HISTORIAL DE VERSIONES		
VERSIÓN	FECHA	RESUMEN DE MODIFICACIONES
00	11/12/2017	Documento Vigente.
01	17/12/2020	Actualización del Instructivo para adicionar las nuevas tendencias y herramientas tecnológicas que actualmente se utilizan en el IGD.
02	29/12/2022	Incorporación del Procedimiento para la ejecución de Respaldos y Recuperación de la Información del IGD.
03	31/03/2023	Incorporación del Procedimiento para regular las comunicaciones de telefonía del IGD.

FUNCIÓN	MEMORÁNDUMS/RP/ PUNTO DE ACTA	FECHA
Responsable:	Unidad de Tecnología de la Información. TI-0014-A-2023	07/03/2023
Revisor(es):	UL-0008-2023 AI-0005-2023 FP-0017-2023	29/03/2023 28/03/2023 23/03/2023
Aprobador(es):	RP-09310323	31/03/2023

Índice

1. Objetivo

Establecer Normas y Procedimientos de Seguridad Informática del Instituto de Garantía de Depósitos (IGD) para la protección y uso efectivo de los recursos tecnológicos en cuanto al acceso y cuidado de la información, explicando los factores y recomendaciones para el buen cumplimiento de esta normativa.

2. Alcance

Los empleados permanentes, temporales, eventuales y personal externo (auditores y consultores) que presten servicios dentro de las instalaciones de la Institución y/o fuera de la misma bajo la modalidad de teletrabajo, a quienes se les asigne recurso informático o que por la naturaleza de sus funciones utilicen datos, recursos tecnológicos e información de esta Institución están obligados al cumplimiento del presente instructivo.

3. Base Legal

El presente instructivo ha sido emitido en directa ejecución de la atribución asignada a la Presidencia del Instituto de Garantía de Depósitos en el literal O del Artículo 25 del Instructivo del Funcionamiento del Consejo Directivo.

4. Desarrollo

4.1. Uso de Recursos Tecnológicos

Los recursos tecnológicos son la herramienta que sirven al personal del IGD, para realizar labores que permitan lograr los objetivos institucionales. En tal sentido, solamente está permitido la utilización de éstos para los fines institucionales.

4.1.1 Usuarios Autorizados para utilizar los Recursos Tecnológicos

a) Se considera usuarios autorizados de los recursos tecnológicos de la institución a todos los empleados permanentes, a plazo definido, temporales o personas externas que la Presidencia autorice, previa solicitud hecha por *la unidad solicitante.* **(V01)**

b) Todo contratación temporal, a plazo definido o permanente del personal en el IGD, deberá ser notificado a la Unidad de Tecnología de la Información por la Presidencia del IGD o la Unidad administradora del contrato, para asignarle los derechos correspondientes (equipo de cómputo, creación de usuario en la red, perfil de usuario en el directorio activo, correo electrónico), esto se deberá hacer mediante el Sistema de Servicio de Asistencia Técnica. El anexo 6.1 del presente instructivo presenta un procedimiento para el uso del Sistema de Servicio de Asistencia Técnica.

c) *La Unidad de Tecnología de la Información administrará el sistema telefónico del Instituto para los funcionarios y empleados que estén facultados para el uso de telefonía fija, celular y/u oficina móvil, por medio del Procedimiento para regular las comunicaciones de telefonía del IGD.* **(V03)**

4.1.2 *Asignación de los Equipos de Tecnología* **(V01)**

a) *La Unidad de Tecnología asignará un equipo de cómputo a los empleados, a plazo definido, permanentes, temporales y personal externo, que por la naturaleza de su cargo lo requieran.*

b) *Los equipos tecnológicos asignados, se entregarán con un acta de recepción, para que el usuario y el jefe inmediato validen y firmen la recepción del equipo asignado.*

4.1.3 Responsabilidad en el uso de los Recursos Tecnológicos

a) Evitar acciones que puedan incurrir en daño, deterioro, pérdida o degradación de los recursos tecnológicos que provee la Institución.

b) Reportar de forma inmediata a la Unidad de Tecnología de la Información cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones asignados a los usuarios, así también los de uso común, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

4.1.4 Reporte de fallas y extravío de los Recursos Tecnológicos

a) Se deberán reportar inmediatamente cualquier falla detectada en los recursos tecnológicos bajo su utilización.

b) Dichas fallas serán reportadas mediante el Sistema de Servicio de Asistencia Técnica, a la Unidad de Tecnología de la Información, quien enviará el bien a dictamen técnico. Si de acuerdo al dictamen la causa del desperfecto es debido a descuido o negligencia del usuario, el costo de reparación y/o deducible del seguro del bien no cubierto por la Sociedad de Seguros, será trasladado al usuario que lo tiene asignado al momento del evento, a quien además se le trasladará el costo de los honorarios que cobre la empresa que realice el dictamen técnico aludido.

c) En caso de extravío, robo o hurto de algún recurso tecnológico que esté asignado a un usuario, éste deberá informar por escrito con atención a la Presidencia sobre dicho incidente con copia a *la Unidad de Tecnología de la Información.* Si el hecho se dio por negligencia del usuario, el personal que

tenga asignado los bienes al momento del evento deberá cancelar el valor de reposición de los mismos. **(V01)**

4.1.5 Uso y Resguardo de los equipos portátiles

a) Para poder trasladar o sacar de la Institución un recurso tecnológico de uso común el usuario deberá realizar una solicitud en el Sistema de Servicio de Asistencia Técnica.

b) Los usuarios que utilicen los equipos portátiles *deberán* devolverlos al lugar de resguardo destinados para ellos. **(V01)**

c) Una vez utilizados los equipos, *se debe* verificar que han sido guardados todos los accesorios pertenecientes a dicho equipo. Entiéndase como equipo portátil no sólo las computadoras, laptops sino también el equipo de proyección.

d) *Para el préstamo de los equipos de proyección y accesorios, el usuario solicitante deberá firmar el control de préstamo de equipos tecnológicos. Este control es gestionado por la Unidad de Tecnología.* **(V01)**

e) Se debe mantener el equipo informático en un lugar limpio y sin humedad.

f) Los usuarios deben asegurarse *de que* los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos. En caso de que no se cumpla, *se debe* solicitar una reubicación de cables con el personal de la Unidad de Tecnología de la Información. **(V01)**

4.2. Instalación, mantenimiento y uso de equipo Multifuncional

Define la metodología para el mantenimiento preventivo, correctivo y la responsabilidad sobre la instalación y configuración de dichos equipos de la Institución.

4.2.1 Instalación, Conexión y Configuración de los equipos

a) Será responsabilidad del personal de la Unidad de Tecnología de la Información, la instalación, conexión y configuración de los equipos informáticos de la Institución.

b) Los usuarios en general no están autorizados a cambiar la ubicación de los equipos de uso común, ni alterar las conexiones o configuraciones de los mismos. Cuando exista necesidad de realizar cambios en los equipos, ya sea de ubicación o de configuración, se deberá hacer el respectivo requerimiento a la Unidad de Tecnología de la Información según el Sistema de Servicio de Asistencia Técnica.

c) El usuario deberá solicitar asistencia técnica necesaria para el manejo de los recursos informáticos que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo los mismas.

4.2.2 Intercambio de piezas en los equipos

Cualquier cambio de partes o sustracción de piezas en los equipos informáticos, deberá ser realizado únicamente por el personal responsable de la Unidad de Tecnología de la Información o la empresa encargada de su mantenimiento o garantía, previo requerimiento realizado en el Sistema de Servicio de Asistencia Técnica.

