POLITICAS DE SEGURIDAD

CONTROLES DE ACCESO

• En caso que INFOTIC considere la modalidad laboral de Teletrabajo, el colaborador debe acceder con las credenciales asignadas a los sistemas de información.
• Las credenciales asignadas para el acceso a los sistemas de información, son de uso personal e intransferible, por tanto, no se comparten o divulgan.
• Salvaguardar la información contenida en los diferentes sistemas de información a los que se tenga acceso autorizado, evitando compartir el equipo de cómputo con personas ajenas.

Controles de servicios en red

• Evitar instalar programas ajenos a los autorizados por INFOTIC o que no correspondan al desarrollo normal de las actividades asignadas. El único proceso autorizado para instalar software en los equipos de cómputo institucionales es el departamento de TIC.
• Evitar abrir y ejecutar ventanas emergentes, barras de herramientas, programas, enlaces desconocidos; estos pueden conducir a sitios de suplantación web para capturar datos que pueden afectar la disponibilidad, integridad y confidencialidad de la información de INFOTIC.

Controles de acceso remoto

Para el establecimiento de la conexión remota se tienen en cuenta los siguientes aspectos:
• Bajo ninguna circunstancia se instalarán herramientas en equipos de propiedad del colaborador.
• Evitar establecer conexiones a redes inalámbricas desconocidas o que estén habilitadas sin seguridad, es decir, que no solicite claves de ingreso. El riesgo aparece cuando el punto de acceso está abierto intencionalmente con un propósito malicioso, para obtener información de forma indebida por parte de una persona no autorizada.
• Cambiar periódicamente las credenciales para el establecimiento de la VPN.
• Dichas solicitudes se registran en la mesa de servicio de INFOTIC.
• Las credenciales asignadas para el establecimiento de la VPN son de uso personal e intransferible, por tanto, no se comparten o divulgan. Su uso inadecuado es responsabilidad exclusiva del funcionario.
Controles de acceso de usuarios a sistemas y aplicativos
• Todos los colaboradores serán responsables por las credenciales (usuario y contraseña) que le sean asignadas y que reciben para el uso y acceso de los recursos.
• Los usuarios no deben proporcionar información de los mecanismos de control de acceso a los sistemas y aplicativos a personal externo, a menos que se tenga visto bueno de su jefe inmediato.
• Todo colaborador que acceda a los sistemas y aplicativos debe contar con un identificador de usuario (ID) único y personalizado.
• Ninguna persona debe compartir sus cuentas de usuario y contraseñas asignados para el ingreso a los servicios de red y los sistemas de información.

GESTIÓN DE ACTIVOS

• Usar el repositorio institucional asignado por INFOTIC para guardar la información, en caso de almacenarla en los discos locales del equipo asignado, se debe utilizar la partición protegida y descargar la información en los repositorios institucionales posteriormente, para prevenir qué ante una situación de hurto del equipo de cómputo, se pierda y exponga la información de la institución.
• La conexión de medios extraíbles al equipo como (USB, Unidades CD/DVD, Discos externos, entre otros, son monitoreadas y eventualmente podrá ser restringida de acuerdo con los lineamientos que INFOTIC disponga para evitar la fuga de información y garantizar la confidencialidad y protección de los datos.
• En los equipos de cómputo no se permite el almacenamiento de archivos de música, videos y cualquier otro formato o información de carácter personal, salvo aquellos cuyo uso o almacenamiento sea para ejecutar labores propias de INFOTIC.
• Los funcionarios de INFOTIC son responsable por los daños ocasionados a los equipos de cómputo generados por mal uso de los mismos, por lo tanto, se tienen en cuenta las siguientes recomendaciones:
• Evitar exponer el equipo de cómputo en sitios públicos como centros comerciales o campos abiertos.
• Hacer uso del equipo de cómputo asignado únicamente en el lugar de teletrabajo aprobado por INFOTIC.
• Evitar exponer el equipo de cómputo en zonas donde exista humedad.
• Evitar golpes y consumir líquidos mientras se desarrollan actividades propias del cargo ya que existe el riesgo de avería parcial o total del equipo de cómputo.
• Evitar utilizar o dejar el equipo de cómputo donde pueda sufrir calentamiento, esto generaría daño en la fuente y a nivel general.
• No está autorizado ningún tipo de modificación en el hardware.
• Las personas en el momento de desvinculación o cambio de labores, deben realizar la entrega de su puesto al jefe inmediato o a quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

SEGURIDAD DE LAS COMUNICACIONES

Mensajería Electrónica

• Los colaboradores de INFOTIC deben conocer que la cuenta de correo electrónico asignada es de carácter individual; y no se debe utilizar una cuenta de correo que no sea la propia, a menos que se autorice la administración de varias cuentas.
• Los colaboradores deben utilizar el correo electrónico para envío de mensajes e información relacionada con el desarrollo de las labores y funciones asignadas a cada usuario.
• Las cuentas de usuario de correo son generadas bajo el estándar estipulado en la creación de cuentas de INFOTIC, en caso de que un usuario deba realizar un cambio de cargo se conserva la misma cuenta de correo, se parte del principio que el correo es un medio de comunicación mas no de almacenamiento de información.
• Cada cuenta de correo electrónico tiene asociado un conjunto de recursos de almacenamiento que es limitado de conformidad con lo establecido con google.
• El servicio de correo administrativo permite la transferencia de archivos como adjuntos del mensaje o compartidos a través de sus herramientas.
• Las imágenes enviadas en el cuerpo del mensaje electrónico no son mayores a 10 Megabytes, un mayor peso de la imagen genera lentitud en la distribución y saturación del correo.

Uso del Internet

El área de Sistemas debe:

• Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos.
• Monitorear continuamente el canal o canales del servicio de internet, en cuanto a carga y tráfico.
• Establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.
• Los colaboradores deben hacer uso del servicio de internet que provee INFOTIC para las actividades que guarden relación con su labor.

Línea Telefónica

• Evitar el intercambio de información en la comunicación telefónica con personas ajenas a INFOTIC, puesto que esta herramienta facilita la aplicación de técnicas de ingeniería social para obtener información sensible de la Organización.

Elaboró:	Revisó:	Aprobó:
Michael Avila Soporte Técnico	Leonardo Henao Vicepresidencia de Operaciones	Leonardo Henao Vicepresidencia de Operaciones