmación de Contraseña
 - Correo Electrónico
3. Ingreso de Información de la Persona
Datos de la Institución Compradora
 - RUC
 - Razón Social
 - Nombre Comercial
 - Página web
 - Año Inicio de actividadesDatos del Representante Legal
 - Apellido Paterno
 - Apellido Materno
 - Primer Nombre
 - Segundo Nombre
 - Sexo
 - Estado Civil
 - Documento de Identificación
 - Número de Identificación
 - Cargo
 - Nivel de Educación
 - Área de Especialidad
 - Fecha de Nacimiento
4. Ingreso de Dirección y Teléfono
 - Calle
 - Intersección
 - Número
 - Edificio
 - Departamento
 - Provincia
 - Canton
 - Parroquia
 - Ciudad
 - Teléfonos
6. Finalización de Registro



A.9: Sistema Integrado de Planificación e Inversión Pública - SIPeIP

A.9.1: Creación de Usuario / Activación de Códigos

Responsable: Administrador SIPeIP
BackUp: Coordinador de Servicios de TI

La Dirección de Planificación, Inversión, y Seguimiento de Planes, Programas y Proyectos, será el responsable del manejo del Sistema Integrado de Planificación e Inversión Pública – SIPeIP, para lo cual coordinará la generación y actualización de las claves de acceso para la utilización de este sistema en base a las directrices detalladas por parte de la Secretaría Técnica Planifica Ecuador y que son las siguientes:

1. El representante legal o máxima autoridad de la institución, remitirá la petición escrita de creación, entrega o deshabilitación de una credencial lógica (usuario y contraseña) del Usuario/a Principal. Esta solicitud debe ser remitida al Coordinador/a de Información, con copia al Director/a de Tecnologías de la Información de Planifica Ecuador, adjuntando la siguiente documentación:
 - Copia/s del nombramiento, contrato o algún otro documento habilitante.
 - Acuerdo de Responsabilidad por el uso de medios o servicios electrónicos.
 - Ficha de creación de Usuario/a.
 - Copia de cedula de identidad
2. La solicitud de creación y deshabilitación de usuarios/as con perfil secundario y básico debe ser realizado por el/la Usuario/a Principal de la institución a la dirección electrónica: ayuda@planificacion.gob.ec, adjuntando:
 - Acuerdo de Responsabilidad por el uso de medios o servicios electrónicos
 - Ficha de creación de Usuario/a.
 - Copia de cedula de identidad.
3. El restablecimiento de la contraseña de los Usuarios/as Principales, Secundarios y Básicos deberá ser solicitado, a través de correo electrónico dirigido a ayuda@planificacion.gob.ec, por parte del usuario Principal.
4. Mesa de servicios de TI de la STPE, mediante correo electrónico notifica la creación del usuario en el sistema SIPeIP para acceder al sistema para su activación.
5. Es responsabilidad de cada funcionario el manejo del sistema SIPeIP, manejo de sus claves y manejo de sus funcionalidades.



CAPÍTULO 6.- MANUAL DE PROCEDIMIENTOS

VI. MANUAL DE PROCEDIMIENTOS


B.1: RespalDOS

Responsable: Agentes de soporte
Requerimiento: Ticket de mesa de ayuda / Quipux


- a) El responsable de toda la información almacenada, respaldada y/o extraída del equipo indicado es el AGENTE DE SOPORTE encargado de realizar dicha tarea.
- b) Para el respaldo de datos se debe respaldar desde el perfil de **ADMINISTRATOR**
- c) Las carpetas a ser respaldada son:



- d) Se debe respaldar imágenes, audio y videos pertenecientes o de importancia para el SNAI.
- e) **NUNCA** se respaldará fotos, canciones, películas, software que sean de carácter “personal”.
- f) Al respaldar los perfiles, se debe constatar que no exista información fuera de dicho perfil como en el disco C y en otra partición.
- g) La información respaldada debe estar almacenada en una carpeta con el siguiente formato: “*id_de_usuario ip_de_equipo*”, ejemplo:

 moncayog 192.168.4.69

- h) De ser posible y necesario, generar un archivo comprimido en el mismo formato.

 moncayog 192.168.4.69

- i) **EL CUSTODIO DE LA INFORMACIÓN RESPALDADA ES EL AGENTE QUE LA GENERA, DEBE SER ALMACENADA EN LOS DISCOS EXTERNOS Y/O EL SERVIDOR ASIGNADO A ESA TAREA.**

B.2: Generación de Informe Técnico

Responsable: Agentes de soporte
Requerimiento: Ticket de mesa de ayuda / Quipux

1. Para la generación de informe técnico es necesario que el/los equipo/s en mención se encuentren en el Departamento de Tecnología o en su defecto en el SNAI.
2. Si el equipo pertenece a alguna zonal y no se cuenta con personal técnico “*in situ*”, se coordinará la visita técnica respectiva.
3. EL informe es generado por Quipux con los siguientes parámetros:

PARA: *Funcionario que solicita la revisión e informe técnico.*

DE: *Director de Tecnologías de la Información y Comunicaciones*

COPIA: *Administrador de Bienes*

4. El informe debe contener los siguientes formatos:

ANTECEDENTES: *Se debe citar No. De ticket y/o No. De Memorando, fecha, requerimiento, datos del equipo:*

UNIDAD	FUNCIONARIO	DISPOSITIVO	MARCA	MODELO	No. SERIE	CODIGO	ESTADO

TRABAJO REALIZADO: *Detalle de todas las acciones realizadas desde pruebas de funcionamiento, revisión física, revisión de partes internas, etc.*

CONCLUSIONES: *Después de las revisiones realizadas, definir en la conclusión el fallo encontrado.*

RECOMENDACIONES: *Que acciones el SNAI debe tomar para solventar el incidente encontrado, de ser el caso, mantenimiento por parte de empresas especializadas, cambio de partes y piezas, reposición de equipo completo y la baja de activos.*

5. Una vez emitido el informe, el equipo en mención será devuelto al usuario custodio.

B.3: Preparación de equipo

B.3.1: Equipo nuevo

Responsable: Agentes de soporte
Requerimiento: Ticket de mesa de ayuda / Quipux

1. Instalación y/o explotación de Sistema Operativo Original.
2. Instalación de drivers necesarios
 - a. Video
 - b. Audio
 - c. Red (*Ethernet y Wireless*)

- d. Bios
 - e. USB
 - f. Todos los adicionales
3. Crear usuario local **ADMINISTRADOR** ó **SNAI** y configurar la clave local
4. Ingreso de máquina a DOMINIO *minjusticia-ddhh.int*
 - a. El nombre de equipo es designado por Administrador Active Directory.
 - b. La IP es asignado por el Administrador Active Directory.
5. Iniciar sesión como **ADMINISTRATOR**
6. Instalar los programas básicos: ([\\192.168.1.20\Instaladores\Basicos](#))
 - a. Adobe Reader
 - b. Firefox
 - c. Flash Player para IE
 - d. Flas Player para other systems
 - e. LibreOffice
 - f. Spark
 - g. Winrar
 - h. OCS
 - i. Cualquier otro adicional siempre que se tenga la autorización respectiva (Office, Autocad, ArcGis, CS)
7. Instalar antivirus: ([\\192.168.1.115\TICs\Antivirus](#))
 - a. Instalar NetAgent_10.0.3361
 - b. Instalar KES_10.1.0.867
8. Instalar las impresoras necesarias para su normal funcionamiento, dependiendo de la ubicación del servidor público ([\\192.168.1.115\TICs\Instaladores\Drivers](#))
9. Iniciar sesión como **FUNCIONARIO**
10. Configurar navegadores con proxy (<http://192.168.1.115\TICs\proxycfg.js>)
11. Predeterminar las páginas de inicio:
 - a. Internet Explorer
 - i. intranet.atencionintegral.gob.ec
 - ii. <https://mail.atencionintegral.gob.ec/>
 - b. Firefox
 - i. intranet.atencionintegral.gob.ec
 - ii. <https://mail.atencionintegral.gob.ec>
 - iii. www.gestiondocumental.gob.ec
12. Notificar a la Unidad de bienes y entregar el equipo configurado, probado y listo.

B.3.2: Equipo en uso

Responsable: Agentes de soporte
Requerimiento: Ticket de mesa de ayuda / Quipux

Evaluar el funcionamiento del equipo, desinstalar todos los programas adicionales que no tengan que interferir en el trabajo cotidiano.

Si el equipo no está operativo y necesita formatear:

- ✓ Respalidar TODOS los perfiles creados de acuerdo al **Anexo B.1.1: RESPALDOS** numeral 5.
- ✓ Proceder a formatear el equipo tomando en cuenta:
 - a. Si el equipo es antiguo, el S.O. será Windows XP o Windows 7 32 bits.
 - b. Si son máquinas actuales cuya memoria RAM es de 4 GB o superior, el S.O. será Windows 7 64 bits.
- ✓ Seguir los pasos detallados en el **Anexo B.1.3.1: Equipos nuevos**, numeral 2.

Si el equipo está operativo y no necesita formatear:

- ✓ Validar la contraseña local de **ADMINISTRADOR**
- ✓ Iniciar sesión como **ADMINISTRATOR**
- ✓ Instalar y/o desinstalar el software de acuerdo a las disposiciones emitidas en el **Anexo B.1.3.1: Equipos nuevos**, numeral 6.
- ✓ Iniciar sesión como **FUNCIONARIO**
- ✓ Configurar navegadores con proxy (<http://192.168.1.115/TICs/proxycfg.js>)
- ✓ Predeterminar las páginas de inicio:
 - Internet Explorer
intranet.atencionintegral.gob.ec
<https://mail.atencionintegral.gob.ec>
 - Firefox
intranet.atencionintegral.gob.ec
<https://mail.atencionintegral.gob.ec>
www.gestiondocumental.gob.ec
- ✓ Notificar a la Unidad de bienes y entregar el equipo configurado, probado y listo.



B.4: Habilitación de Puntos de Red

Responsable: Agentes de soporte
Requerimiento: Ticket de mesa de ayuda / Quipux

1. Verificar la factibilidad de la instalación del punto de red en el área solicitada.
2. Ubicar el switch o router más cercano.
3. Desde este equipo hasta el punto final se debe temprar el cable, dejando en ambas puntos alrededor de 50 cm como provisión.
4. Procurar evitar curvaturas de 45° y/o juntar el cable de datos con cable eléctrico.
5. Para interiores usar canaleta decorativa, **NO DEJAR EL CABLE EXPUESTO.**
6. El cable debe estar desde el origen de la red, un conector RJ45 y la terminación un cajetín con Jack RJ45 o en su defecto un conector RJ45 directamente.
7. El punto debe ser etiquetado en las dos puntas.
8. Realizar prueba de conectividad, testar de seguimiento.
9. Una vez instalado el punto de red, instalar el equipo a utilizar el servicio.
10. Terminado todo el proceso, informar.

Materiales Requeridos:

1. Cable UTP categoría 5E o 6A
2. Conectores RJ-45 categoría 5E o 6A
3. Jack categoría 5E o 6A
4. Canaleta de piso (simple y dobles)
5. Canaleta de pared (simple y doble)
6. Cinta doble faz
7. Tester
8. Ponchadora RJ-45
9. Ponchadora de impacto





B.5: Restricciones

Responsable: Agentes de soporte
Requerimiento: Ticket de mesa de ayuda / Quipux

Equipos

1. No se puede configurar equipos ajenos al SNAI, como son:
 - a. Portátiles
 - b. PC de escritorio
 - c. Tablets
 - d. SmarthPhone
 - e. Impresoras

Software

1. No se puede instalar software licenciado dentro de los equipos del SNAI sin que estén debidamente adquiridos y registrados.
2. Es deber de la Dirección de Tecnologías, facilitar soluciones Open Source, así como su respectiva inducción.



CAPÍTULO 7.- FORMULARIOS



C.2: Formulario para Solicitar Carpetas Compartidas

Entrega:

Solicita:

Jefe inmediato Aprobado:

Técnico responsable

Funcionario Autorizado:

Director de Tecnologías:

SNAI		FORMULARIO NO. SNAI-DTIC 002		EL GOBIERNO DE TODOS	
PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y ADOLESCENTES INFRACTORES		CARPETAS COMPARTIDAS			
Fecha de la Solicitud: _____					
DATOS DE CARPETA COMPARTIDA					
Carpeta Existente	<input type="checkbox"/>	Nombre de Carpeta Existente:	_____		
		(Máximo 25 caracteres)			
Carpeta Nueva	<input type="checkbox"/>	Nombre de Carpeta Nueva:	_____		
		(Máximo 25 caracteres)			
Responsable de Carpeta Compartida: _____					
PERSONAS QUE TENDRÁN ACCESO		TIPOS DE PERMISO			
		LECTURA	ESCRITURA		
OBSERVACIONES (PARA USO DE TIC)					

<input type="checkbox"/> Ubicar Unidad Organizacional (Para uso de Tecnología)					
FIRMAS DE RESPONSABILIDAD					
ÁREA REQUIRIENTE					
_____			_____		
SOLICITADO POR			AUTORIZADO POR		
			Firma Jefe Inmediato		
			Nombre: _____		
NOTA: LA FIRMA DE AUTORIZACIÓN CONLLEVA RESPONSABILIDAD EN RELACIÓN AL USO DE LOS RECURSOS CONCEDIDOS, CUALQUIER MAL USO DE ÉSTOS SERÁ NOTIFICADO PARA LOS FINES PERTINENTES.					
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (Con Sello)					
_____			_____		
AGENTE DE SOPORTE			DIRECTOR TIC		

C.3: Formulario para Solicitar Desarrollo de Software

Entrega: Técnico responsable
Solicita: Funcionario Autorizado:
Jefe inmediato Aprobado: Director de Tecnologías:

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A
PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD
Y A ADOLESCENTES INFRACTORES



FORMULARIO NO. SNAI-DTIC 003

Área Requiriente: ...

Sistema: ...

Nuevo desarrollo / Modificación: ...