4.2.3 Uso y responsabilidad de Equipo Multifuncional (Impresoras)

a) Los equipos multifuncionales serán asignados a la Unidad de Tecnología de la información, sin embargo, la responsabilidad y el uso son de forma general.

b) Los usuarios son responsables del uso racional de los impresores y deberán asegurarse de evitar el desperdicio por impresión de documentos incompletos o de versiones obsoletas, para ello deberán utilizar las consultas en pantallas y la presentación preliminar de los documentos antes de enviarlos a la impresora.

c) Cada usuario es responsable de retirar sus impresiones, y de colocar papel en caso de que dicho equipo lo necesitara.

d) La Unidad de Tecnología de la Información podrá reubicar los impresores de acuerdo con las necesidades de los usuarios.

e) La Unidad de Tecnología de la Información es la única que puede configurar los accesos para la impresión de los documentos.

f) Dicha Unidad creará los accesos para el recurso de copiado e impresión, y será la responsable de instalar los drivers correspondientes en el ordenador.

g) *Se llevará un control del consumo mensual de las impresiones realizadas y fechas de cambio de consumibles.* **(V01)**

4.2.4 Mantenimiento Preventivo y Correctivo de Equipo Informático

a) La Unidad de Tecnología de la Información, será responsable de asegurarse que se realicen los mantenimientos preventivos y correctivos según la necesidad o *de acuerdo al cronograma propuesto por* los proveedores para que todos los recursos tecnológicos trabajen de forma correcta. **(V01)**

b) Serán responsables de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella que se encuentre en el equipo, para dichos respaldos se asignará una carpeta en el servidor de archivos, previendo así la perdida involuntaria de información, derivada del proceso de reparación. *Los respaldos de la información se harán de acuerdo a lo regulado en el Instructivo de Archivo.* **(V01)**

4.3. Instalación de programas (Software)

Establece los lineamientos de instalación de programas que deben cumplir los usuarios que tengan a su cargo equipos informáticos para la buena utilización de los mismos.

4.3.1 Instalación de programas en computadoras personales

a) Toda instalación de programas en las computadoras personales de la Institución está a cargo únicamente de la Unidad de Tecnología de la Información.

b) Cuando exista *la* necesidad de la utilización de algún programa en particular, el usuario deberá *ingresar el requerimiento en el sistema de soporte para que sea verificado por la Unidad de Tecnología de la Información.* La cual, en virtud de las políticas correspondientes, deberá ser de uso legal. **(V01)**

4.3.2 Inventario de programas autorizados

La Unidad de Tecnología de la Información debe mantener y realizar cada año un inventario de los programas que están autorizados en la Institución. Asimismo, se debe mantener un inventario por computadora de los programas que cada máquina tiene instalado y se enviará una copia a Presidencia para su información.

4.3.3 Instalación de programas con base a licencias

Todo programa que requiera de licencia para su instalación podrá ser instalado únicamente bajo los términos y condiciones establecidas en el licenciamiento.

4.3.4 Instalación de programas de nula utilidad para la Institución

No está autorizada la instalación de programas que no beneficien a la Institución en el cumplimiento de sus metas (Ej. Reproductores de música, reproductores de video, juegos, etc.).

4.4. Daño o deterioro en Equipos Tecnológicos

Define las responsabilidades que deben de cumplir los usuarios de los Equipos Tecnológicos para evitar daños y deterioro.

4.4.1 Utilización bajo especificaciones del fabricante

a) Todos los equipos informáticos deben ser operados e instalados atendiendo las especificaciones que el fabricante proporciona.

b) Es responsabilidad de la Unidad de Tecnología de la Información, investigar estas especificaciones y proporcionar los elementos necesarios (manuales) para la debida utilización del equipo al usuario responsable.

c) Es deber de los usuarios el observar y seguir las instrucciones que le sean dadas por la Unidad de Tecnología de la Información en relación al uso del software y hardware asignado.

4.4.2 Alimentos, bebidas y otros objetos cerca de los Equipos Informáticos

a) No deben colocarse alimentos o bebidas en las cercanías de los equipos electrónicos o en lugares en que, ante un eventual accidente, el equipo pueda resultar afectado por el líquido o por el alimento, según corresponda.

b) Evitar tocar o manipular los equipos informáticos mientras toma sus alimentos. **(V01)**

4.4.3 Protección de computadoras portátiles

a) Los usuarios que utilicen computadoras portátiles deberán hacer uso del maletín correspondiente en las siguientes situaciones:
   i. Cuando se transporte el equipo hacia o desde el exterior de la Institución.
   ii. Cuando se requiera mantener almacenado el equipo.

b) Los maletines deben utilizarse para portar las computadoras portátiles y sus respectivos cables. A fin de evitar ejercer presión sobre el equipo.

c) Evitar tocar el monitor de éstas con objetos punzantes.

d) Siempre se debe posar la computadora sobre una superficie plana, firme con su respectivo candado y suficiente espacio.

e) Nunca se deberán colocar objetos sobre la computadora portátil, o tapar las salidas de ventilación del equipo.

f) En la medida de lo posible, cuando se transporte la computadora se deberá evitar realizar movimientos bruscos que puedan provocar daño al equipo.

g) En ningún caso deberá cargarse más allá de su capacidad de almacenamiento ni almacenarse más que lo indicado en la política.

h) La computadora portátil debe permanecer bajo la custodia de la persona a la cual se le ha asignado. No está permitido prestarla a usuarios no autorizados.

4.4.4 Apagado o Reinicio de los Equipos

a) Al finalizar su jornada laboral los usuarios son responsables de apagar los equipos que les han sido asignados, para el caso específico de las computadoras, deben apagarlas a través del menú "INICIO" de Windows.

b) El apagar bruscamente el equipo, daña los archivos del sistema, en caso de tener dudas con respecto a la forma correcta, solicitar asistencia a la Unidad de Tecnología de la Información.

c) En caso de necesitar reiniciar las computadoras y que por cualquier razón no sea posible realizarlo con el botón "Reiniciar", se podrá apagar el equipo y para encenderlo nuevamente deberá esperar el tiempo requerido para hacerlo, esto es porque es necesario detener cada una de las partes que se encuentra en funcionamiento, especialmente el disco duro.

d) Si después del reinicio, el equipo presenta un problema, deberá notificar inmediatamente a la Unidad de Tecnología de la Información para solucionar dicho problema.

e) En el caso de equipos compartidos (impresores, scanner, entre otros), todos los usuarios del recurso son responsables de apagarlo, previa verificación de que nadie más seguirá utilizando el equipo.

4.5. Control de Acceso

Define el área lógica del Sistema de Control de Acceso a la red del IGD, con un énfasis específico en la Administración de las Claves de Acceso y Procesos de Conexión a los Sistemas Informáticos.

4.5.1 Contenido de contraseñas

a) Todas las contraseñas deben de tener por lo menos 8 caracteres en su conformación.

b) Todas las contraseñas seleccionadas por los usuarios, dentro de la longitud mínima permitida, deberán contener al menos un carácter alfabético.

c) Los caracteres no alfabéticos o numéricos incluyen números (0-9) y puntuaciones.

d) Todas las contraseñas escogidas por el usuario deben de ser difíciles de suponer.

e) Todas las contraseñas seleccionadas por los usuarios deberán contener al menos un carácter en letra mayúscula o minúscula, esto ayuda a crear contraseñas difíciles de adivinar de parte de personas no autorizadas, hackers o espías industriales.

f) Los usuarios no deberán utilizar contraseñas que son idénticas a contraseñas previamente empleadas, se almacenara un total de 12 contraseñas a fin de evitar se reciclen o se utilicen nuevamente.

g) Todas las contraseñas seleccionadas por los usuarios deben de ser pronunciables, de tal forma que el usuario pueda recordarlas con facilidad.

h) Cada 45 días el usuario tendrá que cambiar su contraseña como medida de seguridad.

i) Los usuarios resguardarán sus contraseñas en una carpeta dentro del servidor de archivos, mediante una aplicación encriptada que la Unidad de Tecnología asigne, cada usuario tendrá una llave maestra de sus contraseñas y deberá ser entregada a Presidencia. El anexo 6.2 del presente instructivo presenta un procedimiento para proteger y resguardar las contraseñas.

