RESOLUCIÓN No. 874 /2014

Guatemala, veintisiete de junio de dos mil catorce.

CONSIDERANDO:

Que es imprescindible el control total y sistematizado de la tecnología de información y telecomunicación, por medio de medidas técnicas y organizativas que coadyuven en la seguridad de los datos y trabajadores que interactúan a nivel institucional.

Que para optimizar de forma efectiva la infraestructura tecnológica de información y telecomunicación, deben atenderse inequívocamente los lineamientos que permitan su correcto funcionamiento.

CONSIDERANDO:

Que derivado de las funciones asignadas al Departamento de Informática, es necesario dotarle de un instrumento administrativo que sirva de apoyo, orientación y guía a los colaboradores del Departamento de Informática que tienen participación en la ejecución de cada uno de los procesos que permiten el funcionamiento de dicha dependencia.

CONSIDERANDO:

Que mediante el Acuerdo del Gerente No. 1/2014, se delega en cada uno de los Subgerente del Instituto la facultad de aprobar por resolución, los Manuales de Organización y de Normas y Procedimientos de las Dependencias que se encuentren bajo la línea jerárquica de autoridad y ámbito de competencia.

POR TANTO:

El Subgerente Administrativo con base en los considerandos y de conformidad con lo establecido en el Acuerdo de Gerencia número 65/2013 "Delegación de Funciones" de fecha 28 de junio de 2013 y en base a lo considerado en el Acuerdo del Gerente 1/2014 de fecha 27 de enero de 2014.

ACUERDA:

PRIMERO. Aprobar el **"MANUAL DE NORMAS INTERNAS DEL DEPARTAMENTO DE INFORMÁTICA",** el cual consta de carátula, índice y contenido en veinticinco (25) folios numerados, rubricados y sellados por el Subgerente Administrativo y forman parte de la presente Resolución.

RESOLUCIÓN No. 874 /2014

SEGUNDO. El presente Acuerdo aprueba la normativa de observancia general para la implementación, funcionamiento y utilización de la infraestructura tecnológica de información y telecomunicación a nivel institucional.

TERCERO. La inobservancia del presente Manual, será objeto de sanción con base a lo preceptuado en el Acuerdo 1090 de Junta Directiva "REGLAMENTO GENERAL PARA LA ADMINISTRACIÓN DEL RECURSO HUMANO AL SERVICIO DEL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL".

CUARTO. Los incidentes en los que se involucra las telecomunicaciones o la transmisión de datos que fueran considerados como delitos de acuerdo con las leyes del país, deberán ser denunciados por el Jefe del Departamento de Informática o autoridad competente.

QUINTO. El cumplimiento y aplicación del presente Acuerdo, es responsabilidad de todo el recurso humano que sea trabajador o este contratado para brindar sus servicios al Instituto, bajo la supervisión de su Jefe Inmediato o Autoridad institucional que reciba los servicios contratados, quienes deberán solicitar la validación del incumplimiento del Manual al Jefe del Departamento de Informática, quien deberá confirmar por escrito el hecho para que se continúe con la gestión administrativa que establece el Acuerdo 1090, por parte de la dependencia en la cual se halla ocasionado la falta.

SEXTO. Las revisiones, modificaciones y actualizaciones necesarias en el Manual, se realizarán a solicitud y propuesta expresada por el Jefe del Departamento de Informática, con anuencia del Subgerente Administrativo, derivado de reformas aplicables a la reglamentación vigente o por cambios relacionados con la administración, funcionamiento e innovación tecnológica; con el apoyo de las instancias técnicas designadas; a través de una nueva Resolución que anule la emitida anteriormente, la que será aprobada por el Subgerente Administrativo.

SEPTIMO. Cualquier situación que no estuviere expresamente regulada en el Manual que por este acto se aprueba, se resolverá con la aplicación de otros instrumentos administrativos específicos aprobados por la Autoridad del Instituto; y, cuando se refiera a problemas de interpretación en la aplicación del Manual, serán resueltos en su orden, por el Jefe del Departamento de Informática, Ente Técnico Normativo Rector según corresponda y por el Subgerente Administrativo.

OCTAVO. Trasladar copia certificada de la presente Resolución y Manual de forma inmediata a la Gerencia, al Departamento de Informática, al Departamento de Comunicación Social y Relaciones Públicas, para su publicación dentro del portal del Instituto, al Departamento de Organización y Métodos y al Departamento Legal, para su guarda y custodia en el área de recopilación de leyes.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL SUBGERENTE ADMINISTRATIVO

LENNY RODAS ASISTENTE ADMINISTRATIVO I.G.S.S. - S.G.A.

RESOLUCIÓN No. 874 /2014

NOVENO. La presente Resolución entra en vigencia al día siguiente de la fecha de su emisión y complementa las disposiciones internas del Instituto.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBGERENTE ADMINISTRATIVO

DR. ALVARO MANOLO DUBÓN GONZÁLEZ MBA
SUBGERENTE

LENNY RODAS
ASISTENTE ADMINISTRATIVO
I.G.S.S. - S.G.

AMDG/lerv

Instituto Guatemalteco
de Seguridad Social

MANUAL DE NORMAS INTERNAS DEL DEPARTAMENTO DE INFORMÁTICA

GUATEMALA, ENERO DE 2014

ÍNDICE

I. INTRODUCCIÓN

El presente Manual es un instrumento de gestión que contiene la normativa general que se establece para la implementación, funcionamiento, registro y control de las herramientas informáticas a nivel institucional bajo la administración del Departamento de Informática.

