Instituto Salvadoreño de Formación Profesional

POLÍTICAS GENERALES Y CONTROLES ESPECIFICOS PARA LOS SISTEMAS DE INFORMACIÓN

Antiguo Cuscatlán, Octubre 2014

INDICE

I. OBJETIVO

Definir las principales políticas y controles de aplicaciones específicas aplicables a los Sistemas de Información del INSAFORP.

II. ALCANCE

El presente manual define las políticas de acuerdo al análisis efectuado en lNSAFORP, sobre la administración y control de:

a) Centro de datos
b) Adquisición, mantenimiento de software y hardware del sistema
c) Antivirus
d) Uso y acceso a VPN
e) Custodia de activos informáticos
f) Solicitud de computadora y accesorio de cómputo
g) Acceso a dispositivos
h) Información institucional
i) Uso aceptable de equipo informático
j) Software
k) Cuenta de acceso a red
l) Puntos de red
m) Desarrollo y mantenimiento de aplicaciones
n) Correo electrónico
o) Impresión
p) Uso de redes sociales
q) Equipo de préstamo
r) Atención de help desk

Unidades involucradas:

a. Gerencia de Tecnologías de la información.
b. Unidades Organizativas que utilizan los recursos tecnológicos en la institución.
c. Personal sub-contratado y personal que hace uso de los servicios tecnológicos del INSAFORP

III. BASE LEGAL

Normas Técnicas de Control Interno específicas para INSAFORP, Art. 31 y 32.

IV. POLÍTICAS

El objeto de las políticas es definir los lineamientos generales y específicos, para realizar acciones y administrar sistemas de Información, que contribuyan al logro de objetivos institucionales.

i. CENTRO DE DATOS

i. Plan de contingencia

Para garantizar el restablecimiento de servicios, luego de presentar algún siniestro la Gerencia de TI administrará un plan de contingencia; gestionando entre otros, el resguardo de dato mediante una caja de seguridad externa.

ii. Infraestructura del hardware

Los activos informáticos de misión crítica (servidores, equipos de comunicación, etc.) deberán estar ubicados en áreas que cumplan con requisitos de alimentación eléctrica controlada y regulada.

iii. Acceso al centro de cómputo (Cuarto de Servidores)

1. Sólo al personal autorizado le está permitido el acceso al Centro de Cómputo.
2. Sólo bajo supervisión de personal autorizado, puede el personal externo tener acceso al Centro de Cómputo.
3. No se permite consumir ningún tipo de alimentos y/o bebidas en el centro de cómputo, tomar fotografías (Sin autorización) y tampoco se permite el uso de teléfonos celulares (Sin autorización) dentro de dicha ubicación.

iv. Cambio de servidores.

1. Los servidores deben de iniciar su proceso de evaluación de reemplazo cuando estos alcancen un uso superior al 50% de sus recursos o cuando cumplan su vida útil de cinco años.
2. Se deberá analizar si satisface la demanda actual y capacidad de crecimiento para soportar la carga de trabajo del área.
3. Se deben adquirir con partes redundantes, para alta disponibilidad, en los siguientes componentes: fuentes de poder, tarjetas de red, ventiladores y discos.
4. Todo servidor debe de comprarse con una garantía mínima de tres años.

v. Cambio de Switch

1. Los Switch deben iniciar su proceso de cambio cuando cumplan su vida útil de cinco años, no soporten la demanda de los servicios que se administran o por mejorar la seguridad.
2. Se deberá analizar si satisface la demanda actual y capacidad de crecimiento para soportar la carga de trabajo del área.
3. Deberán de comprarse con una garantía mínima de tres años.
4. Se deben adquirir con la opción de ser administrables
5. Se deberán adquirir con fuente redundante

vi. Wireless

Los recursos de red inalámbrica deben emplearse en tareas relacionadas con la función institucional.

1. Consultores, auditores u otras personas que realicen actividades para la institución podrán acceder a servicios de internet e impresión, mediante solicitud del Gerente/Jefe/Coordinador responsable de los servicios y estos serán proporcionados dependiendo de la disponibilidad.