4.5.2 Grado de dificultad en la conformación de la Contraseña

Las contraseñas seleccionadas no deberán de incluir los siguientes aspectos:

a) Derivaciones de la identidad del usuario.
b) Secuencia de caracteres comunes tales como "123456789".
c) Detalles personales tales como el nombre de esposo(a), hijos o familiares, mascotas.
d) Número de identificación de la licencia de conducir o de vehículo.
e) Número de identificación del seguro social.
f) Fecha de cumpleaños personal o familiares (al menos que acompañe la clave con caracteres adicionales que no estén relacionados).
g) Nombres propios.
h) Localización geográfica.
i) Siglas comunes (eje. IGD, BCR, SSF, SV, SP, Integración, VARE, NPB4-22, NRSF-01, entre otros)
j) Dialectos del ambiente o lenguaje coloquial.

Las contraseñas no deberán almacenarse en forma legible en archivos, scripts de conexión automática, teclas de función de terminales, en computadores sin ningún control de acceso u en otras localizaciones donde el personal no *esté* autorizado pueda descubrirlas. **(V01)**

4.5.3 Uso de Contraseñas

a) Para impedir un ataque especulador de contraseñas, se limitará a 5 intentos consecutivos para ingresar una contraseña incorrecta.

b) Después de tres intentos no exitosos de querer ingresar una contraseña, el código del usuario (User-ID) deber ser suspendido hasta que sea restablecido por la Unidad de Tecnología de la Información.

c) Todas las contraseñas deberán ser inmediatamente cambiadas, si existe la sospecha de que han sido descubiertas, o se tenga conocimiento que han sido descubiertas por partes no autorizadas.

d) Si un sistema de cómputo multiusuario emplea contraseñas fijas como un mecanismo de control de acceso primario, todas las contraseñas administrativas del sistema multiusuario deberán ser inmediatamente cambiadas, después de evidenciar que el acceso al sistema ha sido violentado o descubierto.

e) De forma instantánea, todos los usuarios deberán ser instruidos a cambiar sus contraseñas fijas en este sistema y en todos aquellos donde las hayan definido de forma similar.

f) Independiente de las circunstancias, la contraseña nunca deberá ser compartida o revelada a nadie, el hacer esto, se expone al usuario autorizado a responsabilizarse de acciones que la otra parte realice con el uso de la contraseña.

g) Los usuarios son responsables de todas aquellas actividades ejecutadas con su código de usuario (User-ID) personal.

h) Los usuarios no deben permitir a otros ejecutar cualquier tipo de actividad con sus User-ID.

i) Todo solicitud o cambio de contraseña deberá ser solicitada a la Unidad de Tecnología de la Información.

4.5.4 Bloqueo de Usuarios Ausentes

a) Cuando un usuario se retire o ausente por tiempo igual o mayor a dos semanas, la jefatura inmediata tiene la responsabilidad de notificar a la Unidad de Tecnología de la Información para que bloquee el usuario.

b) En caso definitivo de retiro del usuario de la institución también se deberá informar a la Unidad de Tecnología de la Información para que elimine dicho usuario de la red y reasignar los roles al nuevo usuario responsable.

4.5.5 Reasignación de contraseña y Monitoreo de actividades

a) Si el usuario involucrado ha olvidado o perdido su contraseña.

b) La Unidad de Tecnología de la Información realizará monitoreo de las actividades realizadas por el usuario cuando utilice recursos de tecnología de la Información.

c) El monitoreo se realiza para que el usuario utilice adecuadamente los recursos tecnológicos de la mejor manera.

4.5.6 Ingreso y Salida a Sistemas

a) Si el sistema al que los usuarios están conectados contiene información sensible o valiosa, los usuarios no deberán desatender su terminal, estación de trabajo o PC, sin antes salirse de su aplicativo o sesión y bloquear su estación de trabajo.

b) Cuando no exista actividad en la estación de trabajo o computador (PC) por *5* minutos, el sistema administrador bloqueará la estación de trabajo. **(V01)**

c) Si el sistema administrador no tiene la función para realizarlo de forma automática, es responsabilidad total del usuario el bloquear su equipo al levantarse.

4.5.7 *Dispositivos de almacenamiento externos* (V01)

El uso de dispositivos de almacenamiento externo está permitido en el IGD para los empleados y consultores, con el fin de facilitar el compartir y transportar información que no sea de carácter confidencial ni sensible de la institución dentro de las normas y responsabilidades del manejo de información institucional.

En caso de que sea información sensible solicitada por auditorías, se permite el traslado por dispositivos de almacenamiento externo.

Es responsabilidad del usuario al momento de utilizar un dispositivo de almacenamiento, ejecutar el respectivo análisis para detectar amenazas (virus).

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos, mediante una conexión inalámbrica directa o cualquier equipo de cómputo del Instituto. Entre estos, se pueden encontrar, pero no se limita a:

i. *Memoria USB*
ii. *Reproductores portátiles MP3/MP4*
iii. *Cámaras con conexión USB*
iv. *iPhone/Smartphones*
v. *SD Cards/Mini SD Cards/Micro SD Cards*
vi. *Tablet*
vii. *Dispositivos con tecnología Bluetooth*
viii. *Discos duros de uso externo*

El acceso y empleo de servicios de almacenamiento de archivos OneDrive está permitido utilizando la cuenta institucional de Microsoft. Los demás servicios tales como Google Drive, SkyDrive, Dropbox, Rapishare, MediaFire, 4share, etc. no están permitidos.

En caso de requerir la utilización de otros servicios de almacenamiento en la nube, se deberá consultar con la Unidad de Tecnología para evaluar la factibilidad del uso.

<u>Uso indebido de dispositivos de almacenamiento externo:</u>

a) *Almacenar o transportar información sensible, confidencial o reservada del IGD.*

b) *Ejecutar cualquier tipo de programa no autorizado por el Instituto desde cualquiera de las unidades de almacenamiento en mención.*

c) *Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en la redes y equipo informáticos.*

d) *Utilizar mecanismos y sistemas que intenten ocultar o suplantar de alguno de esto medios de almacenamiento.*

e) *Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información privada de los usuarios o colaboradores del Instituto.*

No obstante, lo anterior, es importante mencionar que, para el cumplimiento de las funciones y objetivos del Instituto, la Unidad de Tecnología de la Información podrá en todo momento y en cualquier Unidad o puesto de trabajo operar, almacenar, adquirir o retirar dispositivos de almacenamiento externo que les permite garantizar la seguridad de la información del IGD.