II. OBJETIVOS DEL MANUAL

1. Que el Departamento de Informática cuente con lineamientos que estén enmarcados dentro de los estándares internacionales aplicados en el campo de la tecnología de información.

2. Que los trabajadores del Departamento cuenten con instrumentos administrativos que faciliten el desarrollo de las actividades que desempeñan.

III. CAMPO DE APLICACIÓN

El presente manual es de observancia y aplicación para el Departamento de Informática, por ser el único ente responsable de manejar la infraestructura informática, para optimizar el aprovechamiento de los servicios informáticos que están a disposición de los usuarios del Instituto.

IV. NORMAS DE APLICACIÓN

A. NORMAS GENERALES

1. El Departamento de Informática podrá autorizar a los usuarios del Instituto cualquier servicio informático, como acceso a la red institucional, hacer uso de las herramientas de correo electrónico, mensajería instantánea, internet y cualquier otra aplicación a implementar, cuando exista solicitud firmada y sellada por el jefe de la dependencia a la cual estén asignados y queda a discreción del Departamento de Informática su autorización.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBGERENTE ADMINISTRATIVO

2. Los documentos de referencia en el presente manual, podrán ser consultados en la página de *intranet* oficial del Instituto, en la sección documentos de la carpeta informática.

3. El Departamento de Informática deberá exigir a todos sus trabajadores y proveedores, la firma de un acuerdo de confidencialidad y acceso apropiado a la información institucional.

4. Cuando el usuario deje de laborar o sea trasladado a otra dependencia del Instituto, se deberá notificar al Departamento de Informática por la máxima autoridad de esa dependencia, a fin de habilitar o inhabilitar las cuentas del usuario.

5. El Departamento de Informática se reservará el derecho de prohibir o restringir el uso de los servicios informáticos por cualquier propósito y en cualquier momento.

B. NORMAS ESPECÍFICAS

1. DE LA ATENCIÓN DE SERVICIOS DE SOPORTE DE INFORMÁTICA

a. El Departamento de Informática brinda atención de servicios de soporte de tecnología de la información a las distintas dependencias del Instituto y registra las solicitudes recibidas y atendidas en el sistema de Mesa de Ayuda. Para garantizar la continuidad, disponibilidad y calidad de atención al usuario, se ha desarrollado la estrategia de brindar soporte por niveles, según la complejidad del problema, de la forma siguiente:

a.1 Soporte de primer nivel (asistencia desde las instalaciones del Departamento de Informática).

a.2 Soporte de segundo nivel (asistencia personal y directa de los técnicos).

a.3 Soporte de tercer nivel (atención personal y directa de un especialista en el área).

b. Cuando se determine el nivel de soporte requerido, debe establecerse su prioridad dentro del Instituto, con base en los parámetros siguientes:

b.1 Impacto. Determinar la importancia del incidente y evaluar cómo afecta los procesos del Instituto y al número de usuarios.

b.2 Urgencia. Determinar el tiempo máximo necesario para la resolución del incidente.

c. Cuando el responsable no pueda resolver el incidente, puede recurrir a:

c.1 Escalado funcional. Apoyo de un especialista de soporte de Informática del tercer nivel para resolver el problema.

c.2 Escalado jerárquico. Apoyo de la jefatura del Departamento de Informática, para tomar decisiones que no están dentro de las atribuciones asignadas del responsable.

d. Todos los incidentes reportados al Departamento de Informática deben atender lo siguiente:

d.1 Registro de incidentes.

d.1.1 Los incidentes pueden provenir de diversas fuentes, deben ser ingresados en el sistema inmediatamente y registrarse en la base de conocimiento la información básica necesaria para el procesamiento del incidente (hora, descripción del incidente, sistemas afectados, etcétera).

d.1.2 El soporte de informática de primer nivel debe ser capaz de evaluar en primera instancia si el servicio requerido se incluye en la base de conocimiento del Departamento de Informática y en caso contrario, reenviarlo a la persona responsable, dependiendo del caso.

d.1.3 Comprobar que el incidente no haya sido registrado con anterioridad por otro usuario.

d.1.4 Asignar una referencia que le identificará inequívocamente, tanto en los procesos internos como en las interacciones con el usuario.

d.1.5 Incluir cualquier información relevante para la resolución del incidente, que puede ser solicitada al usuario u obtenida de la propia base de conocimiento del sistema.

d.1.6 En caso que el incidente pueda afectar a otros usuarios, estos deben ser notificados para que conozcan cómo esta incidencia puede afectar su flujo habitual de trabajo.

d.2 Clasificación de incidentes.

d.2.1 Asignar una categoría dependiendo del tipo de incidente o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por incidente.

d.2.2 Establecer el impacto o la urgencia, con base al nivel de soporte de informática.

d.2.3 Realizar el *monitoreo* del estado y tiempo de respuesta esperado, asociar un estado al incidente (registrado, activo, suspendido, resuelto, cerrado, otros) y estimar el tiempo de resolución del incidente.

d.3 Análisis, resolución y cierre de incidentes.

d.3.1 Examinar el incidente con ayuda de la base de conocimiento, para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado.