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A
PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD
Y A ADOLESCENTES INFRACTORES



Información General

TÍTULO:
SUBTÍTULO:
VERSIÓN:
AUTORES:

Elaboración, Revisión y Aprobación Funcional

ELABORADO POR:	NOMBRE:	
	CARGO:	
	ÁREA:	
FECHA:		FIRMA:

Revisión Técnica (No llenar – Información de la CGPGE)

ELABORADO POR:	NOMBRE:	
	CARGO:	
	ÁREA:	
FECHA:		FIRMA:

ELABORADO POR:	NOMBRE:	
	CARGO:	
	ÁREA:	
FECHA:		FIRMA:

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A
PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD
Y A ADOLESCENTES INFRACTORES



Contenido

1.	Nombre del Aplicativo a Crear	1
1.1	Breve Descripción	1
2.	Definiciones, Acrónimos, Abreviaturas	1
3.	Actores	1
4.	Precondiciones	1
5.	Flujo de Eventos Funcionalidades	1
5.1	Flujo Básico Funcionalidades Requeridas	1
5.2	Sub-Flujos	1
5.2.1	SF01	1
5.2.2	SF02	1
5.2.3	SF03	1
5.3	Flujos Alternos	1
6.	Reglas del Negocio	1
7.	Requerimientos Especiales	1
8.	Pos condiciones	1
9.	Relaciones	1
10.	Modelamiento	1
11.	Anexos	1

C.4: Formulario para Solicitud de Respaldos

Entrega:




Solicita:

Jefe inmediato Aprobado:

Técnico responsable

Funcionarios Autorizado:

Director de Tecnologías:

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES INFRACTORES		  
FORMULARIO NO. SNAI-DTIC 004 SOLICITUD DE RESPALDOS		
Fecha de la Solicitud (dd/mm/y) _____		
DATOS PERSONALES DEL FUNCIONARIO SOLICITANTE		
Nombres Completos: _____		
Apellidos Completos: _____		
Área: _____		
Puesto: _____		
Cargo: _____		
Solicitado a través de:		
Correo Electrónico	<input type="checkbox"/>	_____
Llamada Telefónica	<input type="checkbox"/>	_____
Ticket	<input type="checkbox"/>	_____
Otro	<input type="checkbox"/>	_____
RESPALDOS SOLICITADOS DE:		
Nombres Completos: _____		
Apellidos Completos: _____		
Área: _____		
Puesto: _____		
Cargo: _____		
RESPALDOS ENTREGADOS EN:		
DVD	<input type="checkbox"/>	_____
Impreso	<input type="checkbox"/>	_____
USB / Disco Externo	<input type="checkbox"/>	_____
Otro	<input type="checkbox"/>	_____
Es importante que el funcionario solicitante FACILITE los medios para el respaldo		
DETALLE DE LA INFORMACIÓN ENTREGADA		

FIRMAS DE RESPONSABILIDAD		
ÁREA REQUIRIENTE (Con Sello)		

SOLICITADO POR		AUTORIZADO POR
_____		Firma Jefe Inmediato
		Nombre: _____
NOTA: LA FIRMA DE AUTORIZACIÓN CONLEVA RESPONSABILIDAD EN RELACIÓN AL USO DE LOS RECURSOS CONCEDIDOS, CUALQUIER MAL USO DE ÉSTOS SERÁ NOTIFICADO PARA LOS FINES PERTINENTES.		
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (Con Sello)		

AGENTE DE SOPORTE		DIRECTOR TIC
_____		_____

C.5: Acuerdo de Confidencialidad SGP




Entrega: Responsables de información
Recibe: Personal en General
Aprobado: Director de Tecnologías

<p>SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES INFRACTORES</p>	  																
<p>FORMULARIO N° SNAI-DTIC 005 Nro. SNAI-DTIC-AC-_____</p> <p>SISTEMA DE ADMINISTRACIÓN DEL SECTOR PÚBLICO</p> <p>ACUERDO DE RESPONSABILIDAD DE SEGURIDAD DE LA INFORMACIÓN PARA EL ACCESO AL SISTEMA DE GESTIÓN PENITENCIARIA (SGP)</p>																	
<p>Yo, _____ con cédula de ciudadanía _____ en calidad de funcionario de _____ perteneciente a la Subdirección Técnica _____ mediante formulario de Creación de Usuarios y Permisos "SGP" (SNAI-DTIC 001), solicito accesos al Sistema para ingreso y consumo de datos, por lo que suscribo el presente Acuerdo de Responsabilidad de Seguridad de la información para el acceso al Sistema Gestión Penitenciaria del SNAI, que se detalla a continuación:</p>																	
<p>CLÁUSULA PRIMERA. - OBJETO:</p> <ol style="list-style-type: none">El acceso al SGP será exclusivamente para propósitos de trabajo, el mal uso del usuario y la clave asignada es estrictamente responsabilidad del funcionario a cargo, la información que se genere en el Sistema será solo para funcionarios.El SNAI puede revisar cualquier información que se haya generado en cualquier momento que lo requiera del usuario y clave que se me ha sido asignado.																	
<p>CLÁUSULA SEGUNDA. - OBLIGACIONES:</p> <ol style="list-style-type: none">Seré responsable de no divulgar, revelar ni alterar la clave personal, información confidencial, procedimiento, formatos y demás aspectos técnicos y administrativos que se generen dentro del sistema, derivados de la entrega del usuario y clave institucional, para proteger la información contra uso no autorizado o incorrecto, aun después que haya terminado mi relación laboral con la institución a la cual pertenezco.La clave es un mecanismo importante para la protección de los sistemas y aplicaciones, por lo cual se entiende que su manejo es personal e intransferible y acuerdo no divulgar la(s) clave(s) de acceso asignada a ninguna persona.Los privilegios del Usuario solicitados, me facultarán para ejecutar actividades como:																	
<ul style="list-style-type: none">• Dactiloscopia• Inicio / Libertad• Jurídico• Laboral• Educativo• Estadística• Sanciones• Trabajo Social• Director• Consultas	<table border="0" style="width: 100%;"><tr><td style="width: 50%;"><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td><td style="width: 50%;"><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td></tr><tr><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td></tr><tr><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td></tr><tr><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td></tr><tr><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td></tr><tr><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td></tr><tr><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td></tr><tr><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td><td><div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div></td></tr></table>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>
<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>																
<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>																
<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>																
<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>																
<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>																
<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>																
<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>																
<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>	<div style="border-bottom: 1px solid black; height: 15px; width: 100%;"></div>																

Página 1 de 2

C.6: Solicitud de Atención Incidente en Sistema SGP (Modificación)




Entrega: Técnico responsable
Solicita: Responsable de Carpeta / Jefe departamental
Aprobado: Director de Tecnologías

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES INFRACTORES				
FORMULARIO Nro. SNAI-DTIC 006				
SOLICITUD DE ATENCIÓN INCIDENTE DEL SISTEMA "SGP"				
Fecha de la Solicitud (dd-mm-yyyy) _____				
DATOS DE USUARIO				
Nombre Completo de Solicitante: _____				
Nombre del Centro o Dependencia: _____				
Área a la que Pertenece: _____				
Jefe Inmediato: _____				
Fecha del incidente: _____				
Número Prontuario: _____				
Nombre PPL: _____				
EJES DE INFORMACIÓN				
INGRESOS	<input type="checkbox"/>	SEGURIDAD	<input type="checkbox"/>	
TRASLADO	<input type="checkbox"/>	VISITA	<input type="checkbox"/>	
DACTILOSCOPIA	<input type="checkbox"/>	LABORAL	<input type="checkbox"/>	
JURIDICO	<input type="checkbox"/>	OTRO	<input type="checkbox"/>	
EDUCATIVO	<input type="checkbox"/>			
DETALLE DEL INCIDENTE				
Colocar prontuario, delito, centro origen, dato(s) actual, dato(s) nuevo, descripción del incidente				
Causa del Incidente : Digitación <input type="checkbox"/> Documentación Incorrecta <input type="checkbox"/> Red <input type="checkbox"/> Sistema <input type="checkbox"/>				
(Analista TIC's del centro)				

FIRMAS DE RESPONSABILIDAD				
AREA REQUIRIENTE				
SOLICITADO POR				
DIRECTOR				
Firma y Sello				
Nombre: _____				
APROBADO				
Subdirección Técnica de Rehabilitación Social - Planta Central				
Nombre: _____				
NOTA: LA FIRMA DE AUTORIZACIÓN CONLLEVA RESPONSABILIDAD EN RELACIÓN AL IMPACTO QUE TENGA LA MODIFICACIÓN DE DATOS SOLICITADA SOBRE EL PROCESO DEL PPL				
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (Con Sello)				
Analista TICs Centro				
Nombre: _____				
Analista TIC's Planta Central				
Nombre: _____				
DIRECTOR/A TIC				
Nombre: _____				




C.7: Solicitud de Usuario y Permisos SGP

Entrega: Técnico responsable
Solicita: Responsable de Carpeta / Jefe departamental
Aprobado: Director de Tecnologías

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES INFRACTORES				
FORMULARIO Nro. SNAI-DTIC-007 SOLICITUD DE USUARIO Y PERMISOS "SGP"				
Fecha de la Solicitud (dd-mm-yyyy) _____				
DATOS DE USUARIO				
Creación de Usuario:	<input type="checkbox"/>	Nombre de Solicitante:	_____	
Extender Permisos:	<input type="checkbox"/>	Máximo 25 caracteres)	_____	
Inhabilitar Usuario:	<input type="checkbox"/>	Centro o Dependencia:	_____	
Suspender Permiso:	<input type="checkbox"/>	rea a la que Pertenece:	_____	
Jefe Inmediato que Autoriza la Solicitud: _____				
ROLES (Un rol por Usuario)				
INGRESO / DACTILOSCOPIA	<input type="checkbox"/>	SANCIONES	<input type="checkbox"/>	
INICIO / LIBERTAD	<input type="checkbox"/>	TRABAJO SOCIAL	<input type="checkbox"/>	
JURIDICO	<input type="checkbox"/>	DIRECTOR	<input type="checkbox"/>	
LABORAL	<input type="checkbox"/>	CONSULTAS	<input type="checkbox"/>	
EDUCATIVO	<input type="checkbox"/>	SECRETARIA	<input type="checkbox"/>	
ESTADISTICA	<input type="checkbox"/>			
Motivos para Brindar los Permisos (Solicitante)				
_____ _____ _____ _____ _____				
FIRMAS DE RESPONSABILIDAD AREA REQUIRIENTE				
_____ SOLICITADO POR		_____ DIRECTOR/A Firma y Sello Nombre: _____		
_____ APROBADO Subdirección Técnica de Rehabilitación Social - Planta Central Nombre: _____				
NOTA: LA FIRMA DE AUTORIZACIÓN CONLLEVA RESPONSABILIDAD EN RELACIÓN AL USO DE LOS RECURSOS CONCEDIDOS, CUALQUIER MAL USO DE ÉSTOS SERÁ NOTIFICADO PARA LOS FINES PERTINENTES.				
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (Con Sello)				
_____ AGENTE DE SOPORTE		_____ DIRECTOR/A TIC		

C.8: Solicitud de Usuario y Permisos ALFRESCO

Entrega: Responsables de información
Recibe: Personal en General
Aprobado: Director de Tecnologías

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES INFRACTORES				
FORMULARIO Nro. SNAI-DTIC-008 SOLICITUD DE USUARIO Y PERMISOS "ALFRESCO"				
Fecha de la Solicitud (dd-mm-yyyy) _____				
DATOS DE USUARIO				
Creación de Usuario:	<input type="checkbox"/>	Nombre de Solicitante:	_____	
Extender Permisos:	<input type="checkbox"/>	Máximo 25 caracteres)	_____	
Inhabilitar Usuario:	<input type="checkbox"/>	Centro o Dependencia:	_____	
Supender Permiso:	<input type="checkbox"/>	rea a la que Pertenece:	_____	
Jefe Inmediato que Autoriza la Solicitud: _____				
ROLES				
CONTRIBUIDOR	<input type="checkbox"/>	COORDINADOR	<input type="checkbox"/>	<input type="checkbox"/>
COLABORADOR	<input type="checkbox"/>	EDITOR	<input type="checkbox"/>	<input type="checkbox"/>
CONSUMIDOR	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Motivos para Brindar los Permisos (Solicitante)				

FIRMAS DE RESPONSABILIDAD ÁREA REQUIRIENTE				
SOLICITADO POR		DIRECTOR/A Firma y Sello		
		Nombre: _____		
APROBADO Planta Central				
Nombre: _____				
NOTA: LA FIRMA DE AUTORIZACIÓN CONLLEVA RESPONSABILIDAD EN RELACIÓN AL USO DE LOS RECURSOS CONCEDIDOS, CUALQUIER MAL USO DE ÉSTOS SERÁ NOTIFICADO PARA LOS FINES PERTINENTES.				
DIRECCIÓN DE TECNOLOGÍAS (Con Sello)				
AGENTE DE SOPORTE		DIRECTOR/A DTIC		

C.9: Acuerdo de Confidencialidad ALFRESCO

Entrega: Responsables de información
Recibe: Personal en General
Aprobado: Director de Tecnologías

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A
PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD
Y A ADOLESCENTES INFRACTORES

Lenín

Trabaja con Mito

EL GOBIERNO
DE TODOS

FORMULARIO N° SNAI-DTIC 009

Nro. SNAI-DTIC-AC-_____

SISTEMA DE ADMINISTRACIÓN DEL SECTOR PÚBLICO

ACUERDO DE RESPONSABILIDAD DE SEGURIDAD DE LA INFORMACIÓN PARA EL ACCES AL SISTEMA DE SEGURIDAD PENITENCIARIO

Yo, _____ con cédula de
ciudadanía _____ en calidad de funcionario de
_____, perteneciente a (digitar Área Administrativa)
_____, mediante formulario de Creación de
Usuarios y Permisos "ALFRESCO", solicito accesos al Sistema para ingreso y consumo de datos,
por lo que suscribo el presente Acuerdo de Responsabilidad de Seguridad de la Información
para el acceso al Sistema Gestión Documental ALFRESCO del SNAI, que se detalla a
continuación:

CLÁUSULA PRIMERA. - OBJETO:

1. El acceso a ALFRESCO será exclusivamente para propósitos de trabajo, el mal uso del usuario y la clave asignada es estrictamente responsabilidad del funcionario a cargo, la información que se genere en el Sistema será solo para funcionarios.
2. El SNAI puede revisar cualquier información que se haya generado en cualquier momento que lo requiera del usuario y clave que se me ha sido asignado.

CLÁUSULA SEGUNDA. - OBLIGACIONES:

1. Seré responsable de no divulgar, revelar ni alterar la clave personal, información confidencial, procedimiento, formatos y demás aspectos técnicos y administrativos que se generen dentro del sistema, derivados de la entrega del usuario y clave institucional, para proteger la información contra uso desautorizado o incorrecto, aun después que haya terminado mi relación laboral con la institución a la cual pertenezco.
2. La clave es un mecanismo importante para la protección de los sistemas y aplicaciones, por lo cual se entiende que su manejo es personal e intransferible y acuerdo no divulgar la(s) clave(s) de acceso asignada a ninguna persona.
3. Los privilegios del Usuario solicitados, me facultarán para ejecutar actividades como:

- Contribuidor _____
- Colaborador _____
- Coordinador _____
- Editor _____
- Consumidor _____

Página 1 de 3

CAPÍTULO 8.- SLA

**SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS
ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES
INFRACTORES**



**ACUERDO DE NIVEL DE SERVICIO (SLA)
MESA DE AYUDA.**

**DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIÓN**

Diciembre 2020

Versión 2.0

Elaborado por: Juan Carlos Muñoz Mejía - DTIC

DEFINICIONES Y OBJETIVOS

El presente acuerdo tiene como finalidad:

Definir el Acuerdo de Niveles de Servicio (SLA) “Service Level Agreement” entre la DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES a quien en adelante se lo define como DTIC y todos los funcionarios pertenecientes a esta Cartera de Estado, el cual describe los objetivos de desempeño y disponibilidad.

Proporcionar una mayor visibilidad y conocimiento de los **Servicios de la mesa de ayuda** que demandan los funcionarios para su normal desempeño.

Conocer los alcances, limitaciones y responsabilidades tanto de la DTIC como del funcionario.

Los objetivos de desempeño y disponibilidad serán los parámetros medibles de la relación DTIC - funcionario, y podrán estar sujetos a revisiones continuas.

RELACION DTIC – FUNCIONARIO

El SLA descrito en este documento establece un acuerdo entre DTIC y el FUNCIONARIO, a través de la provisión de canales para el Servicio de Mesa de Ayuda y cuyo sistema servirá para la implementación de los servicios contratados para uso exclusivo de DTIC (GLPI).

GRUPOS DE TRABAJO

La DTIC establecerá un Grupo de Trabajo, cuyas tareas serán:

Soporte Técnico (Help Desk)

Problemas de Hardware (Monitor, teclado, mouse, portátil, CPU, impresoras, equipos BlackBerry y tabletas **pertenecientes a la Institución**).

Problemas de Software (Windows, office, internet, virus, correo institucional, instalación de aplicaciones bajo autorización de ser el caso).