Responsabilidades:

a) *Cada empleado o colaborador es responsable de conocer, adoptar y acatar esta política.*

b) *Cada empleado es responsable por el uso de la información a su cargo y de los dispositivos de almacenamiento externo que emplee para el transporte de dicha información.*

c) *Cada usuario deberá velar que estos medios de almacenamiento externos estén libres de software malicioso, espía o virus, para lo cual deberá realizar una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la Institución, por medio de software de antivirus dispuesto para tal fin. En caso de que la Unidad de Tecnología detecte presencia de troyanos, virus, malware, etc. procederá a informar sobre la situación al Jefe inmediato para que se tomen las medidas correspondientes.*

d) *Todos los eventos realizados sobre los dispositivos de almacenamiento externo, conectados a cualquier equipo de cómputo de la Institución, podrán ser auditados con el ánimo de registrar y controlar las actividades sobre cada uno de estos, la ubicación y usuario que los empleó. Dichos reportes podrán ser solicitador por Presidencia.*

Los intentos de habilitar el uso de estos dispositivos donde su uso ha sido negado o no autorizado igualmente podrán ser registrados. **(V01)**

4.5.8 Uso recomendable del sistema VPN (Acceso Remoto)

a) Es responsabilidad del usuario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.

b) El uso del sistema VPN debe ser controlado utilizando una contraseña de autenticación fuerte, manteniéndola siempre en secreto.

c) *La VPN debe ser configurada en una computadora del IGD, u otra que tenga las mínimas condiciones de seguridad iguales o similares a las de los equipos del IGD.* **(V01)**

d) Las puertas de enlace VPN serán configuradas y administradas por La Unidad de Tecnología de la Información.

e) Los usuarios del sistema VPN serán automáticamente desconectados de la sesión, una vez que hayan transcurrido 30 minutos de inactividad. El usuario deberá conectarse nuevamente para volver a *ingresar* a la red. **(V01)**

f) *La Unidad de Tecnología deberá deshabilitar los accesos de VPN luego de que éstos hayan sido utilizados por los usuarios solicitantes.* **(V01)**

g) *En caso de requerir acceso de VPN, se deberá solicitar por correo electrónico a Presidencia con copia a la Unidad de Tecnología de la Información.* **(V01)**

h) *El procedimiento de uso de la VPN está en el anexo 6.3.* **(V01)**

4.6 Correo Electrónico

Establece los lineamientos bajo los cuales el personal de la Institución debe utilizar el correo electrónico o e-mail para el desempeño de sus labores, así como las responsabilidades, obligaciones y derechos de los usuarios de este servicio.

4.6.1 Creación de Cuentas de Correo Electrónico

a) La Unidad de Tecnología de la Información será únicamente la responsable de la creación de las cuentas de correos electrónicos.

b) Para definir la creación de la cuenta se utilizará la primera letra del nombre y el primer apellido del usuario según corresponda. (Esta política se utilizará para los nuevos usuarios, y para los que ya tengan cuentas asignadas que no cumplan con dicho caso se le creará un alias para poder tener orden en las cuentas).

c) En caso de dos o más usuarios coincidan en nombre y apellido se utilizará cualquier combinación formada con el segundo nombre y el segundo apellido, o utilizando las iniciales de tal forma que la cuenta sea única.

d) El espacio de los buzones de correo electrónico que residan en el servidor tendrá una cuota asignada en función del espacio disponible en el servidor y el número de cuentas de usuarios.

4.6.2 Utilización del Correo Electrónico

a) El correo electrónico deberá ser utilizado para propósitos institucionales, de intercambio de información técnica o de cualquier otra información necesaria para el eficiente desempeño de las funciones de las distintas unidades de la Institución.

b) Todo correo electrónico enviado institucionalmente se considera una remisión oficial y tendrá la misma validez que el que envió tradicional en papel. Excepto aquellos documentos que requieran tener firma y sello correspondiente.

c) Es deber de cada empleado utilizar el sistema de correo electrónico de forma responsable, profesional legal y ética.

d) Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

e) Será responsabilidad de los usuarios el depurar la información contenida en su buzón, de lo contrario se *aplicarán* las políticas configuradas en la institución. **(V01)**

f) Solamente el software que provea la Institución para correo electrónico será el autorizado para tal fin.

g) En caso de fallas en el Correo Institucional se permitirá el uso de correos electrónicos externos (por ejemplo: Gmail, Hotmail o Yahoo!).

h) Los correos electrónicos con carácter de aviso a todo el personal y que por lo tanto tengan una fecha de vigencia, deberán enviarse con la opción de caducidad del mensaje, los cuales dichos mensajes serán borrados automáticamente, si no fueran leídos por el destinatario pasada la fecha de vigencia.

i) Los empleados son responsables por sus cuentas de correo y de los mensajes enviados, antes de enviar un mensaje revise el texto que lo compone y los destinatarios.

j) *La recepción* de información no solicitada e indeseada se debe reportar a la Unidad de Tecnología de la Información para su monitoreo y bloqueo si fuese posible. **(V01)**

k) La Unidad de Tecnología de la Información podrá realizar investigaciones al contenido de los buzones del correo electrónico, siempre y cuando se cuente con una autorización de Presidencia y que esta actividad este orientada a solucionar problemas de seguridad.

4.6.3 Prohibiciones sobre el uso del Correo Electrónico

a) El usuario deberá abstenerse de participar y divulgar "cadenas de correo electrónico" o contenido no relacionado al Instituto. En caso de encontrar a un usuario participando en dichas cadenas de correo, se levantará un reporte por incumplimiento de política.

b) Quedan prohibidas las discusiones públicas entre dos o más personas a través del correo electrónico, que involucren a terceros con el fin de llamar la atención.

c) El usuario podrá sustituir el correo Institucional por un correo personal, *en caso de algún incidente que lo requiera, previa a la solicitud a Presidencia.* **(V01)**

d) Los usuarios no deberán utilizar su dirección electrónica institucional como referencia en suscripciones de carácter personal.

e) No deberán enviar correos a través de cuentas ajenas, ni permitir que nadie más envíe correos electrónicos usando su cuenta.

f) Cualquier material fraudulento, amenazante, sexualmente explícito, obsceno, intimidante, difamatorio o de alguna manera ilegal o inapropiado, no debe ser enviado por correo electrónico, ni mostrar o almacenar en el sistema de correo electrónico institucional. Los empleados que encuentren o que reciban esta clase de material deben inmediatamente dar a conocer el incidente a su Jefe inmediato y a la Unidad de Tecnología de la Información.

g) Toda comunicación electrónica recibida de forma repetitiva e indeseada puede ser considerada acoso. En general, la comunicación dirigida a una persona específica con la intención de acosarla o amenazarla queda prohibida.

h) Los usuarios no deberán utilizar las opciones de confirmación de entrega y lectura a menos que sea un mensaje muy importante, es innecesario para su uso, ya que provoca mucho tráfico en la red.

i) Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

j) Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

k) Los usuarios deberán evitar el envío de archivos adjuntos de gran tamaño (25MB). En caso de ser necesario, se deberá enviar el enlace de la ubicación del archivo dentro del servidor de archivos. *Si es un envío para personas fuera de la Institución, se podrá hacer los envíos de enlaces mediante el servicio de OneDrive.* (V01)

l) El usuario deberá abstenerse de abrir aquellos correos electrónicos cuya procedencia se desconozca y eliminar inmediatamente dichos correos para evitar ser infectados de virus. Si existiera dudas duda de cómo eliminarlos, solicitar asistencia a la Unidad de Tecnología de la Información para poder resolverlo.