d.3.2 Cuando el soporte de primer nivel no está en posibilidades de la resolución del incidente, éste lo redireccionará (si fuera necesario se puede emitir una Solicitud de Gestión de Cambio) a un soporte de segundo nivel para su investigación y si no es capaz de resolver el incidente, pasará al soporte de tercer nivel.

d.3.3 Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las base de conocimiento, para disponer de la información completa sobre el estado del mismo.

d.4 Al solucionar el incidente se verificará lo siguiente:

d.4.1 Confirmar con los usuarios la solución satisfactoria del mismo.

d.4.2 Incorporar el proceso de resolución a la base de conocimiento.

d.4.3 Reclasificar el incidente si fuera necesario.

d.4.4 Cerrar el incidente.

e. El Departamento de Informática priorizará los requerimientos que deben atender de soporte, de acuerdo con las categorías siguientes:

e.1 Protección de anti-virus y desinfección.

e.2 Configuración de la red.

e.3 Fallas de *hardware*.

e.4. Reinstalación de programas y configuración.

e.5 Infraestructura de la red.

e.6 Administración de la red.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBGERENTE ADMINISTRATIVO

e.7 Otros.

f. El soporte de primer nivel deberá resolver la mayor parte de los incidentes, con base a las consideraciones siguientes:

f.1 ¿Cuáles son las necesidades?

f.2 ¿Quiénes serán los responsables de atender este nivel de atención?

f.3 ¿Se deben contratar servicios?

f.4 ¿Qué estructura tendrá la atención, distribuido, central o virtual?

f.5. ¿Qué herramientas tecnológicas se necesitan?

f.6 ¿Qué métricas determinarán el rendimiento de este soporte?

f.7 Establecer estrictos protocolos de interacción con el usuario.

f.8 Informar a los usuarios de los beneficios de este nuevo servicio de atención y soporte.

f.9 Monitorear a los usuarios para conocer mejor sus expectativas y necesidades.

2. DE LA GESTIÓN DE CAMBIOS

El Departamento de Informática debe llevar un registro de los cambios o reemplazos efectuados por motivos de fallas, actualización de equipo o defectos de fábrica del equipo informático y sus periféricos.

3. DEL CORREO ELECTRÓNICO

a. El Departamento de Informática podrá revisar, controlar o revelar eventualmente el contenido de los mensajes enviados por correo electrónico, en los casos siguientes:

a.1 Exista razón para creer que hay violaciones a la ley o a la normativa institucional.

a.2 Cuando el mensaje represente falta de respeto o atente contra las normas aceptables de la moral.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBGERENTE ADMINISTRATIVO

4. DEL ACCESO REMOTO

La dependencia que requiera acceso remoto, deberá enviar al Departamento de Informática la solicitud respectiva, indicando el tiempo de duración del permiso, para eliminarla una vez finalice el trabajo autorizado o dar aviso al momento que la persona autorizada finalice su relación de trabajo con la Institución. Queda a discreción del Departamento de Informática su autorización.

5. DEL USO DEL INTERNET

a. El Departamento de Informática debe proteger los recursos de la Institución contra la intrusión de *software* malintencionado; prevenir conexiones no autorizadas y sin protección hacia internet que pueda permitir el ingreso de contenido no seguro en la red del Instituto y comprometer la integridad de los datos y la seguridad del sistema de toda la red.

b. Las conexiones de internet físicas o conexiones para otras redes privadas o públicas serán autorizadas y aprobadas por el Departamento de Informática.

c. El Departamento de Informática está autorizado en todo momento para poner a funcionar un *cortafuego* en la conexión hacia otras redes, con la finalidad de restringir o permitir el acceso de acuerdo al nivel de seguridad que el Departamento requiera.

d. Los controles de internet y el sistema de registros realizarán lo siguiente:

d.1 El sistema evitará que los usuarios visiten sitios web inapropiados, pornografía o sitios peligrosos. Este mismo sistema no requiere un ingreso adicional de identificación, utilizará el Directorio Activo para identificar a los usuarios. El sistema deberá ser capaz de registrar el tiempo de actividad en internet, la duración de la actividad, los sitios web visitados y el tipo de datos descargados.

d.2 El Departamento de Informática podrá *monitorear* en cualquier momento el contenido al que los usuarios tendrán acceso.

d.3 Los usuarios recibirán un mensaje de las políticas de acceso al ingresar al internet por primera vez o cada 30 días, el cual deberán de aceptar para poder ingresar.

6. DEL ACCESO INALÁMBRICO

a. Los puntos de acceso que son conectados a las redes de área local, se deben adherir al proceso de autenticación del Instituto.

b. Todos los equipos que se autoricen para utilizar la red inalámbrica, deberán ser evaluados y configurados por personal del Departamento de Informática.