2. A fin de satisfacer la demanda de conexión a internet de personal externo, se creará una red inalámbrica que no tenga acceso a la red interna del INSAFORP.
3. De las redes inalámbricas del INSAFORP no se tendrá acceso a servicios de FTP, Telnet y otros que permitan la transferencia de archivos.
4. Los Access Point deberán tener una clave de acceso asignada, la cual deberá ser cambiada periódicamente.

vii. Internet

1. La determinación de las especificaciones de servicios de comunicación de datos, lo establecerá la Gerencia de Tecnologías de la Información, para la cual se evaluará la demanda.
2. El uso del servicio de Internet estará relacionado a la consecución de los objetivos institucionales. Todo servicio que la Gerencia de TI evalué como no indispensable para el quehacer institucional será bloqueado.
3. Dentro del INSAFORP el Internet es una herramienta de trabajo, por lo que todos los equipos cuentan con acceso a Internet y éste se concede exclusivamente para actividades de trabajo.
4. Internet es una red pública, cualquier persona puede interceptar información enviada o recibida, por tanto no se debe enviar por este medio, información de carácter confidencial de la institución.
5. El acceso a internet cuenta con restricciones según las categorías de los sitios web. El Gerente/Jefe/Coordinador/usuario podrá solicitar la habilitación de alguna categoría o sitio web específico para el desempeño de sus labores o del personal a su cargo.
6. Cada computadora tendrá instalado un Software de antivirus, el cual detectará en tiempo real los archivos infectados. Es responsabilidad de cada usuario reducir la posibilidad de infección de virus, es decir, evitar posibles infecciones.
7. Del Internet no se deberá descargar ejecutables, .exe, u otro tipo de archivo que no sea indispensable para la ejecución de sus tareas diarias.
8. No deberán navegar en sitios web con contenido dudoso/malicioso.
9. En caso de recibir un mensaje del antivirus en el cual se indique que la computadora ha sido infectada o que se ha detectado un virus, el usuario deberá comunicarse inmediatamente con el personal técnico de la Gerencia de TI para que se tomen las acciones respectivas.
10. El uso de Internet será restringido o suspendido a petición del Gerente/Jefe/Coordinador inmediato del usuario, o según recomendación del personal técnico de la Gerencia de TI, cuando el usuario haya sido recurrente al infectar su computadora debido a descarga de archivos del Internet.
11. El Gerente/Jefe/Coordinador podrá solicitar reporte de sitio visitados por sus colaboradores en forma escrita, Help desk o mediante correo electrónico, dirigida al Gerente de Tecnologías de la Información.
12. El Gerente/ Jefe/ Coordinador podrá solicitar eliminación del acceso a Internet en forma escrita, Help desk o mediante correo electrónico, dirigida al Gerente de Tecnologías de la Información, especificando sí la suspensión será de forma indefinida o temporal o por horario, además de los motivos para la misma.

viii. Mantenimientos preventivos y correctivos

1. Se debe de ejecutar mantenimiento preventivo por lo menos una vez al año a todo el equipo informático del INSAFORP. En el caso del equipo en el Centro de Cómputo se deberá ejecutar en horas no hábiles.
2. En el caso de que algún mantenimiento correctivo requiera compra de componentes, éstos deberán de ser de la marca y modelo apropiados para el servidor.

ix. Custodia y tenencia de activos informáticos

Los activos informáticos en el Centro de Cómputo serán custodiados por el encargado de administrar el centro de cómputo.

ii. ADQUISICIÓN, MANTENIMIENTO DE SOFTWARE Y HARDWARE DEL SISTEMA

1. Toda inversión por compra y/o arrendamiento de bienes informáticos (equipos de cómputo, equipo para la transmisión-recepción de datos, programas operativos y de aplicación específica), y servicios (desarrollo y mantenimiento de sistemas, procesamiento de datos y captura), deberán ajustarse a lo estrictamente indispensable para el cumplimiento de objetivos y metas institucionales. La Gerencia de Tecnología de Información determinará sobre su reemplazo o actualización.
2. La Gerencia de TI decidirá, para lograr el óptimo aprovechamiento de bienes informáticos, sobre la ubicación física de éstos en las Gerencia y Unidades Organizativas, incluyendo aquellos que por sus características técnicas, de operación y depreciación, requieran darse de baja.