Incidentes de primer orden (Soporte in situ hardware y software, conectividad, internet).

Requerimientos Puntuales (Preparación de equipos informáticos, respaldos, generación de especificaciones técnicas, etc.).

Soporte Técnico Infraestructura

Cableado estructurado.

Habilitación de áreas y redes.

Habilitación de Wireless.

Creación de puntos de red.

Conectividad y servicios continuos.

Restricción de navegación.

Creación de cuentas.

Cámaras web.

Soporte Técnico Aplicaciones

eSIGPEN.

Mejora de conectividad.

Creación de nuevos módulos.

Soluciones integrales con otras instituciones.

Administración de Base de Datos.

Creación de usuarios de sistemas propios.

Nuevos sistemas dependiendo la necesidad institucional.

CONDICIONES DE SERVICIO

Se define como **servicio** a la solución informática que la DTIC brinda a los FUNCIONARIOS del SNAI a través de la mesa de ayuda GLPI.

Siendo un servicio implementado por esta cartera de Estado, se detallan condiciones de asistencia soporte técnico.

Todo soporte técnico será atendido siempre y cuando este documentado en la mesa de ayuda “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI se envía un correo electrónico a (soporte@atencionintegral.gob.ec).

EL soporte técnico se aplica a equipos, impresoras, tabletas, celulares y portátiles pertenecientes al SNAI, los cuales estarán debidamente codificados y marcados por parte de la Unidad de Bienes.

El soporte técnico en relación al software se realizará cumpliendo las disposiciones establecidas en las **POLÍTICAS DE USO, SERVICIO, CONECTIVIDAD Y EQUIPOS**.

Todo soporte técnico se documentará desde su solicitud hasta su resolución.

Cualquier soporte técnico fuera de las dependencias de la matriz del SNAI, será atendido en la brevedad posible dependiendo la disponibilidad de agentes de soporte.

Si el soporte técnico es fuera de la ciudad, será atendido una vez que se realicen las gestiones de traslado y estadía de ser el caso.



NIVELES DE SERVICIO

Los niveles de servicio se detallan a continuación:



Nivel 1.- Soporte técnico de primer orden

Modalidad.- Solicitud a través de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI se envía correo electrónico a (soporte@atencionintegral.gob.ec).

Autorización.- Ninguna

Agentes de Soporte.- Soporte Técnico (Todos), Infraestructura (Todos).

Tiempo de respuesta.- mínimo 5 minutos – máximo 24 horas

Nivel 2.- Soporte técnico de segundo orden

Modalidad.- Solicitud a través de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI se envía correo electrónico a (soporte@atencionintegral.gob.ec).

Autorización.- Previa factibilidad por parte del área de DESARROLLO

Agentes de Soporte.- Desarrollo (Todos).

Tiempo de respuesta.- mínimo 12 horas– máximo 48 horas

Nivel 3.- Soporte técnico de segundo orden

Modalidad.- Solicitud a través de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI se envía correo electrónico a (soporte@atencionintegral.gob.ec).

Autorización.- Director de Tecnología.

Agentes de Soporte.- Soporte Técnico (Todos).

Tiempo de respuesta.- mínimo 1 horas– máximo 48 horas

PERSONAL DE ESCALAMIENTO

Los puntos de contacto entre DTIC y el FUNCIONARIO serán únicamente de la siguiente manera:

1. eMail.- El funcionario que requiera un soporte técnico debe obligatoriamente “Crear un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) de la Intranet o en caso de no poder acceder a la plataforma GLPI se envía correo electrónico a soporte@atencionintegral.gob.ec; automáticamente se generará un No. De ticket con el cual puede dar seguimiento a su requerimiento.

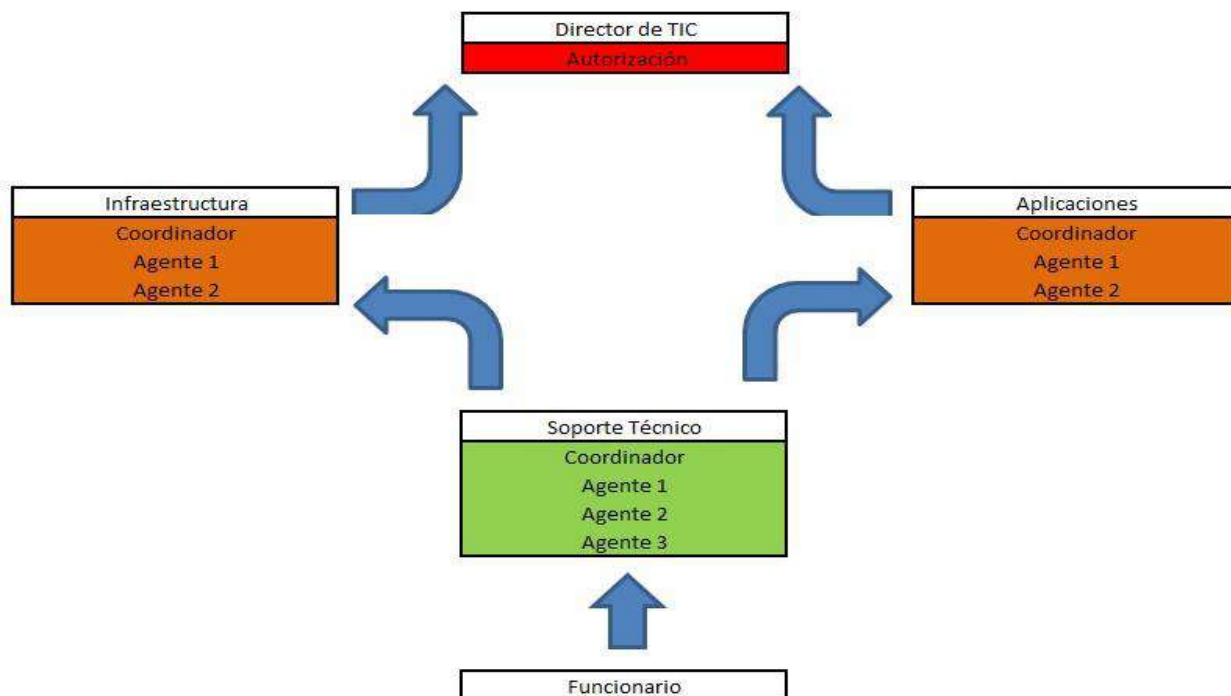
2. Herramienta de acceso GLPI.- Para generar un ticket o dar seguimiento a uno ya generado, el funcionario deberá ingresar al siguiente link: (<http://soporte.atencionintegral.gob.ec/>).

Para el ingreso el funcionario utilizará las mismas credenciales (Usuario y Clave) del computador asignado.

SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES INFRACTORES:

Nivel	Punto de Escalamiento	Región	Teléfono
Nivel 1	Stalin Morales Z.	Nacional/Local	02 3952520 Ext 215
Nivel 2	Martín Carlier P.	Nacional/Local	02 3952520 Ext 213
Nivel 3	Odilo Ipiales G.	Nacional/Local	02 3952520 Ext 212
Nivel 4	Edgar Villa M.	Nacional	02 3952520 Ext 216

FUNCIONARIO:



NORMAS DE USO DE ACTIVOS DE TIC

Los sistemas de información y recursos TIC del SNAI puestos a disposición de los colaboradores y usuarios en general, en especial equipos, correo electrónico y acceso a redes, son para uso exclusivo de los procesos y tratamientos de la Institución por parte de los usuarios autorizados, con finalidades de gestión y administración, y no pueden usarse con otras finalidades comerciales o particulares que no estén expresamente autorizadas.

Cada usuario es responsable del uso que haga de los recursos TIC, así como de las contraseñas o posibilidades de acceso que reciba, no pudiendo sin autorización copiar, difundir, modificar o destruir información de las empresas del SNAI, ni mantener desprotegidos equipos, soportes digitales o documentos en papel.

La Dirección de Tecnologías de la Información y Comunicación (DTIC) es la responsable de la administración y gestión de los recursos TIC, debiéndose autorizar por esta Dirección cualquier instalación, conexión o desconexión de elementos, periféricos, aplicaciones, o herramientas informáticas del tipo que sea en el ámbito de actuación y/o de responsabilidad del SNAI. A las finalidades indicadas, se comunicarán las instrucciones de uso oportunas.

El incumplimiento del contenido de esta norma o de las normas y procedimientos que la desarrollen puede suponer el bloqueo o suspensión de derechos de acceso del usuario, que podrá ser sancionado de acuerdo con la legislación aplicable o del régimen disciplinario interno, sin perjuicio de las posibles acciones administrativas, civiles o penales que en su caso correspondan en función de los hechos, su tipificación y gravedad.

Se fomentará la difusión de información y la concienciación de los usuarios, para crear una cultura de la seguridad y de la protección de la información.

Esta norma se desarrollará en lo que fuera necesario por otras normas, procedimientos e instrucciones técnicas más detalladas. En lo que se refiere a datos personales aquellos procedimientos estarán recogidos o referenciados en el Documento de Seguridad que reposa en la Dirección de Administración de Talento Humano.

Será objeto de mejora continua el Sistema de Gestión de la Seguridad de la Información (SGSI), siguiendo la filosofía de estándares aplicables ISO/UNE, y se evaluarán periódicamente los riesgos, partiendo de la identificación de los activos relacionados, las amenazas que puedan afectar y las posibles salvaguardas a establecer, a fin de eliminar o disminuir dichos riesgos, o gestionarlos de forma adecuada.

En cuanto a la autenticación de usuarios se usarán mecanismos fiables que exijan la identificación inequívoca y personalizada, como contraseñas robustas, certificados digitales, datos biométricos o dispositivos físicos, y los usuarios no suplantarán la identidad de otro. En todos los casos, sobre todo si la autenticación es mediante contraseñas, los datos de autenticación estarán protegidos tanto en los sistemas como cuando se transmitan y por parte del propio usuario.

Cada usuario podrá acceder solamente a los datos y recursos de información a los que esté autorizado por quien tenga competencia para ello, para el desarrollo de sus funciones y según el principio de mínimo privilegio. Los usuarios con perfiles más amplios necesitarán autorización especial, y se revisará periódicamente por si fuera preciso actualizar su perfil.

En cuanto a la Confidencialidad el Usuario se compromete a guardar reserva sobre la información a la que tiene acceso por razón de su actividad profesional, no divulgar dicha información, así como no publicarla de ningún modo, bien directamente o a través de terceras personas o empresas, para ponerla a disposición de terceros sin el previo consentimiento del SNAI. El usuario reconoce que la reproducción, copia, modificación, comunicación pública, distribución o cualquier otro medio de difusión de datos o información del SNAI sin autorización del mismo, constituye un delito.

Solo se utilizarán, siguiendo las instrucciones y/o procedimientos autorizados por el Departamento de Tecnologías de la Información y Comunicación los sistemas, productos, aplicaciones, paquetes y dispositivos que permitan una seguridad adecuada, así como los cambios posteriores que se incorporen. Para el cifrado de datos se emplearán algoritmos de cifrado robustos y fiables, protegiéndose las claves de forma efectiva.

Solamente se grabarán datos del SNAI en soportes informáticos (CDs, DVDs, tarjetas tipo SD, conectables a puertos USB) en los casos autorizados, y los soportes no podrán sacarse de las instalaciones si no es con autorización expresa. Han de estar protegidos, reflejados en un inventario si son varios, y en un registro de salida cuando proceda, y destruyéndolo cuando no sea necesario, según la normativa de datos personales.

Para garantizar la disponibilidad, y bajo la responsabilidad de la Dirección de Tecnologías de la Información y Comunicación, los sistemas y conexiones serán fiables, se obtendrán copias protegidas de la información, que se almacenarán en lugares no afectados por las mismas amenazas que los sistemas primarios, y en los casos más críticos existirán sistemas alternativos de proceso, propios o ajenos que, junto con los planes y procedimientos correspondientes, puedan permitir la continuidad de las operaciones, según la criticidad de los procesos y las circunstancias surgidas.

La red de comunicaciones estará protegida mediante cortafuegos y otros sistemas aplicables para evitar accesos no autorizados, especialmente desde el exterior de la red.

Se podrá registrar la actividad de los usuarios, siempre de acuerdo con la normativa sobre protección de datos personales, a fin de poder monitorizar y revisar las actividades realizadas y los posibles cambios introducidos en los sistemas o referidos a los datos.

Cuando se produzca la baja de un usuario se bloqueará o inhabilitará su cuenta de usuario, y devolverá todas las llaves e identificadores, tarjetas, y los recursos y documentos que sean del SNAI.

Se considerará un mal uso o uso inaceptable aquella actuación del usuario que pueda afectar a la disponibilidad de un servicio, al trabajo del resto de los usuarios, a la confidencialidad y seguridad de la información o que, en general, ponga en riesgo cualquiera de las cinco dimensiones de la seguridad (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) de la información y/o de los servicios relacionados con ella. A continuación, se recogen algunos ejemplos de lo que se considera “mal uso”:

- El uso de una cuenta de usuario para lo que no se tiene autorización o bien la apropiación indebida de las credenciales (usuario y contraseña) de otro.
- Uso de la red del SNAI para conseguir un acceso no autorizado a cualquier ordenador, servidor o aplicación.
- Realizar alguna actuación de forma intencionada que interfiera en el funcionamiento normal de otros ordenadores, impresoras, dispositivos o redes.
- Instalar y ejecutar de forma intencionada en cualquier ordenador o subred, cualquier tipo de software que provoque el mal funcionamiento o la sobrecarga de dicho equipo o subred (malware).
- El abuso deliberado de los recursos puestos a disposición del usuario.
- Los intentos de saltarse medidas de protección de la información o de explotar posibles fallos de seguridad en los sistemas.
- El no cumplimiento intencionado de las condiciones de las licencias de software o de sus derechos de autor.
- El envío de mensajes de correo con contenido fraudulento, ofensivo, obsceno o amenazante.
- Ocultar o falsificar la identidad de una cuenta de usuario o de una máquina.
- El uso de los servicios de difusión de información para fines que no tengan relación con las propias del desempeño laboral o que no sean de interés para el SNAI.
- Los intentos de monitorización y/o rastreo de las comunicaciones de los usuarios.
- La lectura, copia, modificación o borrado de los ficheros de otros usuarios sin la autorización expresa del propietario.

Los usuarios, cuando se les solicite, deben colaborar con los administradores de sistemas, en la medida de sus posibilidades, en cualquier investigación que se haga sobre mal uso de los recursos, aportando la información que tengan y se les requiera.

La DTIC colaborará en la persecución de los delitos informáticos que tengan origen o destino en su infraestructura o usuarios, dando prioridad a los requerimientos que se reciban por parte de las autoridades competentes, aportando toda la información que sea posible para el esclarecimiento del incidente y todo ello dentro del marco de la legalidad vigente.

El incumplimiento de estas Políticas puede acarrear sanciones administrativas sin perjuicio de las acciones legales que pueda tomar el SNAI.

SEGURIDAD, RESPONSABILIDAD DE DTIC Y FUNCIONARIO

Responsabilidades de EL FUNCIONARIO:

EL FUNCIONARIO no realizará ninguna actividad en contra de la seguridad de la red de la DTIC así como los datos que en ella circulen,

Uso ilegal:

Los servicios del FUNCIONARIO no deben ser usados para fines ilegales o en soporte de actividades ilegales. EL FUNCIONARIO se reserva el derecho a cooperar con las autoridades legales y/o terceras partes afectadas en la investigación de cualquier crimen o acción ilegal.

Amenazas:

El uso de servicios del FUNCIONARIO para transmitir cualquier material (por email, subida de archivos, alojamiento u otros) que amenace o aliente el daño físico o destrucción de la propiedad.