4.6.4 Envío de Correos Electrónicos Institucionales

a) Cualquier divulgación de avisos institucionales, actividades culturales, deportivas o sociales podrán ser hechas a través del correo electrónico únicamente por la unidad responsable de acuerdo con su área.

b) En el caso específico de alertas de seguridad informática o suspensión de servicios informáticos, será únicamente la Unidad de Tecnología de la Información la autorizada a enviar este tipo de correos.

c) Toda información de carácter confidencial enviada a través de correo electrónico deberá ser protegida por algún medio que asegure la confidencialidad de la información transmitida, por ejemplo, por contraseña, compresión de archivos con contraseña, certificados digitales o encriptación de mensajes. Sin embargo, en la medida de lo posible no enviar información de carácter confidencial de la Institución.

4.7 Herramientas de trabajo colaborativas (Microsoft Teams) (V01)

Establece los lineamientos bajo los cuales el personal de la Institución debe utilizar las herramientas de trabajo colaborativas para el desempeño de sus labores, así como las responsabilidades, obligaciones y derechos de los usuarios de este servicio.

4.7.1 U*tilización de las herramientas de trabajo colaborativo* (V01)

a) Cada usuario con correo electrónico asignado tendrá a su disposición la herramienta de trabajo colaborativo que designe la Unidad de Tecnología.

b) La herramienta de trabajo colaborativa deberá ser utilizada exclusivamente para usos institucionales donde se podrá compartir documentos para el trabajo en conjunto entre unidades del Instituto.

c) Es responsabilidad del usuario asignado toda publicación realizada en la herramienta de trabajo colaborativa.

4.7.2 *Prohibiciones de las herramientas de trabajo colaborativo* (V01)

a) El usuario deberá abstenerse de escribir contenido no relacionado al Instituto. En caso de encontrar a un usuario participando en conversaciones ajenas al Instituto, se levantará un reporte por incumplimiento de política.

b) Cualquier material fraudulento, amenazante, sexualmente explícito, obsceno, intimidante, difamatorio o de alguna manera ilegal o inapropiada, no debe ser enviado por la herramienta de trabajo colaborativo. Los empleados que encuentren o que reciban esta clase de material deben inmediatamente dar a conocer el incidente a su Jefe inmediato y a la Unidad de Tecnología de la Información.

c) Toda comunicación recibida de forma repetitiva e indeseada puede ser considerada acoso. En general, la comunicación dirigida a una persona específica con la intención de acosarla o amenazarla queda prohibida.

4.8 Antivirus

Define la utilización, recomendación de uso de software de antivirus por computadora.

4.8.1 Utilización de antivirus

a) Todas las computadoras personales y servidores de la Institución deben tener instalado el Software de Antivirus.

b) La Unidad de Tecnología de la Información será la responsable de definir qué antivirus se deberá instalar a los equipos de la institución.

c) Por ningún motivo el usuario podrá sustituir el antivirus que sea definido por la Unidad de Tecnología de la Información.

d) Los usuarios del IGD deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, por lo cual deberán ejecutar el software antivirus autorizado por la Unidad de Tecnología de la Información.

e) Todos los archivos de computadoras que sea proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tenga que ser descomprimidas, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

4.8.2 Actualización de base de datos de virus y vacuna

a) Es responsabilidad del personal de la Unidad de Tecnología de la Información velar por la oportuna actualización de la base de datos de virus y vacunas, del antivirus instalado en la Institución. Para ello, dicha unidad debe implantar y mantener funcionando un procedimiento, que garantice la constante actualización del antivirus.

b) Para el caso de los usuarios que permanecen fuera de la Institución, y que en virtud de sus funciones deben conectarse a redes externas, éstos deberán actualizar la base de datos de virus y vacunas.

4.8.3 Activación de antivirus e impedimento para desactivarlo

a) Toda computadora que esté en funcionamiento deberá mantener habilitada las funciones de protección contra virus que proporciona el antivirus. Como mínimo, deben estar activas las funciones de verificación del sistema, verificación de correo electrónico, y verificación de descargas de Internet.

b) Para las computadoras que tengan instalado antivirus, éste deberá estar configurado de tal manera que periódicamente se active automáticamente para revisar todo el sistema (memoria y discos duros) en busca de virus. Esta revisión no debe ser cancelada ni desactivada por los usuarios.

c) Sin perjuicio de lo anterior, la Unidad de Tecnología de la Información debe hacer uso de las opciones de seguridad del programa antivirus para evitar que el usuario tenga acceso a las opciones de configuración o desactivación.

4.8.4 Notificación sobre desactivación de antivirus

a) Los usuarios deberán notificar a la Unidad de Tecnología de la Información cuando detecten que el antivirus se ha desactivado.

b) Cualquier usuario que sospeche de alguna infección por virus en el ordenador o host, deberá de reportar inmediatamente a la Unidad de Tecnología de la Información para la revisión y erradicación del virus.

4.9 Internet

Establece los lineamientos bajo los cuales el personal de la Institución debe utilizar la navegación en la red pública Internet en el desempeño de sus labores, así como las responsabilidades, restricciones, obligaciones y derechos de los usuarios de este servicio.

4.9.1 Autorización del servicio de navegación en Internet.

a) El acceso a la navegación en Internet y al correo electrónico externo se proporcionará a aquellos usuarios para quienes la Presidencia autorice.

b) La utilización del Internet es para el desempeño de sus funciones y cargo en la institución del IGD, y no para propósitos personales.

c) El usuario deberá responder por el uso racional de los recursos de Internet. Será responsabilidad de la Unidad de Tecnología de la Información proveer la configuración necesaria para dar acceso a la navegación en Internet a aquellos usuarios que hayan sido autorizados.

d) Cada usuario es responsable del uso apropiado del servicio de Internet proveído por la Unidad de Tecnología de la Información. **(V01)**

e) La Unidad de Tecnología podrá llevar un control de los sitios visitados por los usuarios y podrán ser requeridos por la Presidencia del Instituto. **(V01)**

4.9.2 Modificaciones del Navegador y Descarga de Programas

a) Queda prohibido a los usuarios hacer modificaciones a la configuración del navegador realizada por la Unidad de Tecnología de la Información.

b) Queda prohibido descargar programas o archivos de Internet, música, protectores de pantalla, videos y otros elementos sin autorización de la Unidad de Tecnología de la Información.

c) En caso de requerir descarga de software desde internet para efectos de evaluación, deberá de notificarse a la Unidad de Tecnología de la Información.

d) En caso de aprobación de dicha descarga, la Unidad de Tecnología de la Información registrará y descargará el respectivo software en un área de evaluación asignada por la unidad.

4.9.3 Sitios Restringidos

a) En la navegación en Internet queda prohibido el acceso a los sitios relacionados con los siguientes temas:
   i. Crimen, violencia y armas.
   ii. Uso de estupefacientes.
   iii. Entretenimiento y juegos.
   iv. Música y cine.
   v. Juegos de apuestas.
   vi. Charlas interactivas (Chats)
   vii. Ciencias ocultas y astrología.
   viii. Sexualidad y pornografía.
   ix. Sitios de Hackers.
   x. *Y otros sitios que no abonen con el trabajo* **(V01)**

b) Dichas Prohibiciones se hacen por motivos de seguridad, ya que los sitios antes mencionados son de mayor vulnerabilidad, y por medio de ellos los usuarios pueden contraer amenazas de software dañinos como "malware, phishing y robo de información".

c) Será responsabilidad de la Unidad de Tecnología de la Información dar seguimiento a esta política y notificar a la Presidencia cuando un usuario no respete dicha política.

d) En caso de requerir un acceso a algunas de los temas antes mencionado, deberá ser notificado a Presidencia y con visto bueno se evaluará la asignación de dichos permisos.

4.10 Respaldo de Datos

Toda la información que se encuentre en las áreas de almacenamiento institucional deberá ser respaldada diariamente a fin de garantizar al usuario la información contenida en los servidores del IGD. (*véase el anexo 6.4 Procedimiento para la ejecución de Respaldos y Recuperación de la Información del IGD*) **(V02)**

4.10.1 Responsabilidad del Respaldo de Información

a) Será responsabilidad de la Unidad de Tecnología de la Información el mantener un respaldo diario de la información contenida en las áreas de almacenamiento institucional, así como su correspondiente verificación.

b) La información que no se encuentre en dichas áreas será de exclusiva responsabilidad del usuario al que pertenece.

c) Los respaldos deben estar muy bien protegidos, sobre todo aquellos que han sido destinados a conservarse por un período más largo.

d) Estos respaldos deben estar almacenados en un lugar distinto a las instalaciones físicas del instituto, por lo menos el respaldo que será resguardo por más tiempo.

e) Deberán guardarse en un lugar físico estratégicamente seleccionado.

f) Para garantizarnos la calidad de los respaldos, deberá validarse el mecanismo restaurando cada cierto tipo la información contenida tanto el medio principal de respaldo como el alterno.

g) Los respaldos deberán desarrollarse en un ambiente con redundancias para asegurar la información en caso de fallas en los componentes principales.

h) Deberá realizarse copias de respaldo adicionales, estas copias deberán realizarse en un segundo medio de almacenamiento.

i) Los medios alternos deben estar en uno diferente al utilizado como principal o central, deberá ser una copia que no sea producida en el mismo depósito.

4.10.2 Elaboración de Respaldos Diarios

a) Deberá realizarse respaldos diariamente y serán de tipo Incremental, conservándose al menos por cuatro semanas.

b) La frecuencia de este tipo de respaldo debe ser cada 24 horas máximo y dependiendo de la cantidad de documentos que se genere, será realizada en cada día laboral.

4.10.3 Elaboración de Respaldos Semanales

a) Deberá realizarse por lo menos un respaldo de tipo Total cada semana, conservándose durante un trimestre.

b) Se realizará cada viernes y se conservarán durante cuatro meses, mensualmente se tendrá un mínimo de cuatro respaldos Totales.

c) En caso de que viernes sea un día festivo, se realizará ya sea el siguiente día hábil y el ultima anterior.

d) Un respaldo Semanal (Total) más cinco ó cuatro respaldos Diarios (Incremental), deberán contener una semana de trabajo.

4.10.4 Elaboración de Respaldos Mensuales

a) Deberá realizarse un respaldo de tipo total una vez al mes.

b) Este respaldo se realizará el último día hábil de cada mes o el primero en los casos en que se encuentren días festivos en el fin de mes.

c) La cinta que contenga este respaldo deberá ser guardada en una caja de seguridad y conservarla por lo menos tres años.

d) Las cintas para este tipo de respaldo serán etiquetados de la siguiente manera: IGDYYYY-BCKNN, donde YYYY corresponde al año en ejecución y NN un correlativo de cintas.

4.10.5 Programación de Respaldos

a) Los respaldos incrementales o totales deberán realizarse en una hora en que los archivos de interés no estén en uso, garantizado así que la copia de seguridad se obtenga de la mayor parte de los archivos.

b) Hacer los respaldos durante los momentos de bajo tráfico en la red es porque un respaldo consume recursos del sistema como tiempo en CPU.

4.11 Comunicación entre Redes de Datos

Define controlar y asegurar la conexión a la red Institucional, esta política está orientada a controlar el acceso a todos los recursos existentes en la red interna.

4.11.1 Puntos de Red

a) La utilización de los puntos de red debe ser de uso exclusivo para el personal de la Institución, exceptuando aquellos casos autorizados por la Unidad de Tecnología de la Información.

b) Ningún usuario está autorizado para manipular ningún punto de red de la Institución.

c) Los puntos de red serán controlados y administrados por la Unidad de Tecnología de la Información.

d) Cada punto de red deberá estar debidamente identificado y enumerado de la siguiente manera: D-01, donde D corresponde a datos y 01 un correlativo.

e) Se habilitará el acceso a conexiones inalámbricas como extensión del servicio de red local.

f) Todo punto de red no utilizado será deshabilitado de la Red por parte de la Unidad de Tecnología de la Información.

4.11.2 Administración y Configuración de los Accesos a Red

a) La información correspondiente a la configuración de las estaciones de trabajo para el acceso a la red es de uso exclusivo de la Unidad de Tecnología de la Información y NO será divulgada por parte del usuario o técnico bajo ninguna circunstancia.

b) Todo usuario que requiera una configuración de red tendrá que ser justificada por medio del Sistema de Servicio de Asistencia Técnica, con la aprobación de su superior.

4.11.3 Restricción para Acceso a la Red del Usuario

a) No está permitido que el empleado utilice o acceda con su cuenta de usuario a la red Institucional desde otro equipo que no sea el que tiene asignado.

b) Únicamente se permitirá en aquellos casos que el equipo sea de uso compartido (ejemplo: equipo portátil y estaciones de trabajo utilizados para presentaciones o ejecución de aplicaciones centralizadas) o autorizados por la Unidad de Tecnología de la Información.

c) No se permitirá que el empleado conecte su cable de red en un punto de red que no sea el que le corresponde, ya que, si lo hace, estaría bloqueando ese punto de red, y tendría que solicitar a la Unidad de Tecnología de la Información que pueda desbloquear dicho punto.

d) No está permitido que se utilice equipo NO Institucional para acceder a la red Institucional.

e) Todo equipo que no sea Institucional y requiera ser utilizado en la red de la Institución tendrá que solicitar con previa autorización de su superior a la Unidad de Tecnología de la Información para que valore y de acceso a dicho equipo.

4.12 Dispositivos de Red

Define los parámetros de configuración de los dispositivos de Red, así como la responsabilidad y uso de dichos recursos.

4.12.1 Firewall

a) La red de datos institucional al tener conectividad con otra sea red privada o red del proveedor de comunicaciones se deberá instalar y activar un escudo protector como punto de separación de estas redes.

b) Deberá crearse los segmentos de red necesarios para mantener la seguridad del acceso a la misma.

c) Dicha segmentación deberá ser hecha a través del escudo de seguridad, de manera que el riesgo sea minimizado.

d) La administración del Escudo de Seguridad es de exclusiva responsabilidad de la Unidad de Tecnología de la Información.

e) El acceso a la consola de administración del Escudo de Seguridad debe de hacerse de dos maneras:
   i. Directamente en la consola del equipo.
   ii. En forma remota usando comunicación encriptada.

f) La configuración básica del fabricante deberá modificarse de acuerdo con los requerimientos de seguridad de la Institución.

g) El servicio básico de rastreo o Ping será desactivado en el Escudo de Seguridad antes de ponerse en producción.

h) Se activará la caducidad en tiempo por inactividad a toda sesión remota hecha en el Escudo de Seguridad.

i) El nombre de la cuenta de servicio de administración del Escudo de Seguridad será cambiado y la contraseña se cambiará según las normas de seguridad relacionada a Contraseñas.

j) Todo servicio entre la red de datos interna y redes de datos externas será restringido y filtrado a través del Escudo de Seguridad.

k) Cualquier excepción será aprobada por la Unidad de Tecnología de la Información.

l) El acceso a los servicios públicos ubicados en las redes perimetrales será habilitado únicamente a través del Escudo de Seguridad.

m) Se crearán listas de acceso para estaciones o servidores en el Escudo de Seguridad para acceder a un servicio Interno o Externo.

n) Se exceptuará en caso de que existan servicios que requieran acceso a horas diferentes o permanentes.