x. Cambio de computadoras

1. Las computadoras se reemplazarán en caso que se cumplan las siguientes condiciones
   a) Fallas
   b) Dictamen del área de soporte técnico en el cuál se indique que el equipo debe ser reemplazado
   c) Cinco años después de adquirido el equipo
   d) No satisface la demanda actual o no soporta la carga de trabajo
   e) En casos especiales en los cuales se evalué que procederá al reemplazo.
2. PC y Computadoras portátil debe de comprarse con una garantía mínima de tres años.

   Nota importante: Todo reemplazo de equipo informático se realizará según disponibilidad del presupuesto vigente.

iii. ANTIVIRUS

1. Toda PC y LAPTOP con Windows deberá tener instalado y configurado su antivirus, el cual a su vez mantiene la configuración centralizada en las políticas de la consola de administración.
2. La Gerencia de TI es responsable de monitorear y mantener actualizados los antivirus institucionales.

3. El antivirus de cada computadora genera una alerta de cada archivo infectado con virus, además de indicar la ruta y origen de la infección de manera que la Gerencia de TI cuenta con un registro de cada acción realizada por el usuario, a fin de deducir responsabilidades.
4. Cada unidad cuenta con carpetas compartidas, por Gerencia/Unidad, de manera que los usuarios no tengan necesidad de utilizar memorias USB para trasladar información institucional, dentro de las instalaciones del INSAFORP.

iv. USO Y ACCESO A VPN

Una red virtual privada (VPN de las siglas en inglés de Virtual Private Network), es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

1. El Gerente/Jefe/Coordinadora/usuario podrá solicitar la instalación del cliente VPN.
2. El empleado es responsable de su conexión activa de VPN y debe impedir que personas no autorizadas tengan acceso a su equipo informático mientras la conexión VPN se encuentre establecida
3. La conexión VPN es un enlace remoto con la red del INSAFORP, es decir que aplican las mismas políticas cual si estuviese el equipo conectado localmente en las oficinas centrales.
4. Todo acceso a través del VPN queda registrado en los equipos de comunicación del INSAFORP.

v. CUSTODIA DE ACTIVOS INFORMÁTICOS

1. Los activos informáticos de Usuario final (PC´s, monitores, teclados, impresoras, etc.) serán custodiados por el empleado.
2. Los usuarios a quienes se les asignan los activos informáticos, serán responsables del cuido y buen uso de los mismos.

vi. COMPUTADORA Y ACCESORIO DE CÓMPUTO

1. Los Gerente/Jefes/Coordinadores, se les asignará equipo portátil.
2. Los empleados que por sus funciones requieran de equipo informático, se les asignara una computadora personal. El Gerente/Jefe/Coordinador podrá solicitar un equipo portátil para el empleado que por su función lo requiera y dicha solicitud estará sujeta de aprobación por la Dirección Ejecutiva y disponibilidad.
3. Toda solicitud de computadora o accesorio de computo deberá de ser canalizado por medio del Help desk.
4. Cuando un equipo falla el área de Soporte Técnico de la Gerencia de TI, realizará una revisión e identifica si es necesario un cambio o reparación del equipo o accesorio.
5. Todas las computadoras asignadas a un usuario final deben de tener su propio usuario y password de acuerdo a la "Política de Creación de Usuario".
6. El usuario es responsable que su laptop u proyector tenga su cable de seguridad siempre puesto y bloqueado.
7. Toda computadora de escritorio deberá estar debidamente protegida con UPS

8. Los empleado o personal sub-contratado del INSAFORP al usar el equipo de cómputo, se abstendrán de consumir alimentos, bebidas, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles.
9. Para prevenir el acceso no autorizado, los equipos están configurados de manera tal que al cabo ciertos minutos de inactividad, se active el protector de pantalla y se bloquee.