7. DEL USO DE CONTRASEÑAS

a. El Departamento de Informática para el desarrollo de las aplicaciones, debe asegurar que sus programas contengan las precauciones de seguridad siguientes:

a.1 Debe permitir la autenticación por usuario y contraseña.

a.2 No debe almacenar las contraseñas en texto plano o en cualquier formato que pueda ser revisado fácilmente.

b. El uso de contraseñas para los usuarios de acceso remoto debe estar controlado, se usará una sola vez, o bien un sistema de clave privada con una contraseña fuerte.

c. Los sistemas que soportan la gestión de historial de contraseñas deben almacenar como mínimo 12 contraseñas, que no pueden ser reutilizadas.

d. Las contraseñas seguras tienen las características siguientes:

d.1 Estar compuesta por caracteres de cada uno de los siguientes grupos.

d.1.1 Letras mayúsculas y minúsculas (a-z, A-Z).

d.1.2 Números (0-9).

d.1.3 Caracteres especiales que sean soportados.

d.2 Contar con un mínimo de 8 caracteres.

d.3 No están basadas en información personal, tales como nombres de familia, números telefónicos, entre otros.

e. El Departamento de Informática podrá dar acceso a los servicios informáticos de un trabajador ausente, en casos plenamente justificados y cuando exista solicitud firmada y sellada por el jefe inmediato superior de la dependencia.

8. DE LAS LICENCIAS DE SOFTWARE

a. El Instituto debe contar con licencias de *software* autorizadas, que permitan la instalación de los programas que sean necesarios para el desarrollo de las actividades laborales de los trabajadores del Instituto.

b. El Departamento de Informática designará un responsable para administrar y llevar el control de las licencias de *software*, debiendo actualizar el registro con base a la información que provean las dependencias del Instituto de las instalaciones, cambios y ubicación de dichas licencias.

c. El responsable de la administración y control de las licencias de *software* realizará las gestiones con los proveedores de *software*, para la adquisición de licencias que sean necesarias para el Instituto, así como exigir al proveedor que por escrito le haga entrega de dicho *software*.

9. DEL SITIO WEB

a. El Departamento de Informática podrá publicar en el sitio web del Instituto, los diseños que sea requeridos, los cuales deben ajustarse a las características ya establecidas y publicadas en la *intranet* oficial del Instituto.

b. Los diseños para publicar en el sitio web, además de reunir las características que se indican en la norma anterior, deben considerar lo siguiente:

b.1 La página web debe ser visualizada en los navegadores web más utilizados.

b.2 Los derechos de autor, normas y reglamentos deben ser respetados.

10. DE LOS NOMBRES DE EQUIPO

a. Los equipos de cómputo propiedad del Instituto deben regirse conforme la nomenclatura de nombres de equipo ya establecida.

b. Los servidores de servicios instalados en las dependencias del Instituto deben regirse a la nomenclatura de nombres de servidores ya establecida.

11. DE LA DOCUMENTACIÓN DE LA INFRAESCTURA

a. El Departamento de Informática debe contar con diagramas que describan y detallen la infraestructura de red institucional, así mismo cada dependencia del Instituto deberá contar con sus propios diagramas, los cuales deberán ser actualizados periódicamente y trasladarlos al Departamento de Informática para su actualización.

b. El Departamento de Informática llevará control documentado de toda su infraestructura tecnológica, en la cual incluirá los datos relevantes de los equipos críticos incluyendo ubicación, responsable de administrarlos, datos técnicos, entre otros.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
GERENTE ADMINISTRATIVO

12. DEL ACCESO FÍSICO

a. Para facilitar el acceso físico al Departamento de Informática, se deben atender los aspectos de seguridad siguientes:

a.1 Las instalaciones del Departamento de Informática deben estar protegidas físicamente en proporción de la criticidad o importancia de sus funciones.

a.2 El sitio donde se ubiquen los recursos informáticos debe ser físicamente sólido y protegido de accesos no autorizados y de factores naturales, con mecanismos de control, barreras físicas, alarmas, puertas metálicas, vidrios especiales y otros para la prevención de incendios y seguridad en el trabajo.

a.3 Debe existir un área de recepción que solo permita la entrada de personal autorizado.

a.4 Las salidas de emergencia en el perímetro de seguridad, deben tener alarmas sonoras y cierre automático.

a.5 Señalizar las áreas de ingreso y egreso del Departamento.

b. El acceso físico a las instalaciones del Departamento de Informática debe ser restringido, documentado y gestionado de la manera siguiente:

b.1 Las instalaciones deben destinarse exclusivamente al personal autorizado y proveedores, quienes entre sus responsabilidades requieran acceso a las mismas.

b.2 Suministrar una tarjeta de acceso de las instalaciones del Departamento de Informática, con la respectiva aprobación de la jefatura.

b.3 La pérdida o robo de las tarjetas de acceso debe ser reportada de inmediato al Departamento de Informática.

b.4 Las dependencias del Instituto deben entregar al Departamento de Informática la tarjeta de acceso de las personas que sean removidas de su cargo por cualquier motivo.

b.5 El personal de recepción del Departamento de Informática deberá llevar un registro de la hora de entrada y salida de los visitantes.

b.6 Las áreas del Departamento de Informática que permitan el acceso a los visitantes, deben realizar el seguimiento de su visita.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBDIRIGENTE ADMINISTRATIVO

b.7 Los visitantes ingresarán únicamente si la persona responsable se encuentra dentro de las instalaciones del Departamento de Informática.

b.8 La Jefatura debe revisar en forma periódica los accesos grabados de entradas y salidas de los visitantes a las instalaciones e investigar cualquier acceso inusual.

c. El ingreso a las instalaciones del área del centro de datos del Departamento de Informática, inclusive para el personal que labora en esa dependencia, debe ser limitado; únicamente se permite el acceso al cumplir con lo siguiente:

c.1 De la solicitud.