Hostigamiento:

El uso de servicios del FUNCIONARIO para transmitir cualquier material (por email, subida de archivos, alojamiento u otros) que hostigue a un tercero.

Actividad fraudulenta:

El uso de los servicios del FUNCIONARIO para realizar ofrecimientos fraudulentos para vender o comprar productos, objetos o servicios, o para ejecutar cualquier tipo de estafa financiera.

Falsificación o imitación de persona:

Está prohibido agregar, remover o modificar información identificadora en la red, en un esfuerzo de engañar o confundir. Está prohibido el intentar reemplazar a otra persona utilizando su información identificadora. El uso de emails anónimos o de nicknames (apodos) no constituye imitación de persona.

eMail comercial no solicitado / eMail masivo no solicitado (SPAM):

El uso de servicios del FUNCIONARIO para el envío de eMails comerciales o masivos no solicitados está expresamente prohibido. Violaciones de este tipo resultarán en la finalización inmediata del servicio.

Bombardeo de eMails y noticias:

Intentos malignos para impedir el uso a otra persona del servicio de correo electrónico o noticias, resultará en la inmediata remoción del servicio contratado.

Falsificación de eMails y mensajes:

Falsificar cualquier mensaje, completa o parcialmente, de cualquier transmisión electrónica, originada o transitando a través de nuestros servicios es una violación de estas Políticas.

Accesos no autorizados:

El uso de los servicios del FUNCIONARIO para acceder, o intentar acceder, a las cuenta de otros, o penetrar, o intentar penetrar, medidas de seguridad del FUNCIONARIO u otro software o hardware de otra entidad, sistemas de comunicaciones electrónicas o sistemas de telecomunicaciones, ya sea que la intrusión resulte o no en la corrupción o pérdida de información, está expresamente prohibida y el servicio será inmediatamente cancelado.

Infracción en la marca registrada y derechos de autor:

El uso de los servicios del FUNCIONARIO para transmitir cualquier material que viole derechos de autor, marca registrada, patentes, secreto comercial u otros derechos de propiedad de una tercera parte, incluyendo, pero no limitándose, a la copia no autorizada de material con derechos de autor, la digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos de autor, y la transmisión no autorizada de software con copyright.

Recolección de información personal:

El uso de los servicios del FUNCIONARIO para obtener o intentar obtener información personal de terceras personas sin su conocimiento o consentimiento.

Discontinuidades en la red y actividad no amistosa:

El uso de los servicios del FUNCIONARIO para cualquier actividad que afecte la habilidad de otras personas o sistemas para utilizar nuestros servicios o Internet. Esto incluye ataques de “denegación de servicios” (DOS – Denial of Service) contra otras redes de Hosting o usuarios particulares. La interferencia o interrupción de otras redes, servicios o equipamiento está terminantemente prohibida.

Es responsabilidad de la DTIC asegurarse que su sitio esté configurado de una forma segura. Una DTIC no debe permitir que su sitio este configurado de tal forma que le permita a una tercera parte la posibilidad de usar su red para un fin ilegal o inapropiado. La entrada no autorizada y/o el uso del sistema de otra compañía o individuo, resultará en la inmediata finalización de la cuenta.

EL FUNCIONARIO no tolerará que ningún DTIC intente acceder a las cuentas de otros DTIC, o penetrar medidas de seguridad de otros sistemas, ya sea que la intrusión resulte o no en la corrupción o pérdida de información.

Fraude:

Implica una declaración conscientemente engañosa o tergiversada realizada con la intención que la persona que la reciba actúe conforme a ello.

Distribución de Virus:

La distribución intencional de software que intente o cause daños, hostigamiento o molestia a personas, información y/o sistemas de computación están prohibidos. Semejante agravio resultará en la finalización del servicio contratado.

Responsabilidad por terceras partes:

Los FUNCIONARIOS de TICs son responsables y deberán dar cuenta por las actividades de terceras partes, que utilicen sus servicios, y violen esta guía creada como Políticas de uso Aceptable.

Violación en dominios virtuales:

Está absolutamente prohibido alojar contenido pornográfico o servidores IRC en los dominios virtuales. Cualquier dominio que contenga este material será sujeto a la inmediata cancelación sin reembolso.

Redes IRC:

Está absolutamente prohibido alojar un servidor IRC que es parte o está conectado con otra red o servidor IRC. El sitio que esté conectado a alguna de estas redes será inmediatamente removido de nuestra red sin previa notificación y no será reconectado hasta que el DTIC acuerde en remover todos los restos del servidor IRC, y permita tener acceso a su sitio para verificar que el contenido ha sido totalmente removido. Cualquier sitio culpable de una segunda violación será inmediatamente cancelado.

Funcionamiento de la Red:

Las cuentas del FUNCIONARIO operan con recursos compartidos. El uso o abuso excesivo de estos recursos compartidos por un usuario puede tener un impacto negativo en todos los DTIC. El abuso de los recursos de la red en una forma que deteriore el funcionamiento de la misma está prohibido por estas políticas y puede resultar en la cancelación del servicio.



ACEPTACIÓN DE LAS PARTES

En la ciudad de San Francisco de Quito, Distrito Metropolitano, a los ... días del mes de del año comparecen a la celebración del presente Acuerdo de Niveles de Servicio por una parte la DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN representado por, por otra parte el SERVICIO NACIONAL DE ATENCIÓN INTEGRAL A PERSONAS ADULTAS PRIVADAS DE LA LIBERTAD Y A ADOLESCENTES INFRACTORES, representada por, quienes suscriben el presente Acuerdo en relación al Contrato de prestación de servicio de Virtual Data Center, suscrito entre..... y el DTIC, que tendrá vigencia de a partir de la finalización de la instalación implantación del servicio.

Servicio Nacional de Atención
Integral a Personas Adultas
Privadas de la Libertad y a
Adolescentes Infractores

Dirección de Tecnologías de la
Información y Comunicación



CAPÍTULO 9.- PLAN DE CONTINGENCIA

PRESENTACIÓN

El Plan de Contingencia Informático implica un análisis de los posibles riesgos a cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información. Corresponde a la Dirección de Tecnologías, aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

El alcance de este plan guarda relación con la infraestructura informática, así como los procedimientos relevantes asociados con la plataforma tecnológica. La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función del negocio. Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. La información como uno de los activos más importantes del SNAI, es el fundamento más importante de este Plan de Contingencia.

Al existir siempre la posibilidad de desastre, pese a todas nuestras medidas de seguridad, es necesario que El Plan de Contingencia Informático incluya el Plan de Recuperación de Desastres con el único objetivo de restaurar el Servicio Informático en forma rápida, eficiente, con el menor costo y pérdidas posibles.

La protección de la información vital ante la posible pérdida, destrucción, robo y otras amenazas de una empresa, es abarcar la preparación e implementación de un completo Plan de Contingencia Informático. El plan de Contingencia indica las acciones que deben tomarse inmediatamente tras el desastre. Un primer aspecto importante del plan es la organización de la contingencia, en el que se detallan los nombres de los responsables de la contingencia y sus responsabilidades. El segundo aspecto crítico de un Plan de Contingencia es la preparación de un Plan de Backup, elemento primordial y necesario para la recuperación. El tercer aspecto es la preparación de un Plan de Recuperación. La empresa debe establecer su capacidad real para recuperar información contable crítica en un periodo de tiempo aceptable. Otro aspecto importante del plan de recuperación identificar el equipo de recuperación, los nombres, números de teléfono, asignaciones específicas, necesidades de formación y otra información esencial, para cada miembro del equipo que participa en el Plan de recuperación.

La base del Plan de Contingencia y su posterior recuperación, es establecer prioridades claras sobre qué tipo de procesos son los más esenciales. Es necesario por tanto la identificación previa de cuales de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

El Plan de Recuperación del Desastre (PRD) provee de mecanismos de recuperación para los registros vitales, sistemas alternativos de telecomunicaciones, evacuación de personal, fuente alternativa de provisión de servicios, etc. Además debe ser comprobado de forma periódica para detectar y eliminar problemas. La manera más efectiva de comprobar si un PRD funciona correctamente, es programar simulaciones de desastres. Los resultados obtenidos deben ser cuidadosamente revisados, y son la clave para identificar posibles defectos en el Plan de Contingencia.

El plan de contingencia informático, debe contemplar los planes de emergencia, backup, recuperación, comprobación mediante simulaciones y mantenimiento del mismo. Un plan de contingencia adecuado debe ayudar a las empresas a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal del negocio.

La Dirección de tecnologías debe comprender los principales riesgos para la empresa y las posibles consecuencias de un desastre. Un Plan de contingencia adecuado identifica las necesidades de todos los departamentos e involucra a TODO el personal de todas las áreas del SNAI.

1.- Análisis de Situación Actual Informática

Propósito

Cualquier Sistema de Redes de Computadoras (CPU, periféricos y accesorios) están expuestos a riesgo y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos.

Frente a cualquier evento, la celeridad en la determinación de la gravedad del problema depende de la capacidad y la estrategia a seguir para señalar con precisión, por ejemplo: ¿Qué componente ha fallado?, ¿Cuál es el dato o archivo con información se ha perdido, en que día y hora se ha producido y cuán rápido se descubrió? Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información.

Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o por fallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable. Frente al mayor de los desastres solo queda el tiempo de recuperación, lo que significa adicionalmente la fuerte inversión en recursos humanos y técnicos para reconstruir su Sistema de Red y su Sistema de Información.

Objetivo

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

Importancia

- Garantiza la seguridad física, la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos.
- Permite realizar un conjunto de acciones con el fin de evitar el fallo, o en su caso, disminuir las consecuencias que de él se puedan derivar.
- Permite realizar un Análisis de Riesgos, Respaldo de los datos y su posterior Recuperación de los datos. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la organización.
- Permite definir contratos de seguros, que vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades.

Sistema de Red de Datos

La Administración de Red está dividida en dos clases:

1. **Conectividad:** se encarga de la conexión alámbrica e inalámbrica de los equipos de comunicación
2. **Manejo de servidores:** se encarga de alojar todos los servicios y sistemas de comunicación e información.

Los servicios de Red implementados en el SNAI son los siguientes:

- ✓ Servidor de Correo Electrónico
- ✓ Servidor de seguridad
- ✓ Servidor de seguridad – base de datos
- ✓ Servidor de telefonía IP.
- ✓ Servidor de Políticas de Grupo – Controlador de dominio

Sistema de información

El Sistema de Información, incluye la totalidad del Software de Aplicación, Software en Desarrollo, conjunto de Documentos Electrónicos, Bases de Datos e Información Histórica registrada en medios magnéticos e impresos en papeles, Documentación y Bibliografía.

2.- Plan de Reducción de Riesgos

El Plan de Reducción de Riesgos es equivalente a un Plan de Seguridad, en la que se considera todos los riesgos conocidos, para lo cual se hará un Análisis de riesgos.

2.1 Análisis de Riesgos

El presente realiza un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada, y que deben ser protegidos.

Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

- ✓ Personal Hardware
- ✓ Software y utilitarios
- ✓ Datos e información
- ✓ Documentación
- ✓ Suministro de energía eléctrica
- ✓ Suministro de telecomunicaciones

Daños

Los posibles daños pueden referirse a:

- ✓ Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- ✓ Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- ✓ Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia

Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la compañía son:

- ✓ Acceso no autorizado
- ✓ Ruptura de las claves de acceso a los sistemas computacionales
- ✓ Desastres Naturales:
 - Movimientos telúricos

- Inundaciones
- Fallas en los equipos de soporte (causadas por el ambiente, la red de energía eléctrica, no acondicionamiento atmosférico necesario)
- Fallas de Personal Clave: por los siguientes inconvenientes:
 - Enfermedad
 - Accidentes
 - Renuncias
 - Abandono de sus puestos de trabajo
 - Otros.
- Fallas de Hardware:
 - Falla en los Servidores (Hw)
 - Falla en el hardware de Red (Switches, cableado de la Red, Router, FireWall)
- Incendios

2.1.1 Características

El Análisis de Riesgos tiene las siguientes características:

- Es posible calcular la probabilidad de que ocurran las cosas negativas.
- Se puede evaluar económicamente el impacto de eventos negativos.
- Se puede contrastar el Costo de Protección de la Informática y medios versus el Costo de volverla a producir.

Durante el estudio Análisis de Riesgo, se define claramente:

- Lo que intentamos proteger
- El valor relativo para la organización
- Los posibles eventos negativos que atentarían lo que intentamos proteger.
- La probabilidad de ataque.

Se debe tener en cuenta la probabilidad de suceso de cada uno de los problemas posibles, de tal manera de tabular los problemas y su costo potencial mediante un Plan adecuado. Los criterios que usaremos para tipificar los posibles problemas son:

Escala de Valores para Criterios de Posibles Problemas

Criterios	Escala			
Grado de Negatividad	Leve	Moderado	Grave	Muy severo
Posible Frecuencia del Evento negativo	Nunca	Aleatorio	Periódico	Continuo
Grado de impacto o consecuencias	Leve	Moderado	Grave	Muy severo
Grado de Certidumbre	Nunca	Aleatorio	Probable	Seguro

2.1.2 Clases de Riesgo

La tabla proporciona el Factor de Probabilidad por Clase de Riesgo en función a la ubicación geográfica de la institución y a su entorno institucional; por ejemplo, si la institución:

- Se ubica en zona sísmica el factor de probabilidad de desastre por terremotos será alta.
- Se ubica en una zona marginal con alto índice de delincuencia, las probabilidades de robo, asalto o vandalismo será de un sesgo considerablemente alto.
- Se ubica en zona industrial las probabilidades de “Fallas en los equipos” será alto por la magnitud de variaciones en tensiones eléctricas que se generan en la zona.
- Cambia constantemente de personal, las probabilidades de equivocaciones y sabotaje será alto.

Identificación de Amenazas:

Escala Factor de Probabilidad por Clase de Riesgo

Clase	Factor
Incendio o Fuego	0.40
Robo común de equipos y archivos	0.75
Sabotaje	0.60
Falla en los equipos	0.40
Equivocaciones	0.70
Acción virus informático	0.50

Fenómenos naturales	0.25
Accesos no autorizados	0.75
Robo de datos	0.80
Manipulación y sabotaje	0.80

En lo que respecta a Fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de poca intensidad; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios de techos, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

Clase de Riesgo: Incendio o Fuego

Grado de Negatividad :	Muy Severo
Frecuencia de Evento:	Aleatorio
Aleatorio Grado de Impacto:	Grave
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
El área de Servidores del SNAI cuenta con un extintor cargado, ubicado dentro del Área de Servidores.	Se cumple parcialmente, el extintor se encuentra afuera
En muchas oficinas de SNAI, no cuenta con un extintor.	Instalar extintores para todas las áreas del SNAI.
Se ejecuta un programa anual de capacitación sobre el uso de elementos de seguridad y primeros auxilios, lo que no es eficaz para enfrentar un incendio y sus efectos.	Capacitaciones Permanentes - Simulaciones
Debido al incremento del número de computadores por oficina se hace necesario contar con extintores en las oficinas.	Incrementar el número de extintores por área.

Una probabilidad máxima de contingencia de este tipo en el SNAI, puede alcanzar a destruir un 50% de las oficinas antes de lograr controlarlo, también podemos suponer que en el área de Servidores tendría un impacto mínimo, por las medidas de seguridad y ambiente que lo protege. Esta información permite resaltar el tema sobre el lugar donde almacenar los backups. El incendio, a través de su acción calorífica, es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD's, DV's, cartuchos, Discos duros, pendrives, los mismos que residen en una caja fuerte (medio de seguridad que nos protege frente a robo o terremoto, pero no del calor). Estos dispositivos de almacenamiento muestran una tolerancia de temperatura de 5°C a 45°C, y una humedad relativa de 20% a 80%.