4.12.2 Routers y Switches

a) El router Institucional o del proveedor deberá tener por lo menos dos Interfaces de red. Dichas interfaces serán para conectarse a la red del Proveedor y la otra para la red Institucional.

b) Si el router instalado es propiedad del proveedor se solicitará la creación de una cuenta de usuario de sólo lectura para acceder a la configuración del mismo para efectos de monitoreo.

c) Todo equipo ajeno a la institución tendrá como punto de llegada un puerto de un concentrador proporcionado por el Instituto para efectos de conectividad.

d) Todo dispositivo de red administrable remotamente, como routers y switches serán protegidos por contraseña para su utilización.

e) La Unidad de Tecnología de la Información, será la responsable de administrar dichas credenciales.

4.12.3 Red Inalámbrica Usuarios e Invitados (Wireless)

a) La red inalámbrica de Usuarios como la de Invitados es parte de la red de datos del IGD y como en esta, el uso que se hace de ella debe ser acorde con los fines y el buen nombre de la Institución.

b) La Unidad de Tecnología de la Información es la encargada de brindar los accesos para dichas redes.

c) El usuario por ningún motivo o razón podrá revelar el password de la red de Usuarios, para que otro usuario no autorizado tenga acceso a dicha conexión.

d) No podrán utilizar la red inalámbrica para dar conexión a su teléfono celular o Tablet. En caso contrario tendrá que ser autorizado por medio de su superior, a la Unidad de Tecnología de la Información para su aprobación.

e) Cada 45 días la Unidad de Tecnología de la Información deberá cambiar la contraseña de la red de Invitados por motivos de seguridad.

4.13 Seguridad Física

Define las responsabilidades y características que debe de contemplar el Data Center, así como la utilización de los Ups y Aires Acondicionados.

4.13.1 Data Center

a) Es responsabilidad de la Unidad de Tecnología de la Información velar por que los servidores, equipos de transmisión de datos y los equipos de almacenamiento masivo de información, estén alojados en un espacio con las siguientes características:
   i. Debe ser lo suficientemente amplio para permitir el alojamiento de los equipos y sus respectivos muebles, más el espacio de circulación.
   ii. Debe existir un sistema redundante de aire acondicionado.
   iii. No estar expuestos a la filtración de líquidos.
   iv. Los equipos deben estar sobre un piso falso.
   v. No deben lindar con áreas de acceso público.
   vi. El acceso a esta área debe estar restringido a personal autorizado, y para ello debe contarse con un control de acceso.
   vii. No se debe introducir alimentos, bebidas o sustancias contaminantes.

b) El Data Center deberá permanecer cerrado con llave.

c) El acceso al Data Center es permitido solamente al personal autorizado.

d) Cuando un usuario no autorizado o un visitante requiera la necesidad de ingresar a la sala del Data Center, debe solicitar mediante un comunicado interno debidamente firmado y autorizado por su superior, y para el visitante se debe solicitar la visita con anticipación, y tiene que especificar el tipo de actividad a realizar y siempre será acompañado por el personal de la Unidad de Tecnología de la Información.

e) La Unidad de Tecnología de la Información llevará un registro de todas las actividades realizadas en el Data Center.

f) Toda actividad realizada en los equipos del Data Center por la Unidad de Tecnología de la Información o personal externo a la institución deberá ser registrada de acuerdo a la siguiente forma:
   i. Hora de entrada y salida
   ii. Trabajo realizado

g) Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Data Center, se debe dar aviso con anticipación a los usuarios para evitar daños o pérdidas de datos en los sistemas.

4.13.2 UPS (Unidad Ininterrumpible de Poder).

a) El equipo informático y en especial los equipos del Data Center, salvo las impresoras, deberán permanecer conectados a UPS.

b) Los tomacorrientes conectados a un UPS se encuentran claramente señalados.

c) Los tomacorrientes con servicio de UPS, o los aparatos de UPS en sí mismo, tienen la única finalidad de brindar protección a los equipos contemplados en la (Conexión de Equipos Informáticos a UPS).

d) El usuario no podrá conectar cafeteras, ventiladores o equipo que no sea de cómputo en los tomacorrientes de UPS, esto incluye electrodomésticos, equipos de sonido o televisión, teléfonos y cargadores de cualquier clase.

4.13.3 Aires Acondicionados

a) Se deberá contar con equipos de aires acondicionados adecuados para áreas de Data Center así como para la cantidad de calor que generan todos los componentes de infraestructura que se encuentran en él.

b) Se deberán mantener en buen estado y a la temperatura adecuada que requieran los equipos en el área del Data Center. Esto será determinado por las especificaciones técnicas del fabricante.

c) Se deberán de monitorear de tal forma que recibir alarmas ante aumentos inadecuados de temperatura.

4.14 *Gestión de Riesgos Tecnológicos* (V01)

La gestión de riesgos tecnológicos se hará de acuerdo al Instructivo de Gestión Integral de Riesgos del Instituto de Garantía de Depósitos.

5. Glosario

- **Adjuntos:** Es cualquier archivo que venga junto al correo electrónico y forme parte del mensaje.
- **Antivirus:** Programa especializado en la detección y/o eliminación de virus informáticos.
- **Autenticación:** Proceso de identificación de un individuo, usualmente a través de un código de usuario y una clave. En sistemas de seguridad, la autenticación es

diferente a la autorización, siendo esta última el proceso de otorgar accesos o permisos a objetos del sistema, basados en su identidad. La autenticación básicamente asegura que el individuo que dice ser realmente es, pero no dice nada respecto a los derechos de acceso del individuo.

- **Base de datos de Virus:** Archivo que contiene un listado de los nombres de virus que puede detectar un antivirus. Este archivo es provisto por el fabricante del antivirus y suele proporcionarse a través de Internet.
- **Cadenas de correo electrónico:** Son correos electrónicos iniciados por una persona y que involucran temas de suerte, dinero, aspectos motivacionales, juegos, chistes, venta de artículos, ayuda a gente necesitada. Algunos de estos correos prometen grandes ganancias o buena fortuna si son reenviados a más personas.
- **Chats (Charlas Interactivas):** Comunicaciones en tiempo real entre dos o más usuarios vía computadora. En este tipo de chats o charlas la interacción se da en ambas vías a través de texto, el cual es escrito por uno de los usuarios y visualizado por el otro usuario en su monitor.
- **Componente de Software:** Se refiere a todo programa computacional orientado a desarrollar una función específica. Ejemplo: Sistemas Operativos, programas manejadores de Base de Datos, programas de automatización de oficinas, Sistemas de Información entre otros.
- **Contraseñas (Password):** Claves de acceso, mediante la cual se obtiene el acceso a un recurso o sistema de información.
- **Cuenta de Usuario Administrador:** Son aquellas que tienen los máximos derechos para realizar cualquier cambio sin ningún tipo de restricción tanto en los componentes de hardware como de software.
- **Cuenta de usuario de Servicio a nivel de Sistema Operativo:** Es aquella que no está asociada a un usuario en particular, sino más bien se utiliza para que algunos de los servicios que provea el Sistema Operativo se realicen satisfactoriamente.
- **Data Center (Sala de servidores):** Lugar físico donde se encuentran ubicados los servidores centrales de la Institución, así como todos aquellos componentes de hardware y software necesarios que apoyan su correcto funcionamiento.
- **Directorio (directory):** Grupo de archivos relacionados entre sí que se guardan bajo un nombre.
- **Download (Descarga):** Este término es comúnmente utilizado para describir el proceso de copiar un archivo desde un servicio en línea a la computadora personal, también se puede referir a copiar un archivo desde un servidor de archivos en la red a una computadora dentro de la red.
- **E-mail (Correo electrónico):** El correo electrónico E-mail es una forma de comunicarse por una red o por el Internet. El correo electrónico puede existir en

una red de cualquier tamaño. Después del Web, posiblemente el correo electrónico sea el servicio de mayor uso en el Internet.