c.1.1 Todo ingreso debe estar respaldado a través del formulario DINFO-151 "Solicitud de Visita al Centro de Datos" y en los casos de cambio de equipo deberá adjuntar adicionalmente el formulario DINFO-152 "Solicitud de Cambio de Equipo".

c.1.2 El ingreso de las solicitudes no podrá ser menor de 24 horas a la fecha y hora de visita, lo mismo aplicará a las remitidas desde la dirección electrónica centrodedatos@igssgt.org.

c.1.3 El responsable del área del centro de datos deberá autorizar dichos ingresos e informar al interesado vía telefónica o correo electrónico.

c.1.4 El Jefe del Departamento de Informática o el responsable del área del centro de datos podrán permitir el ingreso a personas que no estén autorizadas, quienes deberán ser acompañadas por personal de esta área.

c.2 Del ingreso a las instalaciones al centro de datos.

c.2.1 El visitante debe anunciarse en la recepción del Departamento de Informática.

c.2.2 La persona responsable de recepción se comunicará con el responsable de turno y éste verificará la autorización de ingreso o cambio de equipo.

c.2.3 El responsable de turno solicitará al visitante completar la hoja de control de ingresos, registra la fecha, hora, empresa, trabajo a realizar, hora de retiro y lo guiará hacia la sala de servidores.

c.2.4 Se permitirá el uso de teléfonos celulares únicamente para tratar temas relacionados con el motivo de la visita.

c.2.5 No se permitirá el ingreso de portafolios, bolsas, dispositivos de almacenamiento externo entre otros. Se podrán ingresar a la sala de servidores únicamente las herramientas o equipo necesario para la ejecución del trabajo a realizar.

c.2.6 No está permitido fumar o ingresar comida o bebidas.

c.2.7 Está terminantemente prohibido tomar fotos sin previa autorización del Jefe del Departamento de Informática o del responsable del área del centro de datos.

c.2.8 Las puertas del área del centro de datos siempre deben permanecer cerradas.

13. DE LOS PRIVILEGIOS DEL USUARIO O ACCESO DE ADMINISTRADOR DE EQUIPO

a. Toda solicitud de usuario con privilegios de administrador debe ser requerida por el jefe de la dependencia, justificando la necesidad de estos privilegios y deberá proporcionar la información adicional que le requiera el Departamento de Informática.

b. El Departamento de Informática será responsable de administrar la adecuada asignación de privilegios de usuarios en los equipos de cómputo del Instituto, según las atribuciones asignadas a los usuarios y a la vez, deberá contar con listados actualizados de los usuarios y privilegios asignados a los diferentes sistemas del Instituto.

c. El usuario que tenga cuentas con privilegios de administrador debe cumplir con las normas de seguridad que establece el Instituto y utilizar dichos privilegios de manera apropiada.

d. Cada cuenta con privilegios de administrador deberá cumplir con lo que establecen las normas específicas del numeral 7 "DEL USO DE CONTRASEÑAS".

e. El Departamento de Informática deberá contar con un repositorio de contraseñas electrónicas y tener acceso a la cuenta en cualquier situación de emergencia.

14. DE LA CONFIGURACIÓN DE RED

El Departamento de Informática establecerá los estándares que deben cumplir las dependencias del Instituto para la instalación de cableado de red, debiendo este Departamento autorizar las especificaciones técnicas del equipo a utilizar y verificar la certificación de dicho cableado.

15. DE LA CONTINUIDAD DE LAS OPERACIONES

a. El Departamento de Informática debe contar con un plan de recuperación de servicios informáticos que contenga los procedimientos actuales para restablecer los servicios más críticos del Instituto, en caso de fallas o eventualidades inesperadas.

b. El plan de recuperación de servicios informáticos debe contar con procedimientos que garanticen la continuidad del servicio posterior a una eventualidad que afecte la funcionalidad y la continuidad.

c. El plan de recuperación de servicios informáticos debe revisarse y probarse anualmente para asegurar que el mismo funcione al momento de ser requerido.

d. El Departamento de Informática debe efectuar la divulgación respecto del plan de recuperación de servicios informáticos al personal responsable de su ejecución.

16. DE LA ADQUISICIÓN Y CONTRATACIÓN DE EQUIPO Y SERVICIOS DE INFORMÁTICA

a. El Departamento de Informática realizará una revisión anual del equipo y servicios con que cuenta, evaluará las solicitudes de las dependencias del Instituto, a fin de incluir dentro del Plan Operativo Anual -POA- las compras de equipo y servicios necesarios para mejorar los servicios que presta el Instituto, en concordancia con el Plan Estratégico Institucional.

b. En los eventos de cotización o licitación para adquisición y contratación de equipo y servicios de informática, debe participar dentro de la comisión adjudicadora al menos un experto en materia de sistemas del Departamento de Informática.

c. La adquisición y entrega de productos y servicios de informática, deben realizarse dentro de la normativa contemplada en la Ley de Contrataciones del Estado, además de las disposiciones emitidas por el Instituto.

d. En los casos en que se contrate servicios en los que debe darse acceso a las redes internas y a los sistemas conectados de las computadoras, el Departamento de Informática requerirá dentro de las bases del evento, las condiciones de confidencialidad que sean necesarias, constituidas dentro de las cláusulas del contrato a celebrar.

e. El Departamento de Informática debe configurar el nuevo *hardware*, el *software* y los sistemas, para asegurar que el equipo esté configurado correctamente y que cuente con las medidas de seguridad informática del Instituto.

f. La instalación de equipos de reemplazo será prioridad sobre los nuevos equipos para garantizar la continuidad en el servicio existente.