Para la mejor protección de los dispositivos de almacenamiento, se colocaran estratégicamente en lugares distantes, con una Segunda Copia de Seguridad custodiada en un lugar externo del SNAI.

Las áreas funcionales distribuidas, existe al menos una computadora, por lo que se debe incrementar los elementos y medidas de seguridad contra incendios.

Uno de los dispositivos más usados para contrarrestar la contingencia de incendio, son los extinguidores. Su uso conlleva a colocarlos cerca de las posibles áreas de riesgo que se debe proteger.

Daños

Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado.

Cuando el daño ha sido menor:

- ✓ Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento
- ✓ Se recoge los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.
- ✓ Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento
- ✓ Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.
- ✓ Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo

Acciones a tomar

ANTES

- ✓ Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
- ✓ No concentrar grandes cantidades de papel, ni fumar cerca de químicos o sustancias volátiles.
- ✓ Verificar las condiciones de extintores e hidratantes y capacitar para su manejo.
- ✓ Si se fuma, procurar no arrojar las colillas a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.
- ✓ No almacenar sustancias y productos inflamables.
- ✓ No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.
- ✓ Por ningún motivo mojar las instalaciones eléctricas, recordar que el agua es un buen conductor de la electricidad.
- ✓ Si se detecta cualquier anomalía en los equipos de seguridad (extintores, hidratantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato a Seguridad.
- ✓ Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.
- ✓ Tener a la mano los números telefónicos de emergencia.
- ✓ Portar siempre la credencial de identificación del SNAI.

DURANTE

- ✓ Ante todo se recomienda conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- ✓ En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá (si el tiempo lo

permite) "Salir de Red y Apagar Computador": Down en el (los) servidor(es), apagar (OFF) en la caja principal de corriente del CIT.

Si se conoce sobre el manejo de extintores, intenta sofocar el fuego, si este es considerable no trates de extinguirlo con los propios medios, solicitar ayuda.

Si el fuego esta fuera de control, realizar evacuación del inmueble, siguiendo las indicaciones del Personal de bomberos.

No utilizar elevadores, descender por las escaleras pegado a la pared que es donde posee mayor resistencia, recuerda: No gritar, No empujar, No correr y dirigirse a la zona de seguridad.

Si hay humo donde nos encontramos y no podemos salir, mantenernos al ras del piso, cubriendo tu boca y nariz con un pañuelo bien mojado y respira a través de él, intenta el traslado a pisos superiores.

Las personas que se encuentren en los últimos pisos, deberán abrir ventanas para que el humo tenga una vía de salida y se descongestionen las escaleras.

Si es posible mojar la ropa.

Verifica si las puertas están calientes antes de abrirlas, si lo están, busca otra salida.

DESPUÉS

Retirarse inmediatamente del área incendiada y ubícate en la zona de seguridad externa que te corresponda.

No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.

El personal calificado realizara una verificación física del inmueble y definirá si esa en condiciones de ser utilizado normalmente.

Colaborar con las autoridades.

Clase de Riesgo: Robo Común de Equipos y Archivos

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Aleatorio Grado de Impacto: Moderado
Grado de Certidumbre: Aleatorio

Situación actual	Acción correctiva
Vigilancia permanente.	Existe vigilancia. La salida de un equipo informático es registrada por el personal de la Oficina y por el personal de seguridad en turno.
No se verifica si el Personal de Seguridad cumple con la inspección de los usuarios, sobre su obligación de cerrar puertas y ventanas al finalizar su jornada.	Al respecto Personal de Seguridad emite recomendaciones sobre medidas de Alerta y seguridad.
Remitir aviso a la Unidad de Bienes y al SNAI, para retirar equipo de informático.	Se Cumple

Se han reportado casos en los cuales ha existido manipulación y reubicación de equipos sin el debido conocimiento y autorización debida entre la Unidad de Bienes y la Dirección de TIC del SNAI.

Según antecedentes de otras instituciones, es de conocer que el robo de accesorios y equipos informáticos, llegaron a participar personal propio de la empresa en colusión con el personal de vigilancia. Es relativamente fácil remover un disco duro del CPU, una disquetera, tarjeta, etc. y no darse cuenta del faltante hasta días después.

Acciones a tomar

Analizar las siguientes situaciones:

En qué tipo de vecindario se encuentra la Institución
Las computadoras se ven desde la calle
Hay personal de seguridad en la Institución y están ubicados en zonas estratégicas
Cuánto valor tienen actualmente las Bases de Datos
Cuánta pérdida podría causar en caso de que se hicieran públicas
Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.
Trabajo no supervisado, especialmente durante el turno de noche, malas técnicas de contratación, evaluación y de despido de personal.

Clase de Riesgo: Vandalismo

Grado de Negatividad:	Moderado
Frecuencia de Evento:	Aleatorio
Aleatorio Grado de Impacto:	Grave
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
El SNAI está en una zona donde el índice de vandalismo es bajo	Hay vigilancia.
Se presentan casos muy aislados de personas que no están conformes con algunas normativas administrativas, tal que al efectuar sus reclamos personalmente asumen actitudes retroactivas, que muchas veces ofenden al trabajador, y sin medir las consecuencias pueden llegar a dañar alguna instalación del SNAI.	Control Interno
Alguna probabilidad de turbas producto de manipulaciones políticas.	Back Prioritarios

La destrucción del equipo puede darse por una serie de desastres incluyendo el vandalismo, robo y saqueo en simultáneo.

Acciones a tomar

Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área del Centro de Cómputo ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.

A continuación se menciona una serie de medidas preventivas:

- Establecer vigilancia mediante cámaras de seguridad en el Site, el cual registre todos los movimientos de entrada del personal.
- Instalar identificadores mediante tarjetas de acceso.
- Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad bancaria donde se custodiaran los datos e información crítica).

Los principales conflictos que pudieran presentarse son:

- En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas.
- Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro de la Delegación Miguel Hidalgo, sería imposible reanudar las actividades que un momento dado fueran críticas, como la nómina, contabilidad, etc; en un sitio alterno, ya que no contarían con copia de la información.

Clase de Riesgo: Falla de Equipos

Grado de Negatividad:	Grave
Frecuencia de Evento:	Aleatorio
Aleatorio Grado de Impacto:	Grave
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
La Red de Servidores en el SNAI NO cuenta con una Red Eléctrica Estabilizada.	Proponer un Estudio para instalar una Red Eléctrica Estabilizada
No existe un adecuado tendido eléctrico en algunas oficinas del SNAI	Tomar previsiones económicas para implementar un adecuado tendido eléctrico
Cada área funcional se une a la Red a través Gabinetes, la falta de energía en éstos, origina la ausencia de uso de los servicios de red: los Sistemas Informáticos, Teléfonos IP, mantenimiento remoto.	Proteger los Gabinetes, y su adecuado apagado y encendido, dependen los servicios de red en el Área
La falla en el hardware de los equipos, requiere un rápido mantenimiento o reemplazo.	Existe Mantenimiento de los equipos de cómputo. Contar con proveedores, en caso de requerir reemplazo de piezas, y de ser posible contar con repuestos

De ocurrir esta contingencia las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos.

El equipo de aire acondicionado y ambiente adecuado en el Área de Servidores, favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varía en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del HW y la información podría perderse.

La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Se ha identificado los siguientes problemas de energía más frecuentes:

- ✓ Fallas de energía
- ✓ Transistores y pulsos
- ✓ Bajo voltaje
- ✓ Ruido electromagnético
- ✓ Distorsión
- ✓ Variación de frecuencia.

Para los cuales existen los siguientes dispositivos que protegen los equipos de estas anomalías:

- ✓ Supresores de picos
- ✓ Estabilizadores
- ✓ Sistemas de alimentación ininterrumpida (UPS)

Existen formas de prever estas fallas, con la finalidad de minimizar su impacto, entre ellas tenemos:

Tomas a Tierra o Puestas a Tierra

Se denomina así a la comunicación entre el circuito Eléctrico y el Suelo Natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra humedad, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y para disipar sobretensiones de origen atmosférico o industrial.

La Toma a Tierra tiene las siguientes funciones principales: a) protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas, b) protege a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales., c) facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Las inspecciones deben realizarse trimestralmente, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se realice en los meses de verano o en tiempo de sequía. Es recomendable un mantenimiento preventivo anual dependiendo de las propiedades electroquímicas estables.

Fusibles

Al cablear la computadora, la carcasa normalmente se conecta a la tercera patilla del cable de alimentación. En algunos casos, puede que la tierra se conecte también al neutro. Si la electricidad fugara a través del aislante y llegase a la carcasa, esta derivación de electricidad aumentaría la intensidad de corriente que va por el circuito. Este incremento puede ser detectado por un fusible o un

diferencial. Estos dos dispositivos están diseñados para interrumpir un circuito si se sobrecargan (un fusible se debe sustituir tras fundirse, un diferencial se debe restaurar tras saltar).

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo. A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Arreglado el problema se puede a conectar el equipo.

Al sustituir los fusibles de una computadora, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el fusible. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado.

Asegurarse que el fusible de recambio es de la misma capacidad que el fundido. Por ejemplo si el fusible fundido viene marcando 2 amperios, no se debe sustituir por uno de 3 amperios. Un fusible de 3 amperios dejara pasar 1 amperio más de la intensidad de lo que fijo el diseñador del equipo.

Extensiones eléctricas y capacidades

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado.

No solo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.

Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.

No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar. Se debe utilizar los enchufes de pared siempre que sea posible.

Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar limitar el daño ante fallas eléctricas.

Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esa cifra el amperaje total de todos los aparatos conectados a ellas.

Adquirir toma corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar con enchufes de espigas planas, como cilíndricas.

Tanto las tomas corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

Casos

Error Físico de Disco de un Servidor (Sin RAID).

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último backup, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Verificación el buen estado de los sistemas.
8. Habilitar las entradas al sistema para los usuarios.

Error de Memoria RAM y Tarjeta(s) Controladora(s) de Disco

En el caso de las memorias RAM, se dan los siguientes síntomas:

1. El servidor no responde correctamente, por lentitud de proceso o no rendir ante el ingreso masivo de usuarios.
2. Ante procesos mayores se congela el proceso.
3. Arroja errores con mapas de direcciones hexadecimales.
4. Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente.

Acciones a tomar

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.



3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, ello evitará que al encender el sistema, los usuarios ingresen
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.



Clase de Riesgo: Equivocaciones

Grado de Negatividad:	Moderado
Frecuencia de Evento:	Periódico
Aleatorio Grado de Impacto:	Moderado
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
Las equivocaciones que se producen en forma rutinaria son de carácter involuntario.	Capacitación inicial en el ambiente de trabajo. Instruir al nuevo usuario con el Manual de Procedimientos
Cuando el usuario es practicante y tiene conocimientos de informática, tiene el impulso de navegar por los sistemas.	En lo posible se debe cortar estos accesos, limitando su accionar en función a su labor de rutina
La falta de institucionalizar procedimientos produce vacíos y errores en la toma de criterios para registrar información.	Reuniones y Actas de Trabajo para fortalecer los procedimientos
La DTIC no recibe comunicación del personal de reemplazo por vacaciones por lo tanto supone que es la Oficina usuaria la que capacita al reemplazante.	Se debe informar a la DTIC del reemplazo para su registro y accesos a la Red y los Sistemas, por el tiempo que dure el reemplazo. Al término del periodo de reemplazo se restituye los valores originales a ambos usuarios
Ante nuevas configuraciones se comunica a los usuarios sobre el manejo, claves, accesos y restricciones, tanto a nivel de Sistemas, Telefonía, Internet	Enviar oficios circulares múltiples comunicando los nuevos cambios y políticas

Acciones a tomar

- ¿Cuánto saben los empleados de computadoras o redes ?
- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?
- Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.

Clase de Riesgo: Acción de Virus Informático

Grado de Negatividad: Muy Severo
Frecuencia de Evento: Continuo
Aleatorio Grado de Impacto: Grave
Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Se cuenta con un Software Antivirus corporativo. Pero no hay un contrato anual para su actualización.	Se debe evitar que las licencias no expiren, se requiere la renovación de contrato anualmente
Todo Software (oficina, desarrollo, mantenimiento, drives, etc.) es manejado por personal de DTIC, quienes son los encargados de su instalación en las PC's con su respectivo software corporativo.	Se cumple
Se tiene un programa permanente de bloqueo acciones como cambiar configuraciones de red, acceso a los servidores, etc.	Se cumple a través de políticas de usuarios
Se tiene instalado el antivirus de red y en estaciones de trabajo. Antes de logear una maquina a la red (dominio) se comprueba al existencia de virus en la PC.	Se cumple
La DTIC no recibe comunicación del personal de reemplazo por vacaciones por lo tanto supone que es la Oficina usuaria la que capacita al reemplazante.	Se debe informar a la DTIC del reemplazo para registrarlo y darle los accesos permitidos a la Red y los Sistemas, por el tiempo que dure el reemplazo. Al término del periodo de reemplazo se restituye los valores originales a ambos usuarios

En estos últimos años la acción de los virus informáticos ha sido contrarrestada con la diversidad de productos que ofrece el mercado de software. Las firmas y/o corporaciones que proporcionan software antivirus, invierten mucho tiempo en recopilar y registrar virus, indicando en la mayoría de los casos sus características y el tipo de daño que puede provocar, por este motivo se requiere de una actualización periódica del software antivirus.



Acciones a tomar

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

Se contará con antivirus para el sistema; aislar el virus para su futura investigación.

El antivirus muestra el nombre del archivo infectado y quién lo usó.

Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

Utilizar los discos de instalación que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado.

Insertar el disco de instalación antivirus, luego instalar el sistema operativo, de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del Scaneado. Finalizado el scaneado, reconstruir el Master Boot del disco duro.





Clase de Riesgo: Fenómenos Naturales

Grado de Negatividad:	Grave
Frecuencia de Evento:	Aleatorio
Aleatorio Grado de Impacto:	Grave
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
La última década no se han registrado contingencias debido a fenómenos naturales como: terremotos, inundaciones, aluviones, etc.	Medidas de prevención.
Potencialmente existe la probabilidad de sufrir inundaciones debido a lluvias que ocurren en épocas de verano.	Medidas de prevención.
Tenemos épocas fuertes lluvias (Fenómeno del Niño) que causas estragos en viviendas de material rustico. Las instalaciones del SNAI están adecuadamente protegidas, sin embargo se debe verificar el tema del suministro eléctrico.	Al ocurrir un corte de energía el personal de vigilancia deberá comunicar al personal de la DTIC, para desconectar el sistema de red de manera preventiva
El ambiente donde se encuentra los Servidores principales, es apropiado ante las filtraciones.	Ubicación apropiada. Pero ante resultado de posibles filtraciones realizar trabajos de mantenimiento preventivo

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en la sala de Computación Central, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar mediante su caída y/o destrucción la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aun en las instalaciones de la institución



Clase de Riesgo: Accesos NO Autorizados

Grado de Negatividad:	Grave
Frecuencia de Evento:	Aleatorio
Aleatorio Grado de Impacto:	Grave
Grado de Certidumbre:	Probable

Situación actual	Acción correctiva
Se controla el acceso al Sistema de Red mediante la definición de “Cuenta” o “Login” con su respectiva clave	Se cumple
A cada usuario de Red se le asigna los “Atributos de confianza” para el manejo de archivos y acceso a los sistemas.	Se cumple
Cuando el personal cesa en sus funciones y/o es asignado a otra área, se le redefinen los accesos y autorizaciones, quedando sin efecto la primera.	Se cumple de modo extemporáneo, siendo lo indicado actualizar los accesos al momento de producirse el cese o cambio.
Se forman Grupos de usuarios, a los cuales se le asignan accesos por conjunto, mejorando la administración de los recursos	Se cumple
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado. En algunos casos los usuarios escriben su contraseña (Red o de Sistemas) en sitios visibles.	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalando la responsabilidad e importancia que ello implica.
No se tiene un registro electrónico de Altas/Bajas de Usuarios, con las respectivas claves	Se debe implementar

Todos los usuarios sin excepción tienen un “login” o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de ocho (8) caracteres. No se permiten claves en blanco. Además están registrados en un grupo de trabajo a través del cual se otorga los permisos debidamente asignados por el responsable de área.

Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla. Ello se aplica tanto a su autenticación como usuario de Red como usuario de Sistemas del SNAI, si lo tuviere.

Acciones a tomar

Enfatiza los temas de:

Contraseñas. Las contraseñas son a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse un número máximo (3) de intentos

infructuosos. El CIT implementa la complejidad en sus contraseñas de tal forma que sean más de siete caracteres y consistentes en números, letras y al menos un carácter especial.

Entrampamiento al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

Privilegio. En los sistemas informáticos del SNAI, cada usuario se le presenta la información que le corresponde. Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. En este punto el administrador de la red ha clasificado a los usuarios de la red en “Grupos” con el objeto de adjudicarles el nivel de seguridad y perfil adecuado.

Clase de Riesgo: Robo de Datos

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Aleatorio Grado de Impacto: Grave
Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Las Oficinas tienen disponible disqueteras, quemadoras de CD/DVD, puertos USB, pero no se lleva un control sobre la información que ingresa y/o sale del ordenador.	Personal de Planta debe manejar información delicada de la Oficina
El servicio de Internet es potencialmente una ventaja abierta para el robo de información electrónica	Existen políticas que regulan el uso y acceso del Servicio de Internet
Los documentos impresos (informes, reportes, contratos, etc.) normalmente están expuestos al robo por que no se acostumbra guardarlos como debe ser. Si no se toma conciencia que esta es una manera de atentar contra el Sistema Informático del SNAI el problema persistirá.	Resguardar la información en archivos. Destruir los reportes malogrados, sobre todo de contenido relevante. (Existen papeleros que convierten el papel en picadillo)
El acceso a los terminales se controla, mediante claves de acceso, de esta manera se impide el robo de información electrónica. A través de las políticas de seguridad se impide el ingreso a los Servidores.	Se cumple parcialmente

El Robo de datos se puede llevarse a cabo bajo tres modalidades:

- La primera modalidad consiste en sacar “copia no autorizada” a nuestros archivos electrónicos aun medio magnético y retirarla fuera de la institución.
- La segunda modalidad y tal vez la más sensible, es la sustracción de reportes impresos y/o informes confidenciales.
- La tercera modalidad es mediante acceso telefónico no autorizado, se remite vía Internet a direcciones de Correo que no corresponden a la Gestión Empresarial.



Acciones a tomar

Se previene a través de las siguientes acciones:

Acceso no Autorizado: Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

- Área de Sistemas.
- Computadoras personales y/o terminales de la red.
- Información confidencial.

Control de acceso al Área de Sistemas: El acceso al área de Informática estará restringido:

- Sólo ingresan al área el personal que trabaja en el área.
- El ingreso de personas extrañas solo podrá ser bajo una autorización.

Acceso Limitado a los Terminales: Cualquier terminal que puede ser utilizado como acceso a los datos de un Sistema, las siguientes restricciones pueden ser aplicadas:

- Determinación de los períodos de tiempo para los usuarios o las terminales.
- Designación del usuario por terminal.
- Limitación del uso de programas para usuario o terminales.
- Límite de tentativas para la verificación del usuario, tiempo de validez de las señas, uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 minutos).

Niveles de Acceso: Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

- Nivel de consulta de la información.- privilegio de lectura.
- Nivel de mantenimiento de la información.- El concepto de mantenimiento de la información consiste en: Ingreso, Actualización, Borrado.



Clase de Riesgo: Manipulación y Sabotaje

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Aleatorio Grado de Impacto: Grave
Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadas a causar daños físicos y lógicos en el sistema de información de la institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje	<p>La protección contra el sabotaje requiere:</p> <p>Una selección rigurosa del personal.</p> <p>Buena administración de los recursos humanos</p> <p>Buenos controles administrativos</p> <p>Buena seguridad física en los ambientes donde están los principales componentes del equipo.</p> <p>Asignar a una persona la responsabilidad de la protección de los equipos en cada área.</p>
No se comunica el movimiento de personal al DTIC, para restringir accesos del personal que es reubicado y/o cesado del SNAI.	Es conveniente la comunicación anticipada del personal que será reubicado y/o cesado con el objeto de retirar los derechos de operación de escritura para otorgarle los derechos de consulta antes de desactivar la cuenta.
Existe el antecedente de origen sabotaje interno. Como es el caso de trabajadores que han sido despedidos y/o están enterados que van a ser rescindidos su contrato, han destruidos o modificado archivos para su beneficio inmediato o futuro.	Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado.

El peligro más temido por los centros de Procesamiento de Datos, es el sabotaje. Instituciones que han intentado implementar Programas de Seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un trabajador o un sujeto ajeno a la propia institución. Un acceso no autorizado puede originar sabotajes.

Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existen un plan idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática u un problema “puntual”, sino que requiere un constante y continuo esfuerzo y dedicación.

Acciones a tomar

Se previene a través de las siguientes acciones:

La protección contra el sabotaje requiere:

1. Una selección rigurosa del personal.
2. Buena administración de los recursos humanos.
3. Buenos controles administrativos.
4. Buena seguridad física en los ambientes donde están los principales componentes del equipo.
5. Asignar a una persona la responsabilidad de la protección de los equipos en cada área.

A continuaciones algunas medidas que se deben tener en cuenta para evitar acciones hostiles:

1. Mantener una buena relación de trabajo con el departamento de policía local.
2. Mantener adecuados archivos de reserva (backups).
3. Planear para probar los respaldos (backups) de los servicios de procesamiento de datos.
4. Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
5. Usar rastros de auditorías o registros cronológicos (logs) de transacción como medida de seguridad.

Cuando la información eliminada se pueda volver a capturar, se procede con lo siguiente:

- Capturar los datos faltantes en las bases de datos de los sistemas. Responsable: Áreas afectadas
- Revisar y probar la integridad de los datos. Responsable: Desarrollo de Sistemas.

La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas demandan demasiado tiempo requerido para el inicio de las operaciones normales, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verían afectados.



2.2 Análisis de las fallas en la Seguridad

El presente realiza un análisis de todos los elementos de riesgos a los cuales está expuesto

En este se abarca el estudio del hardware, software, la ubicación física de la estación su utilización, con el objeto de identificar los posibles resquicios en la seguridad que pudieran suponer un peligro.

Las fallas en la seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona, de ahí que resulte obvio el interés creciente sobre este aspecto. La seguridad de la información tiene dos aspectos importantes como:

- Negar el acceso a los datos a aquellas personas que no tengan derecho a ellos.
- Garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

2.3 Protecciones actuales

Se realizan las siguientes acciones:

- Se hace copias de los archivos que son vitales para la institución.
- Al robo común se cierran las puertas de entrada y ventanas
- Al vandalismo, se cierra la puerta de entrada.
- A la falla de los equipos, se realiza el mantenimiento de forma regular.
- Al daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus.
- A las equivocaciones, los empleados tienen buena formación. Cuando se requiere personal temporal se intenta conseguir a empleados debidamente preparados.
- A terremotos, no es posible proteger la instalación frente a estos fenómenos. El presente Plan de contingencias da pautas al respecto.
- Al acceso no autorizado, se cierra la puerta de entrada. Varias computadoras disponen de llave de bloqueo del teclado.
- Al robo de datos, se cierra la puerta principal y gavetas de escritorios. Varias computadoras disponen de llave de bloqueo del teclado.
- Al fuego, en la actualidad se encuentran instalados extintores, en sitios estratégicos y se brindara entrenamiento en el manejo de los extintores al personal, en forma periódica.





2.3.1 Seguridad de la Información

La Seguridad de información y por consiguiente de los equipos informáticos, es un tema que llega a afectar la imagen institucional de las empresas, incluso la vida privada de personas. Es obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática.

Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y a menudo es vulnerable a cualquier ataque.

La Seguridad de información tiene tres directivas básicas que actúan sobre la Protección de Datos, las cuales ejercen control de:

La lectura

Consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales y mantenimiento de la seguridad en el caso de datos institucionales.

La escritura

Es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad que se les ha confiado.

El empleo de esa información

Es Secreto de logra cuando no existe acceso a todos los datos sin autorización. La privacidad se logra cuando los datos que puedan obtenerse no permiten el enlace a individuos específicos o no se pueden utilizar para imputar hechos acerca de ellos.

Por otro lado, es importante definir los dispositivos de seguridad durante el diseño del sistema y no después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a esos criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

2.3.1. 1. Acceso no autorizado

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados:

Control de acceso a la DTIC

La libertad de acceso a la DTIC puede crear un significativo problema de seguridad. El acceso normal debe ser dado solamente a la gente que trabaja en esta oficina. Cualquier otra persona puede tener acceso únicamente bajo control.

Debemos mantener la seguridad física de la Oficina como primera línea de defensa. Para ello se toma en consideración el valor de los datos, el costo de protección, el impacto institucional por la pérdida o daño de la información.



La forma propuesta de implantar el Control de Acceso a la DTIC, sería la siguiente:

- Para personas visitantes, vigilancia otorgara el Credencial de Visitante.
- Para personal del SNAI, con autorización del encargado de la Oficina

Acceso limitado computadoras personales y/o terminales de la red.

Los terminales que son dejados sin protección pueden ser mal usados. Cualquier Terminal puede ser utilizado para tener acceso a los datos de un sistema controlado.

Control de acceso a la información confidencial.

Sin el debido control, cualquier usuario encontrara la forma de lograr acceso al Sistema de Red, a una base de datos o descubrir información clasificada. Para revertir la posibilidad de ataque se debe considerar:

Programas de control a los usuarios de red

El sistema Operativo residente en los servidores de la DTIC es Windows 2012, 2016 y Linux Server. A través del Servicio de “Active Directory” permite administrar a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.

Contraseña (Password)

Es una palabra o código que se ingresa por teclado antes que se realice un proceso.

Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados. La identificación del usuario debe ser muy difícil de imitar y copiar.

El Sistema de Información debe cerrarse después que el usuario no autorizado falle tres veces de intentar ingresar una clave de acceso. Las claves de acceso no deben ser largas puesto que son más difíciles de recordar. Una vez que se obtiene la clave de acceso al sistema, esta se utiliza para entrar al sistema de Red de Información vía Sistema Operativo.

La forma común de intentar descubrir una clave es de dos maneras:

- Observando el ingreso de la clave
- Utilizando un método de ensayo y error para introducir posibles claves de acceso y lograr entrar.

En todo proceso corporativo es recomendable que el responsable de cada área asigne y actualice de forma periódica el “password” a los usuarios.

Niveles de Acceso

Las políticas de acceso aplicadas, deberá identificar los usuarios autorizados a emplear determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas. Cada palabra clave deberá tener asignado uno de los niveles de acceso a la información o recursos de red disponibles en el SNAI.

La forma fundamental de autoridad la tiene el Administrador de Redes con derechos totales. Entre otras funciones puede autorizar nuevos usuarios, otorgar derechos para modificar estructuras de las Bases de Datos, etc.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

Nivel	Concepto
Consulta de la información	El privilegio de lectura está disponible para cualquier usuario y solo se requiere presentaciones visuales o reportes. La autorización de lectura permite leer pero no modificar la Base de Datos.
Mantenimiento de información	Permite el acceso para agregar nuevos datos, pero no modifica los ya existentes, permite modificar pero no eliminar los datos. Para el borrado de datos, es preferible que sea responsabilidad de la DTIC.

2.3.1. 2. Destrucción

Sin adecuadas medidas de seguridad la institución puede estar a merced no solo de la destrucción de la información sino también de la destrucción de sus equipos informáticos. La destrucción de los equipos puede darse por una serie de desastres como son: incendios, inundaciones, sismos, posibles fallas eléctricas o sabotaje, etc.

Cuando se pierden los datos y no hay copias de seguridad, se tendrá que recrear archivos, bases de datos, documentos o trabajar sin ellos.

Está comprobado que una gran parte del espacio en disco está ocupado por archivos de naturaleza histórica, que es útil tener a mano pero no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia conservados como documentos de referencia o plantilla. Si se guarda una copia de seguridad de estos archivos las consecuencias de organización pueden ser mínimas.

Los archivos Electrónicos Contable son de disposición diferente, ya que volver a crearlos puede necesitar de mucho tiempo y costo. Generalmente la institución recurre a esta información para la toma de decisiones.

Sin los datos al día, si el objetivo se vería seriamente afectado. Para evitar daños mayores se hacen copias de seguridad de la información vital para la institución y se almacenan en lugares apropiados (de preferencia en lugar externo a las instalaciones).

Hay que protegerse también ante una posible destrucción del hardware o software por parte del personal no honrado. Por ejemplo, hay casos en la que, trabajadores que han sido recientemente despedidos o están enterados que ellos van a ser cesados, han destruido o modificado archivos para su beneficio inmediato o futuro. Depende de los Jefes inmediatos de las áreas funcionales dar importancia a estos eventos, debiendo informar al Director de TIC para el control respectivo.

2.3.1. 3. Revelación o Deslealtad

La revelación o deslealtad es otra forma que utilizan los malos trabajadores para su propio beneficio. La información de carácter confidencial es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

- Control de uso de información en paquetes/ expedientes abiertos, cintas/disquetes y otros datos residuales. La información puede ser conocida por personal no autorizadas.
- Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de esa a aquellas personas que pueden usar mal los datos residuales de estas.
- Mantener información impresa o magnética fuera del trayecto de la basura.

El material de papel en la plataforma de descarga de la basura puede ser la fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Para tener una mayor seguridad de protección de la información residual y segregada, esta deberá ser destruida, eliminada físicamente, manualmente o mecánicamente (picadoras de papel).

Desafortunadamente, es muy común ver grandes volúmenes de información sensitiva tirada alrededor de la Oficinas y relativamente disponible a gran número de personas.

2.3.1. 4. Modificaciones

Hay que estar prevenido frente a la tendencia a asumir que “si viene de la computadora, debe ser correcto”.

La importancia de los datos modificados de forma ilícita, esta condicionada al grado en que la institución, depende de los datos para su funcionamiento y

toma de decisiones. Esto podría disminuir su efecto si los datos procedente de las computadoras se verificaran antes de constituir fuente de información para la toma de decisiones.

Los elementos en la cual se han establecido procedimientos para controlar modificaciones ilícitas son:

- Los programas de aplicación: adicionalmente a proteger sus programas de aplicación como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionales a los datos o a su uso no autorizado.
- La información en Bases de Datos: como medidas de Seguridad, para proteger los datos en el sistema, efectuar auditorias y pruebas de consistencia de datos en nuestros históricos. Particular atención debe ser dada al daño potencial que pueda efectuar un programador a través de una modificación no autorizada.
- Nuestra mejor protección contra la pérdida/modificación de datos consiste en hacer copias de seguridad, almacenando en copias no autorizadas de todos los archivos valiosos en un lugar seguro.
- Los usuarios: los usuarios deben ser concientizados de la variedad de formas en que los datos pueden perderse o deteriorarse. Una campaña educativa de este tipo puede iniciarse con una reunión especial de los empleados, profundizarse con una serie de seminarios y reforzarse con carteles y circulares relacionados al tema.