vii. ACCESO A DISPOSITIVOS USB

1. Toda Computadora personal o Laptop se le aplican políticas de antivirus que bloquean los dispositivos de USB bloqueados.
2. Si el usuario necesita que se le active este deberá solicitar el acceso al Gerente/Jefe/Coordinador o encargado del área.

viii. INFORMACIÓN INSTITUCIONAL

1. El equipo informático es propiedad del INSAFORP, por tanto los archivos almacenados en dicho equipo también son propiedad de la institución.
2. Todo archivo almacenado en los equipos institucionales deberá estar relacionado con eventos, capacitaciones, supervisiones y otras actividades de la Formación Profesional.

ix. USO ACEPTABLE DE EQUIPO INFORMÁTICO

1. El INSAFORP se reserva el derecho de auditar, registrar, monitorear los accesos y el uso de los recursos informáticos e información en cualquier momento sin notificación alguna para el usuario del equipo asignado.
2. El monitoreo puede incluir inspección en su equipo de cómputo por potenciales problemas de seguridad.
3. Los usuarios son responsables de la seguridad de sus contraseñas de manera que no permitan que otro usuario pueda tener acceso a ellas.
4. El empleado no deberá acceder o intentar acceder a los equipos informáticos o información a la cual no se le haya antes autorizado.
5. Los equipos informáticos del INSAFORP sólo deben usarse para actividades institucionales.
6. Debe respetarse y no modificar la configuración de Hardware y Software establecida por la Gerencia de TI.
7. Todo el Software del INSAFORP 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.
8. 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.
9. No se permite el uso de Software de distribución gratuita, Shareware o versiones "portables" a menos que haya sido previamente aprobado por la Gerencia de TI.
10. No deben dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial del INSAFORP.

11. Para llevar un equipo informático fuera del INSAFORP se requiere autorización de Servicios Generales.
12. Cada usuario creará una carpeta llamada insa seguida por su nombre y un apellido, por ejemplo insa Juan Pérez, en la cual almacenará toda la información institucional de una forma organizada.
13. Reportar a la Gerencia de TI a través de Help desk sobre problemas técnicos que presente el equipo informático.
14. Se prohíbe abrir el equipo de computación, sus accesorios y periféricos. Esta actividad solamente la realizará el personal de la Gerencia de Tecnologías de la Información o el personal de empresas de servicio contratadas por dicha Gerencia.

x. SOFTWARE

1. Soporte y Red de la Gerencia de TI es responsable de mantener vigentes las licencias del Software institucional que lo requiera.
2. Soporte y red de la Gerencia de TI son responsables de controlar el Software instalado en la infraestructura de hardware de la institución.
3. Conforme a las disposiciones respecto al uso legal del software, todo software instalado deberá estar legalmente licenciado. No se permitirá la instalación de software que no cuente con la respectiva licencia de uso respectiva, ya sean estos: procesador de textos, hoja de cálculo, manejadores de bases de datos, diseño gráfico, etc.
4. La custodia de software se hará en el área de informática.
5. Por otra parte, todo el software considerado como "freeware" o "shareware", no será necesario que se adquieran las licencias de uso respectivas; sin embargo, la unidad solicitante o interesada deberá contar con la autorización respectiva emitida por la Gerencia de TI, para su instalación, previa una justificación de su uso.

xi. CUENTA DE ACCESO A RED

Todo usuario debe tener una cuenta para el acceso a la red, esta cuenta debe tener una contraseña que será sólo de su conocimiento y los recursos de la red deben emplearse en tareas relacionadas con la función institucional delegada.

1. **Solicitud de creación de cuenta de red**
    1. La solicitud de cuentas para el acceso a la red será por medio de nota escrita, help desk o correo electrónico, por parte del **Gerente/Jefe respectivo o a quien este delegue** y dirigido a la Gerencia de Tecnologías de la Información, especificando si a este se le dará **derecho al Internet, correo electrónico interno, etc.**
    2. Para la creación de usuarios se toma en cuenta el siguiente formato: Se tomará la iniciales de la gerencia y el primer nombre del usuario
    3. La contraseña asignada debe tener por lo menos 8 caracteres.
    4. Las contraseñas de cada cuenta de red son asignadas por la Gerencia de TI al momento de la creación de la cuenta respectiva, y la contraseña definitiva es asignada por el usuario.