17. DE LA SEGURIDAD LÓGICA

Los objetivos de seguridad lógica de la información que se pretende alcanzar son:

a. CONFIDENCIALIDAD. Garantizar que solo las personas que están autorizadas a tener acceso a la información sean capaces de hacerlo.

b. INTEGRIDAD. Mantener el valor y el estado de la información, la protege contra modificaciones no autorizadas, asegurando que la información no sea modificada o destruida.

c. DISPONIBILIDAD. Garantizar que la información y sistemas estén disponibles y en funcionamiento cuando sea necesario, de esta forma se asegura que la información esté siempre disponible para apoyar procesos críticos.

18. DE LA SEGURIDAD DE INFORMACIÓN

a. El Departamento de Informática será responsable de proteger los datos de las bases de datos internas, servidores de directorios de usuarios y servidores de respaldo.

b. El Departamento de Informática deberá garantizar la protección de la información a través de equipos de seguridad, mantener registros de los usuarios que acceden y permitir únicamente el acceso a las herramientas informáticas autorizadas.

19. DE LA EVALUACIÓN DE RIESGOS

a. El Departamento de Informática deberá ser sometido de forma periódica a auditorías informáticas que permitan evaluar las áreas de sistemas e infraestructura tecnológica, a fin de identificar posibles riesgos y mejorar el nivel de seguridad actual.

b. El Departamento de Informática podrá realizar en cualquier momento revisiones técnicas a las distintas dependencias del Instituto, a fin de identificar riesgos de sistemas o de infraestructura tecnológica.

c. El Departamento de Informática efectuará de forma periódica análisis de vulnerabilidades y revisiones a sus equipos tecnológicos críticos, a fin de identificar posibles riesgos y tomas las medidas correctivas.

20. DE LA COPIA DE SEGURIDAD

a. El Departamento de Informática será el responsable de respaldar la información confidencial o sensible para el Instituto a través de copias de seguridad.

b. Las copias de seguridad se utilizarán en los casos siguientes:

   b.1 Para restaurar la operación de los sistemas después de un desastre (copia de seguridad del sistema).

   b.2 Para restaurar cualquier información que haya sido borrada o dañada accidentalmente (copias de seguridad de datos).

c. Para resguardar la seguridad de la información, el Departamento de Informática deberá contar con instalaciones de resguardo que garanticen la disponibilidad y almacenamiento de la copia de seguridad en un lugar ajeno a las instalaciones del Instituto.

d. Las cintas magnéticas, discos duros y ópticos de respaldo, entre otros, deberán ser fácilmente identificados y las etiquetas contendrán como mínimo los datos siguientes:

   d.1 Nombre del sistema.

   d.2 Fecha de creación.

   d.3 Clasificación.

   d.4 Plataforma a la que pertenece.

   d.5 Información del contacto en el Departamento de Informática del Instituto.

   d.6 Procedimientos documentados de restauración.

   d.7 Otros que se consideren necesarios.

e. La frecuencia de las copias de seguridad de la información institucional deberá ejecutarse diariamente y cada siete días una copia completa. Las copias se guardan dos meses como mínimo y un año como máximo.

f. Es responsabilidad del Departamento de Informática y del dueño de la aplicación verificar la confiabilidad de la copia de seguridad de la información, las cuales deberán ser sometidas a pruebas dos veces al año para asegurarse que los datos almacenados son recuperables.

21. DEL ANTIVIRUS

a. El Departamento de Informática es responsable que toda computadora o cualquier otro medio electrónico que se encuentre conectado a la red del Instituto, debiendo utilizar protección y contar con la configuración de un programa de antivirus.

b. El Departamento de Informática es responsable que cada servidor de archivos que se encuentre en la red del Instituto, utilice el *software* de protección antivirus aprobado por el Departamento de Informática para detectar y limpiar los virus que puedan infectar los archivos compartidos.

c. Cada entrada de correo electrónico debe ser filtrada por el *software* de protección antivirus aprobado e instalado por el Departamento de Informática.

22. DE LA DETECCIÓN DE INTRUSOS EN LA RED

a. El Departamento de Informática debe contar con equipos de detección de intrusos que permita realizar las acciones siguientes:

   a.1 *Monitorear* y auditar los sistemas de detección de intrusos sobre los equipos de cómputo y la red.

   a.2 Revisar los registros de eventos de detección de intrusos.

   a.3 Informar de las actividades sospechosas a la jefatura del Departamento de Informática.

b. Los equipos de detección de intrusos permitirán al Instituto alcanzar los objetivos siguientes:

   b.1 Aumentar el nivel de seguridad mediante la búsqueda activa de signos de intrusión no autorizada.

   b.2 Fortalecer la confidencialidad de los datos del Instituto en la red.

   b.3 Preservar la integridad de los datos del Instituto en la red.

c. Todos los registros de eventos del detector de intrusos deberán enviar una notificación en caso de un ataque al sistema del Instituto y conservarse durante un mínimo de 90 días, como evidencia para las auditorías de los acontecimientos pasados.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBGERENTE ADMINISTRATIVO

d. Las funciones de alerta de los servidores de seguridad (*cortafuegos*) y otros sistemas de acceso de red perimetral de control deberán estar habilitadas, porque serán objeto de seguimiento por el Departamento de Informática, el cual proporcionará la auditoría de los registros de eventos, conforme a lo instruido por el Jefe del Departamento de Informática.

e. Los controles de seguridad de los incidentes no podrán ser deshabilitados bajo ninguna circunstancia y el Departamento de Informática deberá atender de inmediato cualquier reporte de existencia de anomalías en el rendimiento del sistema, sospecha o intento de intrusiones.