- **Encriptación**: Proceso de traducción de datos en código secreto. La encriptación es el método más efectivo para asegurar los datos, para leer un archivo encriptado se debe tener acceso a la llave o clave que permita desencriptarlo (proceso inverso a la encripción), a los datos desencriptados se les llama también texto plano o claro.
- **Escudo de Seguridad o Firewall**: Componente de hardware y software que administra la seguridad de las redes de datos internas con las redes de datos que se conecten externamente.
- **Hacker**: Este término se refiere a aquellas personas que acceden a computadoras sin autorización o exceden el nivel de autorización otorgado a ellos, pueden causar desde pequeños daños considerados travesuras o daños de gran magnitud como por ejemplo exponer públicamente información confidencial, robo de información o alteraciones a la misma.
- **Internet**: Es una red de varios millones de computadoras (y los datos almacenados en ellas) alrededor del mundo conectadas a través de líneas telefónicas, cables o satélites. Estas computadoras y sus datos pueden ser accedidas por otras computadoras que están conectadas a través de un proveedor de servicios de Internet (ISP, por sus siglas en inglés) o a través de la red interna de una compañía conectada a Internet.
- **Máquina**: Se identificará por máquinas a las computadoras personales de escritorio, computadoras portátiles y a los servidores.
- ***Microsoft Teams**: Es una plataforma unificada de comunicación y colaboración que combina chat persistente en el lugar de trabajo, reuniones de video, almacenamiento de archivos e integración de aplicaciones.* **(V01)**
- **On-Line (En línea)**: Procesos o consultas que son realizadas en tiempo real.
- **Políticas de Seguridad Informática**: Son códigos de conducta para la utilización adecuada de los recursos de Tecnología de Información. Definiendo claramente las actividades que no son permitidas, los pasos a seguir para obtener una seguridad informática adecuada, así como los pasos a seguir en caso de presentarse un incidente de seguridad informática; *estableciendo*, además, responsabilidades y derechos.
- **Recurso Tecnológico**: Todo aparato electrónico, infraestructura de comunicaciones, medios de almacenamiento, bienes intangibles y servicios, orientados al procesamiento, almacenamiento, captura, impresión o transmisión.
- **Recursos compartidos**: Se refiere dentro del contexto de este documento, principalmente al compartimiento de estaciones de *trabajo, carpetas* dentro de la

Red, acceso a Internet y Reloj Marcador. No están considerados a nivel de seguridad otros recursos que se comparten. Ej. Impresores, Fax, entre otros.

- **Red de Datos Institucional:** Interconexión de componentes de hardware que permiten compartir recursos e intercambiar datos, entre otros. Lo de Institucional es para referirse específicamente a la Red de la Superintendencia de Valores.
- **Respaldo de Datos (Backup):** Significa hacer copias de archivos almacenados originalmente en discos rígidos. El backup o respaldo es necesario para recuperar archivos perdido o dañados o para recuperar un sistema que ha caído. Los archivos que se almacenan para backup son redundantes y no están hechos como copias sobre las que se está trabajando.
- **Respaldo Total:** En un back-up total, se almacenan en la cinta todos los datos. Debería siempre guardarse en un lugar seguro.
- **Respaldo Incremental:** Se almacenan todos los datos modificados desde el último backup Total o Incremental realizado, (se almacenan sólo los datos modificados desde el último backup). El backup incremental es más veloz, pero la recuperación de datos desde una serie de backups incrementales será más lenta.
- **Respaldo de Base de Datos:** Proceso de copiado de información de una base de datos a un archivo de respaldo, almacenado en un medio alternativo (cinta magnética, CD, disco duro, zip disk, entre otros).
- **Servidor:** Computadora de características superiores a las de una computadora personal, y cuya administración está a cargo del administrador del sistema.
- **Servidor Proxy:** Servidor que centraliza y registra todas las salidas de los usuarios finales hacia Internet.
- **Sistema / Sistemas de Computación / Aplicaciones Automatizadas:** Conjunto de programas (software) y archivos automatizados, orientados a realizar mecánicamente un proceso o tarea.
- **Sistema Operativo:** Conjunto de programas que permiten la administración de los recursos de un determinado componente de hardware. Ej. Windows NT, Windows 95, Unix, Linux, entre otros.
- **Sistemas de Información:** Conjunto de programas desarrollados internamente o por contratación externa, que automatizan uno o varios procesos.
- **Sitio Web (Servidor Web):** Servidor que publica información en Internet a través de páginas web.
- **SPAM (correo no deseado):** Este tipo de correo, conocido como SPAM se caracteriza por ser un correo no solicitado y distribuido a muchas personas a la vez, usualmente está relacionado con propaganda u ofrecimiento de servicios.
- **UPS:** Sistema de alimentación ininterrumpida de corriente eléctrica. Estos sistemas se pueden clasificar en UPS locales (aquellos que se utilizan en forma

individualizada) y UPS centralizados (aquellos que son utilizados por muchos usuarios a través de una red eléctrica especial).

- **User-ID:** Código que sirve para identificar a un usuario dentro de un sistema de información.
- **Usuario:** Toda persona que utiliza los recursos computacionales, servicios y sistemas de información Institucional. Ejemplo: empleados internos, público que consulta la página web, usuarios de instituciones fiscalizadas, entre otros.
- **Vacuna:** Algoritmo especializado en la neutralización de virus informáticos. Estos Algoritmos forman parte del conjunto de "piezas" de un antivirus, y suelen estar disponibles en el sitio Web del fabricante.
- **Virus, Virus Informático:** Programa de computadora diseñado para causar daño a los sistemas computacionales. Estos pueden clasificarse en virus, troyanos y gusanos.
- **VPN:** Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

6. Anexos

A04-INS01-PRO01 Procedimiento para el Uso del Sistemas de Asistencia Técnica.
A04-INS01-PRO02 Procedimiento para el Almacenamiento de Contraseñas.
A04-INS01-PRO03 Procedimiento para el Uso de VPN (Global VPN Client). **(V01)**
A04-INS01-PRO04 Procedimiento para la ejecución de Respaldo y recuperación de la información del IGD. **(V02)**
A04-INS01-PRO05 Procedimiento para regular las comunicaciones de telefonía del IGD **(V03).**
A04-INS01-PRO05-FMT01 Recepción de teléfonos celulares y/o aparatos de oficina móvil **(V03).**

7. Disposiciones Finales

7.1 Resolución de situaciones no reguladas

Cualquier especificación no contemplada en este documento o duda generada a partir de las presentes normas, deberá ser discutida y analizada con la Unidad de Tecnología de la Información.

7.1. Vigencia

El presente Instructivo entrará en vigencia a partir del día once de diciembre de dos mil diecisiete. *Las modificaciones aprobadas en la versión 01 entrarán en vigencia a partir del día uno de enero de dos mil veintiuno. Las modificaciones aprobadas en la versión 02 entrarán en vigencia a partir del día seis de enero de dos mil veintitrés. Las modificaciones aprobadas en la versión 03 entrarán en vigencia a partir del día doce de abril de dos mil veintitrés* (V03).

7.2. Derogatoria

El presente Instructivo deroga las Políticas de Seguridad Informática POL-02-2003-, que entraron en vigencia el 10 de junio del 2003.