5. Los usuarios de red pueden cambiar su contraseña de acceso al momento que lo deseen, desde sus computadoras. También, cada noventa días se fuerza a cambio de contraseña de red, la cual tiene que ser mínimo de 8 caracteres y debe ser diferente a las últimas tres contraseñas anteriormente utilizadas, además, después de tres intentos fallidos de acceso a la red, el usuario es automáticamente bloqueado.

2. Deshabilitar cuenta de red

1. Todos los usuarios que ya no laboren en la institución no se borran, sino que se deshabilitan esto para mantener el histórico de cambios realizados en los sistemas.
2. Para deshabilitar un usuario es requerido que lo solicite el Gerente/Jefe/Coordinado de la unidad a través de un Help desk o correo electrónico.
3. Las cuentas de red deshabilitadas son eliminadas después de 60 días sin utilización.
4. Las cuentas de red son deshabilitadas después de 30 días sin utilización.

3. Cambio de clave

1. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato.
2. Es requerido el cambio de contraseña de usuario cada 90 días o cuando el usuario lo solicite/desee.
3. Cada usuario es responsable de la confidencialidad de sus contraseñas asignadas al correo electrónico, red, sistemas y otras.

xii. PUNTOS DE RED

1. Todas las unidades de la institución que tengan la necesidad de instalar puntos de red, deberán justificar sus requerimientos con el encargado de Administrar la red.
2. Las computadoras solo podrán conectarse a la LAN en el lugar establecido para hacerlo.

xiii. DESARROLLO Y MANTENIMIENTO DE APLICACIONES

El desarrollo de aplicaciones informáticas estará orientada principalmente a:

1. La generación de información que apoye la toma de decisiones.
2. Distintos proyectos que se identifiquen y determinen en conjunto con la Alta Dirección, que fortalezcan los principales procesos de la institución, y en consecuencia con los objetivos del INSAFORP,
3. Las unidades organizativas identifican necesidad de automatizar procesos que apoyan a la toma de decisiones concerniente al Sistema Nacional de Formación Profesional y lo presenta a la Dirección Ejecutiva.
4. El Gerente/Jefe del área a la que se le aprobó el proyecto presenta a la Gerencia de TI el proceso y el alcance de sistema que fue aprobado.
5. La Gerencia de TI con el responsable del proyecto evalúan alternativas.

6. El desarrollo o adquisición de sistemas deberá contemplar especificaciones establecidos por la unidad de TI, para garantizar la funcionabilidad e integración de sistemas; y el mantenimiento de éstos.

i. Desarrollo de sistema

1. La Gerencia de TI en conjunto con la persona responsable del proceso o líder del proceso acuerdan inicio del levantamiento de requerimiento funcionales del sistema.
2. La GTI una vez aprobado los requerimientos funcionales (Documentación), podrá evaluar formas de atender el servicio solicitado.
3. Con base a los requerimientos funcionales definido con el usuario se programarán las validaciones del procesamiento de datos, integraciones, controles, interface que requiera el proceso, para garantizar que el dato procesado esté completo, exacto y validado según el proceso que administra el usuario. Es responsabilidad del usuario revisar que el aplicativo presente los datos establecidos en los requerimientos o proceso y reportar situaciones que se presenten para realizar el ajuste correspondiente.

ii. Mantenimiento a sistemas

1. El mantenimiento de las aplicaciones se realizará en función de la mejora continua, identificando oportunidades de mejora de procesos y nuevas tecnologías, que contribuyan a impactar en los objetivos institucionales.
2. Todas las modificaciones, cambios y ampliaciones a la funcionalidad actual de los sistemas de informáticos deben de ser solicitado por el dueño del proceso o por quien este delegue por Help desk o medio escrito.
3. El área de desarrollo evaluará los requerimientos de cambios y procurara atenderlos todos, siempre y cuando no causen incompatibilidades funcionales o de datos con otras aplicaciones en funcionamiento.
4. Los cambios mayores se realizarán en horas de poco uso de los sistemas informáticos en el medio día o la tarde. Salvo excepciones, previo análisis de su importancia, se pueden realizar en cualquier momento.
5. Con base a los cambios solicitados por el usuario la Gerencia de TI realiza las validaciones del procesamiento de datos para garantizar que el dato procesado esté completo, exacto y validado según el proceso que administra el usuario. Es responsabilidad del usuario revisar e informar situaciones que se presenten para realizar el ajuste correspondiente al procesamiento.

iii. Administración de la seguridad.

1. La seguridad en los sistemas de información es una forma de garantizar que los datos serán manipulados por personal autorizado.
2. Cualquier usuario del sistema que desee acceder al sistema deberá tener una clave de acceso o password.
3. La clave es responsabilidad del usuario al que se le asigna, por lo que no puede ser transferida a nadie, ya que cualquier operación que registre el sistema, será responsabilidad directa del propietario de la clave.

4. En caso de solicitar la creación de claves, el Gerente/Jefe/coordinador o quien este delegue deberá solicitar por escrito, correo o help desk, identificar las opciones del sistema a las cuales se tendrá acceso.

xiv. CORREO ELECTRÓNICO

1. La cuenta de correo es personal e intransferible dado que el correo electrónico institucional se asigna a cada usuario para que agilice sus labores y establezca una comunicación inmediata con personal del INSAFORP, empresas, consultores y otros relacionados con el quehacer diario institucional
2. Todos los mensajes enviados o recibidos por medio de la mencionada cuenta de correo son considerados como propiedad del INSAFORP.
3. La recepción y envío de mensajes de correo electrónico genera tráfico en la red del INSAFORP y por lo tanto su uso deberá ser para actividades laborales.
4. La cuenta de correo interno es personal e intransferible. El usuario es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre, por lo tanto, es indispensable que cada usuario al momento de retirarse momentáneamente de su escritorio, bloquee su computadora para que ésta no sea utilizada durante su usencia.

iv. Cuenta de correo

El INSAFORP proporcionará:

1. La cuenta de correo electrónico estará conformada por el nombre del usuario@insaforp.org.sv
2. Un buzón para almacenar los mensajes, el cual tendrá una capacidad máxima de 200Mb.
3. Una palabra clave o password para acceder de manera privada a la cuenta.
4. La posibilidad de enviar y recibir mensajes dentro de la institución y hacia Internet utilizando la dirección electrónica asignada.
5. En caso de necesidades especiales, el interesado podrá solicitar la ampliación de la capacidad ante la Gerencia de TI. De igual manera, en caso de necesidad institucional o por razones técnicas, las capacidades máximas de los buzones podrán ser modificadas por parte del INSAFORP.

v. Creación de cuenta de correo

1. Con el fin de garantizar que la identificación del usuario en la dirección de correo electrónico sea única, los nombres de las cuentas de correo electrónico se construirán de acuerdo a la siguiente regla, Se tomará la primera letra del primer nombre seguido del primer apellido. En caso de que un nuevo nombre coincida con el de un usuario ya existente, se tomara la primera letra del segundo nombre seguido del primer apellido y si este también existe entonces se acordará un nombre distinto al nuevo usuario. De igual manera, en casos en que la construcción resulte incómoda, compleja, o difícil de recordar, la Gerencia de TI acordará un nuevo nombre con el o la interesada o interesado.
2. El correo electrónico se define como un servicio de naturaleza institucional propiedad de la institución. En consecuencia, INSAFORP podrá implementar medidas de control y monitoreo al uso de este servicio, para

asegurar su estabilidad y su seguridad. La Gerencia TI es la dependencia encargada de la administración de este servicio y tendrá la potestad para monitorear y controlar el tráfico de mensajes con el fin de evitar riesgos para los usuarios y la institución.

3. Se asignará solamente una cuenta por cada usuario. Las cuentas para proyectos especiales o grupos, se asignarán previo acuerdo entre la Gerencia de TI y el departamento solicitante.
4. Toda solicitud de apertura de cuentas de correo electrónico debe hacerse por escrito o help desk.

vi. Depuración y respaldo de mensajes

El usuario deberá:

1. Depurar periódicamente el contenido del buzón de correo con el fin de administrar el espacio asignado y evitar la saturación del espacio asignado.
2. Los usuarios deberán guardar los correos electrónicos que contienen información relevante para la realización de una transacción de negocios, información importante de referencia, o tiene un valor como evidencia para la toma de decisiones, éste debe ser retenido para referencia futura.

vii. Contenido de los mensajes

Utilizar siempre un lenguaje apropiado en sus comunicaciones.

viii. Acceso a cuenta de correo

1. Los empleados no deben interceptar o ayudar a interceptar correos electrónicos.
2. La solicitud de acceso a un buzón de correo electrónico procederá únicamente sí esta es realizada por el **Gerente/Jefe/Coordinador** del empleado mediante una nota, help desk o correo electrónico. El acceso será autorizado por el Gerente de Tecnologías de la Información.

ix. Suspensión o cancelación de cuenta

1. La Gerencia de TI se reserva el derecho de dar de baja las cuentas que no tengan ninguna actividad por un período continuo de 120 días calendario.
2. El Gerente/Jefe/Coordinar de área mediante una nota o correo electrónico o help desk podrá solicitar la cancelación o suspensión de la cuenta de correo

xv. USOS INDEBIDOS DEL CORREO ELECTRÓNICO

De manera enunciativa señalamos algunos usos indebidos que no están autorizados ni permitidos y que su ejecución por parte del usuario originará la terminación o suspensión del servicio por parte de INSAFORP

Actividades no permitidas:

1. Intentar acceder sin autorización a las cuentas de correo electrónico que no le pertenecen, mediante la utilización de herramientas intrusivas (hacking),

descifrado de contraseñas, descubrimiento de vulnerabilidades o cualquier otro medio no permitido o legítimo.

2. Cargar archivos que contengan virus, caballos de troya ("troyanos"), gusanos ("worms"), archivos dañados o cualquier otro programa o Software similar que pueda perjudicar el funcionamiento de los equipos, de la red de INSAFORP o de propiedad de terceros.
3. Presentar, alojar o trasmitir información, imágenes, textos que en forma indirecta o directa sean de pornografía.
4. Cualquier tipo de Software del cual ni el emisor ni el receptor tengan la respectiva licencia de instalación.
5. Realizar ataques que causen daño o inutilización de los servicios prestados por INSAFORP u otros operadores.
6. Envío de información clasificada como confidencial a personas no autorizadas por INSAFORP a través del correo electrónico.
7. Realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.

xvi. ANTISPAM

1. Se realiza escaneo de los correos enviados hacia INSAFORP y se categorizan si son o no amenaza. Se envía correo de cuarentena al usuario final para verificar si existen correos validos que se hayan detenido. Amenazas confirmadas de virus o Spam son automáticamente rechazados.
2. Es responsabilidad de los usuarios revisar los archivos de spam y liberar los correos que le servirán para realizar su trabajo

xvii. IMPRESIÓN

El uso de los impresores deberá ser sólo para documentos institucionales. Queda a discreción de cada Gerente/Jefe/Coordinador la supervisión directa del buen uso del impresor asignado a su Unidad o Gerencia.

xi. Impresiones monocromática

Impresores de red

1. La Gerencia o Unidad que solicite equipo de impresión deberá de gestionarla con la Dirección Ejecutiva.
2. Estos impresores no están físicamente conectados a las computadoras, sino directamente a la red.
3. Se podrán utilizar estos impresores siempre y cuando el usuario cuente con acceso a red al momento de inicializar la computadora.
4. El área de soporte configura el equipo de impresión para que este realice las impresiones en ambas caras de cada hoja(dúplex), para los equipos que permitan la configuración.
5. El usuario que requiera imprimir a una sola cara deberá solicitarlo median un help desk.