Para la realización de las Copias de Seguridad se tiene que tomar algunas decisiones previas como:

- ¿Qué soporte de copias de seguridad se va utilizar?
- ¿Se van a usar dispositivos especializados para copia de seguridad?
- ¿Con que frecuencia se deben realizar las copias de seguridad?
- ¿Cuáles son los archivos a los que se le sacara copia de seguridad y donde se almacenara?

La DTIC establecerá Directivas y/o Reglamentos en estas materias, para que los usuarios tomen conocimiento de sus responsabilidades. Tales reglas y normativas deben incorporarse en una campaña de capacitación colectiva.

La institución debe tener en cuenta los siguientes puntos para la protección de los datos de una posible contingencia:

- Hacer de la copia de seguridad una política, no una opción.
- Hacer de la copia de seguridad resulte deseable.
- Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).
- Hacer de la copia de seguridad obligatoria.



3.- Recuperación del desastre y respaldo de la información

El costo de la Recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior de edificios e instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El Costo de Recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior a 07 o un incendio de controlable, estará dado por el valor no asegurado de equipos informáticos e información más el Costo de Oportunidad, que significa, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos e información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de Actividades Posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de crear el plan y coordinar las funciones. Típicamente las personas pueden ser: personal del CIT, personal de Seguridad.

Las actividades a realizar en un Plan de Recuperación de Desastres se clasifican en tres etapas:

1. Actividades Previas al Desastre.
2. Actividades Durante el Desastre.
3. Actividades Después del Desastre.





3.1 Actividades previas al desastre

Se considera las actividades de planteamiento, preparación, entrenamiento y ejecución de actividades de resguardo de la información, que aseguran un proceso de recuperación con el menor costo posible para la institución.

3.1.1. Establecimientos del Plan de Acción

En esta fase de planeamiento se establece los procedimientos relativos a:

- Sistemas e Información.
- Equipos de Cómputo.
- Obtención y almacenamiento de los Respaldos de Información (BACKUPS).
- Políticas (Normas y Procedimientos de Backups).

Sistemas de Información

La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los de desarrollo propio, como los desarrollados por empresas externas. Éstos están detallados en el Portafolio de Servicios de TI.

Equipos de Cómputo

Se debe tener en cuenta el catastro de Hardware, impresoras, lectoras, scanner, plotters, módems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación. Por ejemplo etiquetar de color rojo los servidores, color amarillo a los PC con información importante o estratégica, y color verde a las demás estaciones (normales, sin disco duro o sin uso).
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la institución.

Obtención y almacenamiento de Copias de Seguridad (Backups)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución. Las copias de seguridad son las siguientes:



- Backup del Sistema Operativo: o de todas las versiones de sistema operativo instalados en la Red.
- Backup de Software Base: (Lenguajes de Programación utilizados en el desarrollo de los aplicativos institucionales).
- Backup del software aplicativo: backups de los programas fuente y los programas ejecutables.
- Backups de los datos (Base de datos, password y todo archivo necesario para la correcta ejecución del software aplicativos de la institución).
- Backups del Hardware, se puede implementar bajo dos modalidades:
 - **Modalidad Externa:** mediante el convenio con otra institución que tenga equipos similares o mejores y que brinden la capacidad y seguridad de procesar nuestra información y ser puestos a nuestra disposición al ocurrir una contingencia mientras se busca una solución definitiva al siniestro producido.

En este Caso se debe definir claramente las condiciones del convenio a efectos de determinar la cantidad de equipos, periodos de tiempo, ambientes, etc., que se puede realizar con la entidad que cuente con equipo u mantenga un Plan de Seguridad de Hardware.

- **Modalidad Interna:** si se dispone de más de un local, en ambos se debe tener señalado los equipos, que por sus capacidades técnicas son susceptibles de ser usados como equipos de emergencia

Es importante mencionar que en ambos casos se debe probar y asegurar que los procesos de restauración de información posibiliten el funcionamiento adecuado de los sistemas.

Políticas (Normas y Procedimientos)

Todas las detalladas en este documento Capítulo 1

3.1.2. Formación de equipos operativos.

En cada unidad operativa, que almacene información y sirva para la operatividad institucional, se deberá designar un responsable de la seguridad de la información de su unidad. Pudiendo ser el Jefe Administrativo de dicha Área, y sus funciones serán las siguientes:

- Contactarse con los autores de las aplicaciones y personal de mantenimiento respectivo.

El equipo encargado debe estar formado por las siguientes unidades:

- Unidad de Arquitectura y Proyectos Tecnológicos
- Unidad de Desarrollo y mantenimiento de Sistemas
- Unidad de Infraestructura y Operaciones.
- Unidad de Seguridad Informática, Interoperabilidad y Riesgos Informáticos.

- Proporcionar las facilidades (procedimientos, técnicas) para realizar copias de respaldo.
- Esta actividad está dirigida por el Equipo de Soporte y Mantenimiento.
- Supervisar el procedimiento de respaldo y restauración
- Establecer procedimientos de seguridad en los sitios de recuperación
- Organizar la prueba de hardware y software: el encargado y el usuario final dan su conformidad.
- Ejecutar trabajos de recuperación y comprobación de datos.
- Participar en las pruebas y simulacros de desastres: en esta actividad deben participar el encargado de la ejecución de actividades operativas, y los servidores administrativos del área, en el cumplimiento de actividades preventivas al desastre del Plan de Contingencias.

3.1.3. Formación de Equipos de Evaluación.

En cada unidad operativa, que almacene información y sirva para la operatividad institucional, se deberá designar un responsable de la seguridad de la

Esta función debe ser realizada preferentemente por el personal de auditoria o inspectora, de no ser posible, lo realizaría el personal del área de informática-TIC, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- Revisar que las normas y procedimientos con respecto a backups, seguridad de equipos y data se cumpla.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, es decir, información generada en el área funcional, software general y hardware.
- Revisar la correlación entre la relación de los Sistemas e información necesarios para la buena marcha de la institución y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las normas para las acciones de corrección necesarias.



3.2 Actividades Durante el Desastre

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:

- ✓ Plan de Emergencias
- ✓ Formación de Equipos
- ✓ Entrenamiento

3.2.1. Plan de Emergencias

La presente etapa incluye las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro. Solo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas.

Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación, debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que la acción del siniestro causen más daños o destrucciones. Se debe tener en toda Oficina los números de teléfono y direcciones de organismos e instituciones de ayuda. Todo el personal debe conocer lo siguiente:

- ✓ Localización de vías de Escape o Salida: Las vías de escape o salida para solicitar apoyo o enviar mensajes de alerta, a cada oficina debe señalizar las vías de escape
- ✓ Plan de Evaluación Personal: el personal ha recibido periódicamente instrucciones para evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por Defensa Civil a nivel local. Esa actividad se realizara utilizando las vías de escape mencionadas en el punto anterior.
- ✓ Ubicación y señalización de los elementos contra el siniestro: tales como los extintores, las zonas de seguridad que se encuentran señalizadas (ubicadas normalmente en las columnas), donde el símbolo se muestra en color blanco con fondo verde. De existir un repintado de paredes deberá contemplarse la reposición de estas señales
- ✓ Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, lista de teléfonos de instituciones como: Compañía de Bomberos, Hospitales, Centros de Salud, Ambulancias, Seguridad.





3.2.2. Formación de Equipos

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, de acuerdo a los lineamientos o clasificación de prioridades

3.2.3. Entrenamiento

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo a los roles que se hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden realizar recarga de extintores, charlas de los proveedores, etc.

Es importante lograr que el personal tome conciencia que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los Directores, Asesores, Responsables de Unidad, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.





CAPÍTULO 10.- CATÁLOGO DE SERVICIOS





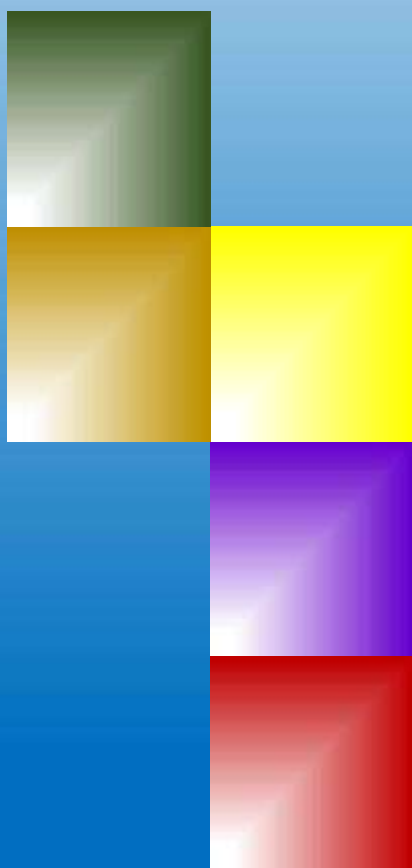
2020

Catálogo de Servicios Institucionales

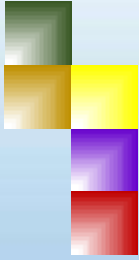
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Detalle de los servicios disponibles por parte de la Dirección de Tecnologías
para todo el personal del SNAI.

JUAN CARLOS MUÑOZ M.
Servicio Nacional de Atención Integral a Personas
Adultas Privadas de la Libertad y a Adolescentes
Infractores



HARDWARE



HARDWARE

HARDWARE

Definición.- Partes tangibles de un sistema informático.

Como parte del equipo de HARDWARE del SNAI, se encuentra:

1. Monitor
2. PC
3. Laptop
4. Tablet
5. Smartphone
6. Impresora
7. Escáner
8. Proyector
9. Teléfono IP
10. Dispositivos USB
11. Servidores
12. Copiadora
13. Equipos Biométricos
14. Equipos de conectividad

ALCANCE.-

Todo equipo perteneciente al SNAI.



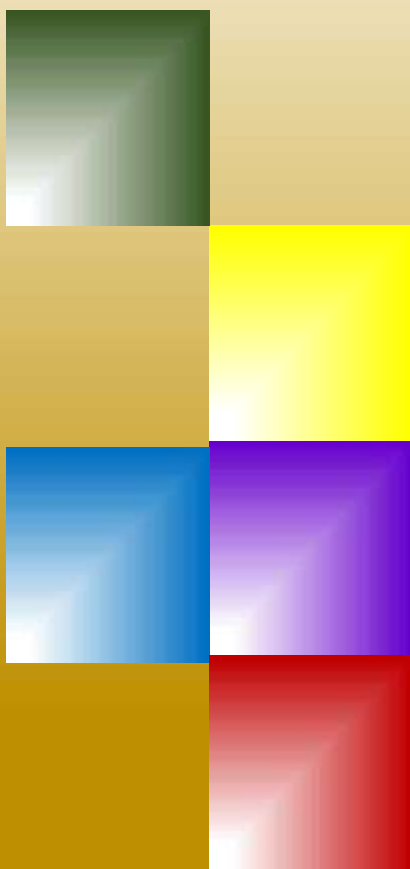
HARDWARE

(<http://soporte.atencionintegral.gob.ec/>)

un eMail a soporte@atencionintegral.gob.ec, automáticamente se generará un No. de ticket con el cual puede dar seguimiento a su requerimiento en la página indicada anteriormente.

Solicitud de Asistencia
<http://soporte.atencionintegral.gob.ec/>

Solicitud de Asistencia
Soporte@atencionintegral.gob.ec



SOFTWARE



SOFTWARE

Definición.- Parte lógica o intangible de un sistema informático. Como parte del equipo de SOFTWARE del SNAI, cumpliendo las disposiciones emitidas por el Gobierno Nacional, a través de Decreto Ejecutivo No. 1014 de fecha 10 de abril del 2008, se encuentra:

1. Software Free
2. Sistema Operativo Windows Licenciado.
3. Office Licenciado
4. Antivirus Licenciado
5. Adobe Licenciado
6. Adicionales licenciados

ALCANCE.-

Todo equipo perteneciente al SNAI.



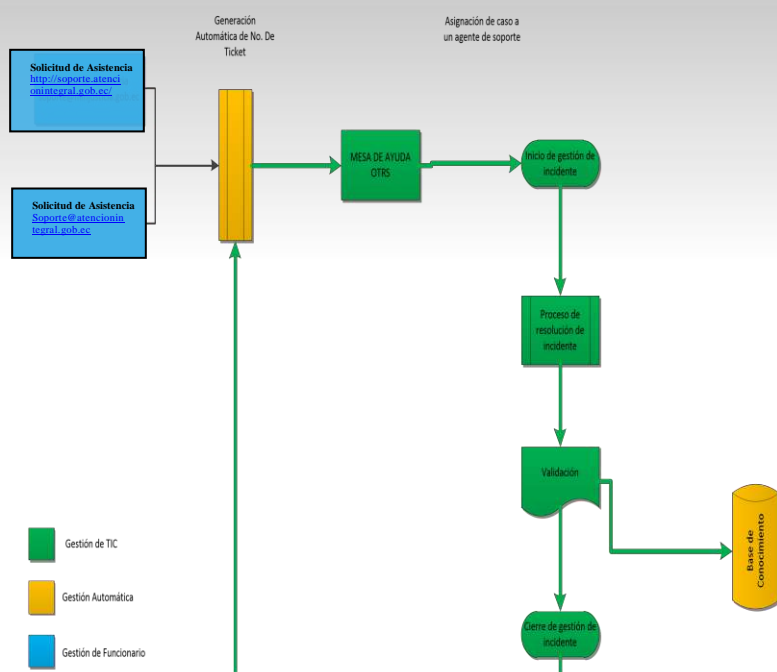
SERVICIO - SOFTWARE

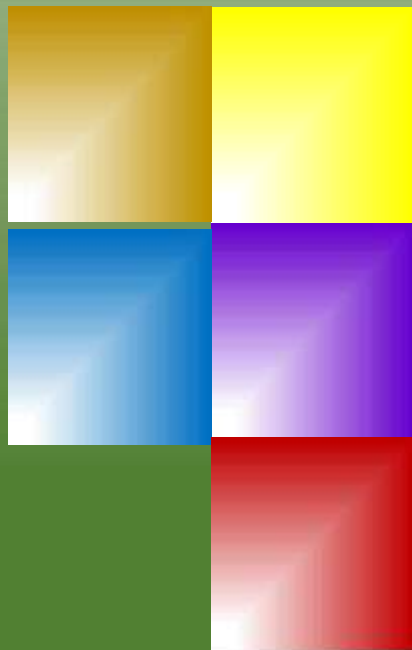
Dentro de los servicios prestados para el SOFTWARE está:

1. Configuración
2. Puesta en marcha
3. Actualización
4. Soporte técnico funcional
5. Revisión y levantamiento de Informe Técnico
6. Instalación de nuevas soluciones

COMO SOLICITAR AYUDA?

El funcionario que requiera un soporte técnico debe “Crear un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) o si no puede acceder a la plataforma GLPI, enviará un eMail a soporte@atencionintegral.gob.ec; automáticamente se generará un No. de ticket con el cual puede dar seguimiento a su requerimiento en la página indicada anteriormente.





SISTEMAS DE GOBIERNO



SISTEMAS DE GOBIERNO

SISTEMAS DE GOBIERNO

Definición.- Software desarrollado, administrador y generalizado para el servicio público.