23. DEL CONTROL DE EVENTOS DE SEGURIDAD

a. El Departamento de Informática para garantizar la seguridad de los sistemas de información del Instituto, deberá contar con las herramientas automatizadas que provean de notificaciones en tiempo real de la detección de irregularidades y explotación de vulnerabilidades. Estas herramientas deberán *monitorear* y reportar lo siguiente:

a.1 Tráfico de internet.

a.2 Tráfico de correo electrónico.

a.3 Tráfico de la red de área local -LAN- y protocolos.

a.4 Parámetros de seguridad del sistema operativo.

b. Los registros que el Departamento de Informática deberá verificar periódicamente, son los siguientes:

b.1 Automatización de registros de eventos de los sistemas de detección de intrusos.

b.2 Registro de eventos del dispositivo cortafuegos.

b.3 Registro de eventos de las cuentas de los usuarios

b.4 Registro de los eventos de escaneo de la red.

b.5 Registro de error de los sistemas.

b.6 Registro de eventos de aplicaciones.

b.7 Registro de los eventos de recuperación y copias de seguridad.

b.8 Incidentes de entradas por servicios de soporte de las distintas dependencias del Instituto.

b.9 Actividad telefónica - Informes detallados de llamadas.

b.10 Registro de impresas de red.

c. Adicionalmente a lo que establece el inciso b. de esta norma, el Departamento de Informática deberá realizar las evaluaciones siguientes:

c.1 Complejidad de la contraseña.

c.2 Dispositivos de red no autorizados.

c.3 Conectividad remota no autorizada.

c.4 Sistemas operativos y licencias de *software*.

d. Cualquier problema de seguridad descubierto será reportado a la jefatura del Departamento de Informática para que se realicen las investigaciones de seguimiento que correspondan.

24. DEL ACONDICIONAMIENTO DE LA SEGURIDAD DE LOS SERVIDORES

a. El Departamento de Informática para garantizar el buen funcionamiento del servidor deberá:

a.1 Instalar el sistema operativo conforme requisitos técnicos y aplicaciones o soluciones requeridas y aprobadas por el Departamento de Informática.

a.2 Aplicar actualizaciones suministradas por el fabricante del sistema operativo.

a.3 Remover el *software*, servicios de sistemas y controladores innecesarios.

a.4 Configurar parámetros de seguridad, protección de archivos y habilitar el registro de eventos de auditoría.

b. El Departamento de Informática supervisará los problemas de seguridad tanto internos como externos y realizará la liberación de las actualizaciones de seguridad en el momento oportuno.

c. El Departamento de Informática validará los aspectos de seguridad de los servidores de las dependencias del Instituto, para evaluar el cumplimiento de normas de seguridad y configuración.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBGERENTE ADMINISTRATIVO

25. DE LA COMUNICACIÓN INTERNA

El Departamento de Informática proporcionará la infraestructura necesaria para publicar y enviar información institucional a solicitud de las dependencias, previa autorización del Departamento de Comunicación Social y Relaciones Públicas que valida los diseños establecidos por el Instituto.

26. DEL *SOFTWARE* ADQUIRIDO POR EL DEPARTAMENTO DE INFORMÁTICA

a. El Departamento de Informática será responsable que los usuarios del Instituto utilicen únicamente el *software* autorizado.

b. En caso que un usuario requiera utilizar otra herramienta de *software* para realizar sus actividades laborales que no se encuentre instalado en su computadora, deberá solicitarlo al Departamento de Informática por escrito firmado y sellado por la máxima autoridad de la dependencia a la que pertenece.

c. El Departamento de Informática deberá evaluar cualquier programa que sea requerido en un ambiente diferente al de producción de los programas, previo a ser instalado y ejecutado en la red del Instituto y realizar lo siguiente:

   c.1 Verificación de la compatibilidad. Comprobar si se cumplen los requisitos para la instalación (*hardware* y *software*), en algunos casos es necesario desinstalar versiones antiguas del mismo *software*.

   c.2 Verificación de la integridad. Verificar que el programa es seguro para evitar la instalación de programas maliciosos.