xii. Impresiones a color

1. La Gerencia o Unidad que solicite equipo de impresión a color deberá de gestionarla su autorización con la Dirección Ejecutiva.
2. Las Gerencia o unidad que cuente con equipo de impresión a color podrá el Gerente/jefe/coordinador solicitar la instalación de este servicio a sus empleados mediante un help desk donde especifique su autorización.
3. Las Gerencia que no cuenten con impresión a color y necesiten para el desarrollo de su funciones deberán de gestionar su autorización con la Dirección Ejecutiva y estará sujeta a disponibilidad presupuestaría del servicio.

xviii. USO DE REDES SOCIALES

1. Toda información institucional que se publica en redes sociales es canalizada y difundida por la Gerencia de Comunicación Institucional
2. El equipo Gerencial tendrá acceso a redes sociales
3. En caso que se desee publicar algo en las redes sociales institucionales, se deberá enviar la documentación a la persona encargada de administrar los contenidos , es decir al "*Community Manager*" designado por la GCI
4. Los empleados del INSAFORP no deberán emitir/publicar mensajes institucionales con su(s) cuenta(s) personale(s) de las redes sociales.
5. En las oficinas del INSAFORP, los empleados tendrán acceso a las redes sociales siempre y cuando su Gerente/Jefe/Coordinador lo haya solicitado. Queda a discreción de cada Jefe o Gerente la supervisión directa del buen uso de este servicio.
6. El Gerente/Jefe/Coordinador de área mediante una nota, correo electrónico o help desk podrá solicitar la cancelación o suspensión de este servicio para alguno de sus colaboradores o propio.
7. No se debe utilizar el correo institucional para registrarse en ninguna red social.

xix. EQUIPO DE PRÉSTAMO

Este servicio esta disponible sólo para actividades institucionales.

1. La Gerencia de Tecnologías de la Información contará con una cantidad limitada de equipo informático, para atender solicitudes de préstamo de equipo para reuniones u otros eventos de corta duración Institucionales.
2. La Gerencia de Tecnologías de la Información designará a una persona como responsable de la administración y custodia de este bien, mientras este se encuentre en la Gerencia TI.
3. Las diferentes unidades del INSAFORP podrán hacer uso de este equipo informático, mediante solicitud (help desk). Dicha solicitud se atenderá por orden de llegada y los equipos son entregados en la Gerencia de Tecnologías al solicitante, quien es el responsable de la custodia del equipo mientras esté en su poder.
4. Las solicitudes para reservar el equipo de préstamo deben de realizarse por lo menos una semana antes del evento.
5. El usuario que gestionó el préstamo del equipo es el responsable de entregar a la Gerencia de TI el equipo que fue prestado con todos los accesorios con los cuales se brindó el préstamo.

6. El préstamo de los equipos dependerá de la disponibilidad del equipo solicitado, debido a que el recurso es limitado.
7. El usuario solicitante del equipo informático deberá de tramitar la salida del equipo con Servicios Generales, sí este será utilizado en eventos institucionales fuera de las Instalaciones del INSAFORP.
8. En caso de Extravío del equipo de préstamo el usuario solicitante deberá de comunicarse con Servicios Generales quien le brindará información sobre el proceso y realizará la gestión correspondiente para tramitar el seguro si procede. En caso de no proceder el reintegro del seguro, el usuario responsable deberá reintegrar el equipo.

xx. ATENCIÓN DE HELP DESK

1. Todo soporte deberá de ser canalizado por medio de help desk
2. Los Help Desk serán atendidos de acuerdo a criticidad y orden de llegada.

xxi. VIGENCIA

Las presentes políticas entrarán en vigencia a partir de su aprobación y estará dando de baja al "MANUAL DE POLITICAS Y PROCEDIMIENTO PARA LOS SISTEMAS DE INFORMACIÓN" y "MANUAL DE POLITICAS Y PROCEDIMIENTO DE CONTROLES DE APLICACIONES ESPECIFICOS"

Revisó:

José Mario Martínez Quintana
Coordinadora Unidad de Planificación

Cecyl Martiny Arriola de Hernández
Gerente de TI

Autorizó:

Ing. Carlos Gómez
Director Ejecutivo