Los sistemas de Gobierno son programas desarrollados por la Presidencia de la República, a través de su respectiva Secretaría de Administración Pública y/o el SNAI responsable de dicha administración:

1. Quipux
2. eSIGEF
3. SINAFIP
4. SPRIN
5. SIITH
6. SIGOB
7. GPR
8. Viajes
9. Portal de Compras Públicas

ALCANCE.-

Todo personal perteneciente al SNAI.



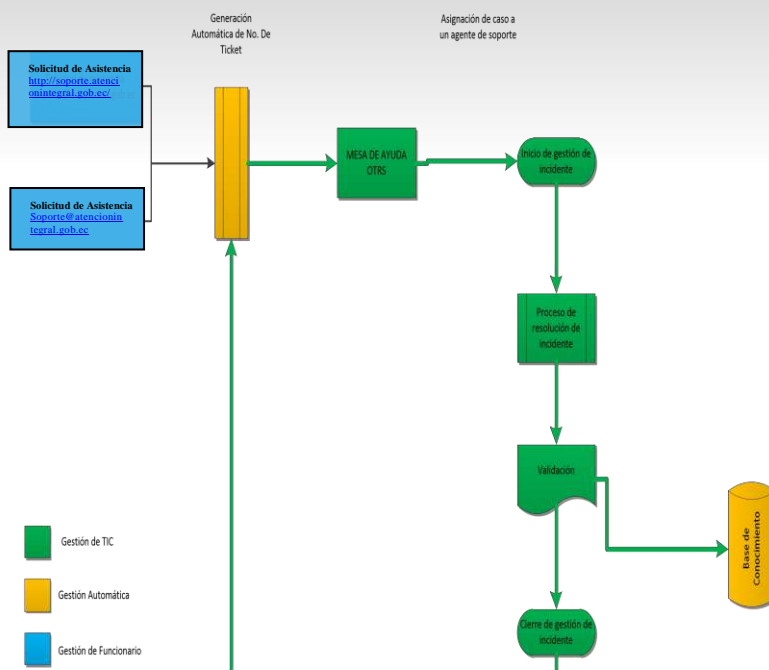
Sistema Oficial de Contratación Pública

SERVICIO – SISTEMAS DE GOBIERNO

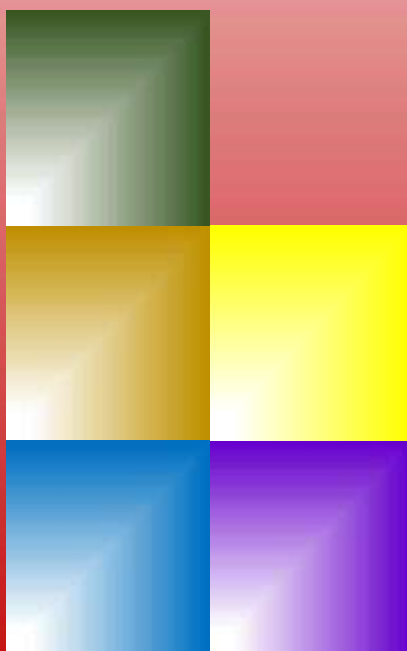
Dentro de los servicios prestados para los Sistemas de Gobierno están:

1. Creación de usuarios
2. Eliminación de usuarios
3. Actualización de datos
4. Soporte técnico funcional
5. Instalación de nuevas soluciones

COMO SOLICITAR AYUDA?



El funcionario que requiera un soporte técnico debe “Crear un Caso” dentro de “Soporte TICs” (<http://soporte.atencionintegral.gob.ec/>) o si no puede acceder a la plataforma GLPI, enviará un eMail a Quipux: Soporte@gobiernoelectronico.gob.ec
eSiGeF: EGuerrero@finanzas.gob.ec
SINAFIP: AdmUsuarios@finanzas.gob.ec
automáticamente se generará un No. de ticket con el cual puede dar seguimiento a su requerimiento en las páginas indicadas anteriormente.



SERVICIOS INTERNOS



SERVICIOS INTERNOS

SERVICIOS INTERNO

Definición.- Servicios brindados por la DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.

Dentro de los servicios internos:

1. Perfiles de usuario
2. Correo electrónico
3. Navegación
4. Preparación de equipos
5. Carpetas compartidas

ALCANCE.-

Todo personal perteneciente al SNAI.



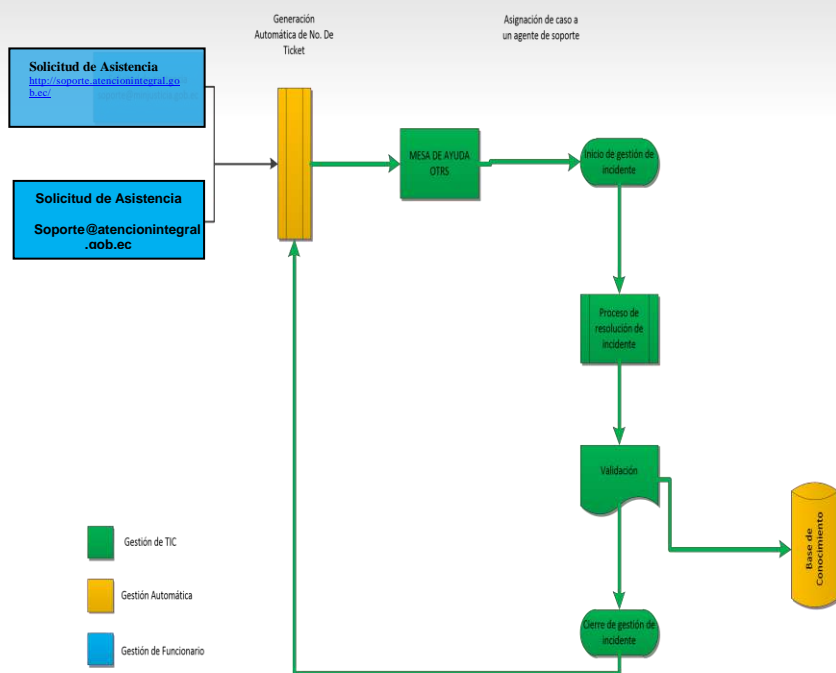
SERVICIOS INTERNOS

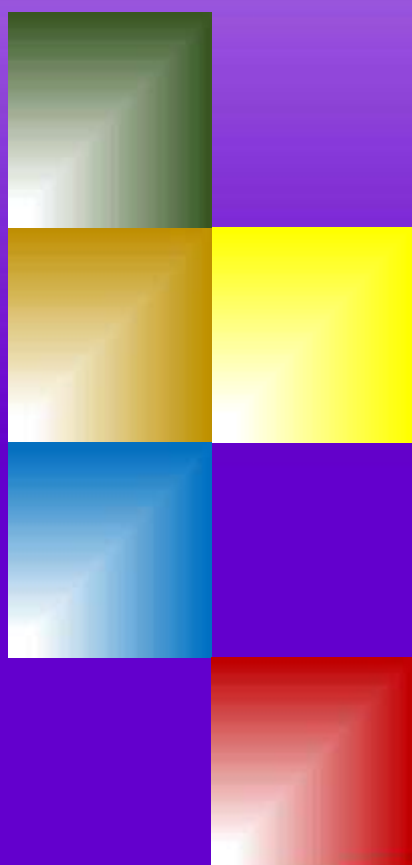
Dentro de los servicios prestados internamente:

1. Creación de perfiles de usuarios
2. Eliminación de perfiles de usuarios
3. Creación de correo electrónico
4. Actualización de datos
5. Creación de perfiles en equipos
6. Aumento de tamaño de buzón
7. Acceso a carpetas compartidas
8. Soporte técnico funcional

COMO SOLICITAR AYUDA?

El funcionario que requiera un soporte técnico debe **“Crear un Caso”** dentro de **“Soporte TICs”** (<http://soporte.atencionintegral.gob.ec/>) o si no puede acceder a la plataforma GLPI, enviará un eMail a soporte@atencionintegral.gob.ec; automáticamente se generará un No. de ticket con el cual puede dar seguimiento a su requerimiento en la página indicada anteriormente.





CONECTIVIDAD Y
COMUNICACIONES



CONECTIVIDAD Y COMUNICACIONES

CONECTIVIDAD Y COMUNICACIONES

Definición.- Servicios proporcionados por la Dirección de Tecnologías para facilitar las labores internas de comunicación.

Dentro de los servicios internos:

1. Internet
2. Intranet
3. Telefonía IP

ALCANCE.-

Todo personal y equipos pertenecientes al SNAI.



SERVICIOS INTERNOS

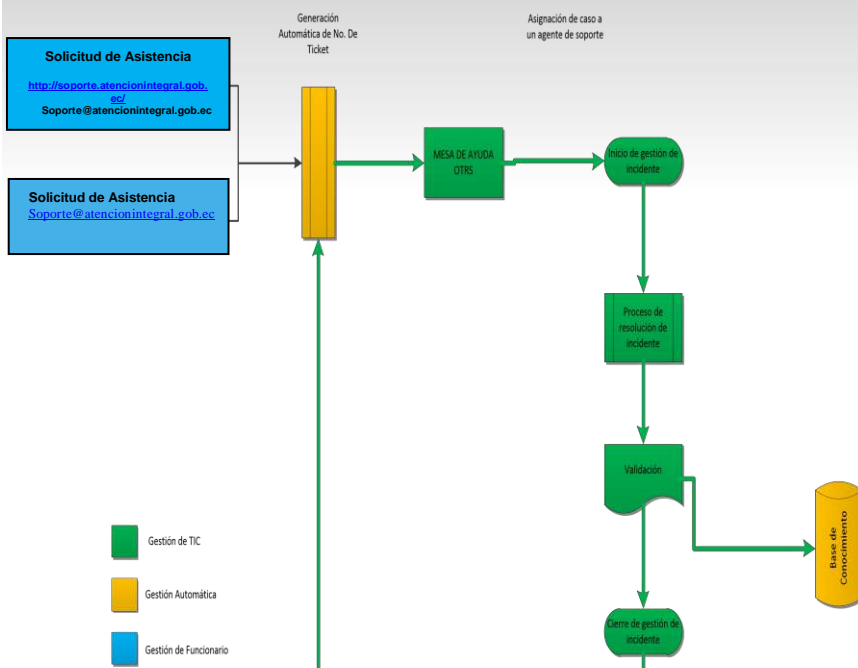
Dentro de los servicios de conectividad y comunicaciones están:

1. Creación de perfiles de usuarios
2. Configuración de proxy
3. Configuración de teléfonos IP
4. Central Telefónica
5. Navegación restringida

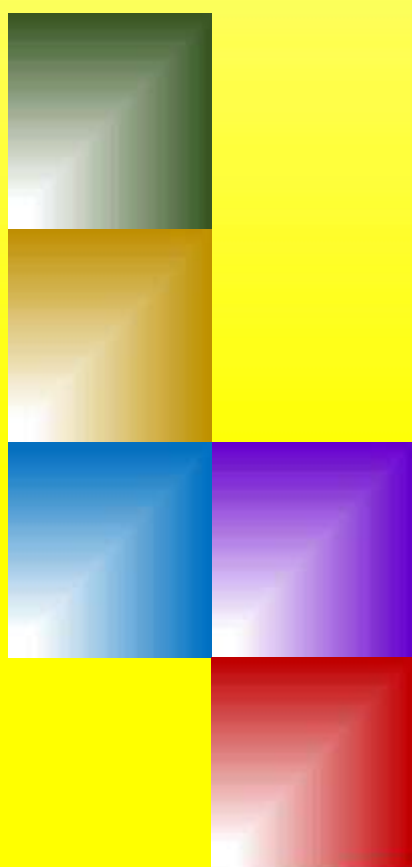
COMO SOLICITAR AYUDA?

El funcionario que requiera un soporte técnico debe ingresar obligatoriamente a la Intranet institucional <http://intranet.atencionintegral.gob.ec/snai/> y seleccionar “Soporte TICs” (<http://soporte.atencionintegral.gob.ec>) y luego de ingresar las credenciales similares a las de acceso al computador seleccionar “Crear un Caso”, automáticamente se generará un No. de ticket y recibirá la confirmación en su correo electrónico, con el cual puede dar seguimiento a su requerimiento en la página indicada anteriormente.

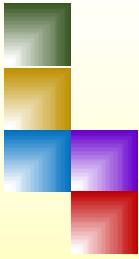
En caso de haber inconveniente con el acceso a la plataforma enviar un correo electrónico a Soporte@atencionintegral.gob.ec



CONECTIVIDAD Y COMUNICACIONES



APLICACIONES
PROPIAS DEL
SNAI



APLICACIONES PROPIAS DEL SNAI

APLICACIONES PROPIAS DEL SNAI

Definición.- Servicios desarrollados por el propio SNAI para el bien de la comunidad y/o propios funcionarios.

Dentro de los servicios internos:

1. S . G . P . (eSIGPEN)
2. Sistema de Garantías
3. SisVIS – sistema de Visitas a PPLs
4. Alfresco – Repositorio de documentación
5. EasyMark – Asistencia y Permisos
6. SisCAI – Sistema Gestiónadolescentes Infractores
7. Moddle – Información y Autocapacitación
8. GLPI – Mesa de ayuda
9. SisASP – Gestión de Agentes de Seguridad Penitenciaria

ALCANCE.-

Todo personal y equipos pertenecientes al SNAI.



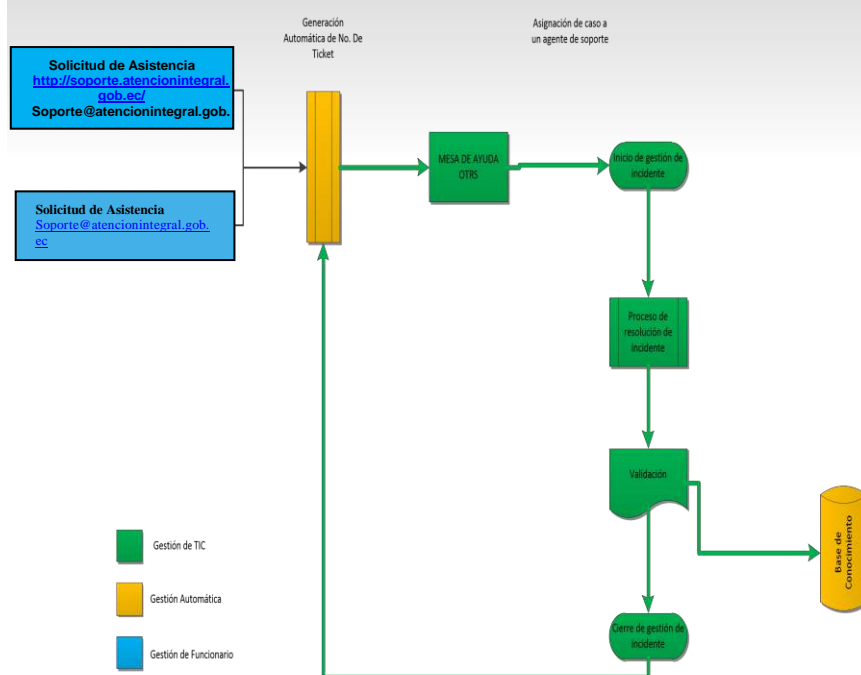
SERVICIOS INTERNOS

Dentro de los servicios de las aplicaciones propias del SNAI están:

1. Creación de perfiles de usuarios
2. Configuración de perfiles
3. Gestión de procesos

COMO SOLICITAR AYUDA?

El funcionario que requiera un soporte técnico enviará un eMail a soporte@atencionintegral.gob.ec; automáticamente se generará un No. de ticket con el cual puede dar seguimiento a su requerimiento en la página indicada anteriormente.



APLICACIONES PROPIAS DEL SNAI