27. DEL CONTROL DE ACTIVOS DE INFORMACIÓN

a. El Departamento de Informática debe llevar control de todos los equipos de cómputo del Instituto, debiendo registrar como mínimo: marca, modelo, número de serie, número de bien, etcétera.

b. El Departamento de Informática a solicitud de las dependencias del Instituto, efectuará revisiones técnicas a equipos de cómputo que están en trámite de baja de bienes de activo fijo, con el fin de validar su funcionamiento u obsolescencia y emitir dictamen técnico al respecto.

c. El Departamento de Informática podrá hacer uso del recurso de *hardware* en buen estado, pertenecientes a equipo de cómputo obsoleto, previa autorización de los Departamentos de Contabilidad y Auditoría Interna.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBGERENTE ADMINISTRATIVO

28. DE LA SOLICITUD DE USUARIOS PARA SISTEMAS INFORMÁTICOS DEL INSTITUTO

a. Las cuentas para cada servicio o sistema que sean creadas por el Departamento de Informática deberán estar respaldadas con una solicitud y una aprobación, previo a conferirles el acceso o modificaciones al mismo.

b. Las cuentas deberán estar identificadas únicamente con el nombre del usuario asignado y las contraseñas para esas cuentas deberán cumplir con lo que establecen las Normas Específicas del numeral 7 "DEL USO DE CONTRASEÑAS".

c. El personal responsable del control de las cuentas para los servicios informáticos o sistemas del Instituto deberá deshabilitar las cuentas y servicios de los trabajadores de la Institución por los motivos siguientes:

c.1 Que asuman nuevas responsabilidades.

c.2 Que el tiempo de acceso autorizado haya finalizado.

c.3 Que su relación laboral está por finalizar.

29. DE LA ACEPTACIÓN DEL USO DE SERVICIOS INFORMÁTICOS

a. El Departamento de Informática será responsable de facilitar los sistemas de comunicación a los trabajadores del Instituto con previa autorización, tales como correo electrónico, *intranet*, mensajería instantánea, entre otros designados para que las operaciones del Instituto sean efectivas y eficientes.

b. El Departamento de Informática debe velar por el buen uso de los servicios informáticos.

30. DEL ACCESO DE LOS PROVEEDORES A LOS RECURSOS TECNOLÓGICOS

a. Cada proveedor deberá proporcionar al Departamento de Informática un listado de los trabajadores de soporte técnico que trabajan en la empresa o institución, la cual deberá estar actualizada e informar los cambios de su personal al Departamento de Informática en un plazo de 24 horas.

b. La empresa o institución contratada deberá informar de inmediato de todos los incidentes de seguridad directamente al personal responsable del área en el Departamento de Informática.

V. ANEXOS

Glosario de Términos Técnicos

Acceso remoto: es poder acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa (como Internet).

ADSL: *Asymmetric Digital Subscriber Line*. Tecnología para transmitir información digital a elevados anchos de banda. A diferencia del servicio *dial up*, ADSL provee una conexión permanente y de gran velocidad. Esta tecnología utiliza la mayor parte del canal para enviar información al usuario y sólo una pequeña parte para recibir información del usuario.

Ancho de banda (*bandwidth*): expresa la cantidad de datos que pueden ser transmitidos en determinado lapso. En las redes se expresa en bps.

Antivirus: programa que busca y eventualmente elimina los virus informáticos que puedan haber infectado un disco rígido o disquete.

Base de Conocimiento: es un tipo especial de base de datos para la gestión del conocimiento. Provee los medios para la recolección, organización y recuperación computarizada de conocimiento.

Base de datos: conjunto de datos organizados de modo tal que resulte fácil acceder a ellos, gestionarlos y actualizarlos.

Controlador de dominio: almacena, mantiene y gestiona la base de datos de usuarios y recursos de la red.

Correo electrónico: es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente.

Directorio (*directory*): grupo de archivos relacionados entre sí que se guardan bajo un nombre.

Domain Name System: (DNS) sistema de nombre de dominio, es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al internet o a una red privada.

Hardware: los componentes físicos de la computadora y sus periféricos.

Intranet: es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.

LAN: *Local Area Network* - Red de Área Local. Red de computadoras interconectadas en un área reducida, por ejemplo, una empresa.

Monitoreo: evaluación de la calidad del control en el tiempo y permite al sistema reaccionar en forma dinámica, cambiando cuando las circunstancias así lo requieran.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
SUBGERENTE ADMINISTRATIVO

Se orienta a la identificación de controles débiles, insuficientes o innecesarios y promueve su reforzamiento.

***Open source* o *software* libre:** *Sotfware* de código abierto o libre, que en ocasiones permite el acceso a su código de programación, lo que facilita modificaciones por parte de otros programadores o usuarios que hacen uso del mismo. Este *software* es libre y se distribuye de manera gratuita.

Página Web: una de las páginas que componen un sitio de la *World Wide Web*. Un sitio web agrupa un conjunto de páginas afines. A la página de inicio se le llama "*home page*".

Protocolo: lenguaje que utilizan dos computadoras para comunicarse entre sí.

Red: en tecnología de la información, una red es un conjunto de dos o más computadoras interconectadas.

Repositorio de contraseñas electrónicas: es la base de datos fundamental que guarda las contraseñas electrónicas.

Servidor: computadora central de un sistema de red que provee servicios y programas a otras computadoras conectadas.

Sistema: es un módulo ordenado de elementos que se encuentran interrelacionados y que interactúan entre sí.

Sitio Web: colección de páginas web relacionadas y comunes a un dominio de Internet o subdominio en la *World Wide Web* en Internet.

Sistema operativo: programa que administra los demás programas en una computadora.

Software: término general que designa los diversos tipos de programas usados en computación.

Spam: correo electrónico no solicitado. Se lo considera poco ético, ya que el receptor paga por estar conectado a internet.

Unidades de almacenamiento: son dispositivos que, conectados a la computadora, permiten el almacenamiento de información (archivos).

Usuario: es una persona que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático.

Virus: programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye