El MAPRE cumpliendo con los estándares internacionales adoptados y con su interés a asegurar el buen manejo de la información generada, proporciona a sus proveedores y/o contratistas los lineamientos definidos sobre la seguridad de la información definidos de manera institucional. Dichos lineamientos son:

- Los proveedores y/o contratistas deben proteger la confidencialidad, integridad y disponibilidad de la información propiedad del MAPRE así como la de sus partes interesadas cuando los servicios contratados así lo requieran, según la política de seguridad de la información del ministerio: **"El Ministerio se compromete a mantener la confidencialidad, integridad y disponibilidad de la información propia y de nuestras partes interesadas en apego al marco legal, regulatorio y contractual aplicable, manteniendo una mejora continua."**
- Las visitas, proveedores y/o contratistas al momento de su llegada deben dirigirse a DRVPN y confirmar su visita notificando el servicio a proveer y la información solicitada por la misma, la DRVPN debe confirmar con la persona del área que solicitó el servicio del proveedor antes de dar acceso al MAPRE. Si es validada le será otorgado un carnet con acceso o etiqueta adhesiva, según el tipo de actividad a realizar en Casa de Gobierno. Será escoltado por el personal de seguridad interna accediendo por módulo de entrada hasta el área donde se encuentra el colaborador que lo recibirá. Luego de culminar el trabajo o servicio brindado por el proveedor deberá retirar o entregar el pase en el módulo de salida.
- La Dirección de TIC será la responsable de entregar a los proveedores de TIC que requieran tener acceso a las instalaciones y activos de información un acuerdo de confidencialidad y un extracto de las políticas aplicables de seguridad de la información y gestionar la firma de los mismos con el objetivo de mantener un apropiado nivel de seguridad de información.
- Los proveedores y/o contratistas no debe tener acceso a las áreas de procesamiento de información como: el CPD, MDF, IDF ni a las áreas de plantas eléctricas, suministro y demás, sin la compañía del personal interno que forma parte de alguna de las áreas mencionadas.
- El contratista no puede mover o tomar ningún activo sin la presencia del personal o el consentimiento del mismo.
- El acceso al CPD a proveedores y/o contratistas que realicen algún tipo de mantenimiento o reparaciones, será responsabilidad del encargado a cargo del CPD, quien deberá enviar días previos a la visita al DRVPN, las siguientes informaciones: (nombres y núm. de documentos de identidad y electoral de los contratistas, compañía que representan y/o trabajos a realizar). Estos datos deberán ser validados por el DRVPN, según proceso correspondiente.
- La entrada y salida de personal del CPD deberá ser registrada en el ***Control de Ingreso al Datacenter.***
- El personal interno que acompañe a los proveedores y/o contratistas al CPD, MDF e IDF debe comunicarles de forma verbal las siguientes restricciones a las que deben abstenerse al estar en estas áreas:
    - No tomar fotos ni grabaciones.
    - Abstenerse a trabajar solo con los equipos autorizados por la Dirección de TIC.
    - Solo en caso de emergencia se debe activar la alarma del CPD.

  - No hacer ruido sin previa autorización de Seguridad Interna.
  - No alimentos en estas áreas.
  - Prohibido fumar y sustancias inflamables.
  - Las actividades que puedan provocar un corte de servicios deben ser autorizados por la Dirección de TIC.
- Las conexiones remotas proporcionadas a los proveedores, empleadas para realizar el teletrabajo en los sistemas de información del MAPRE deben ser hecha a través de una conexión VPN (Red Privada Virtual) segura, suministrada por la DSYM y aprobada por el director de Tecnología.
- Para solicitar el acceso a la red VPN debe realizarse a través del formulario ***Solicitud de Acceso a la Red VPN***. Los usuarios y/o proveedores previamente autorizados serán los responsables del correcto uso del sistema.
- Si el solicitante usará un equipo personal (no provisto por la institución) para acceder a la VPN, este debe ser evaluado por la DSYM.
- Es de responsabilidad del proveedor 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.
- Los usuarios y/o proveedores deberán comprender que los equipos conectados a una VPN son una extensión de las redes del Ministerio, y como tales están sujetos a las mismas normas y reglamentos que se aplican a los equipos computacionales del Ministerio.
- Los encargados o superiores informarán a la DASTIC a través de la Mesa de Ayuda vía correo electrónico: **mesadeayuda@presidencia.gob.do** de la asignación o cancelación de derechos de accesos básicos /privilegiados de empleados, contratistas, etc.
- Cuando expertos externos necesiten intervenir la biblioteca de los códigos fuentes, estarán acompañados por el Encargado de DDIS o una persona designa por él.
- La DDIS debe supervisar y monitorear la actividad de desarrollo de sistemas (Verificación del código) cuando este se lleve a cabo por terceros.
- Está prohibido el uso e instalación de software no autorizado en los equipos pertenecientes al MAPRE.
- Para entrega de equipos tecnológicos por suplidores, la recepción será llevada a cabo por la DAS en el área de entrega y carga (***según procedimiento el Área de Entrega y Carga***) y un representante de la Dirección de TIC para verificar que cumple con lo solicitado.
- La Dirección de TIC junto a sus divisiones deben verificar la implementación y monitorear el cumplimiento de los contratos de prestación de servicios celebrados con terceros (proveedores TIC), así como dar seguimiento a los cambios a dichos contratos a fin de garantizar que los servicios entregados reúnen todos los requerimientos (seguridad de información, calidad, niveles de servicio, etc.), acordados en el contrato.
- Cuando los proveedores de TIC realicen un servicio relacionado con los activos de información o recursos tecnológicos del MAPRE, un empleado de la división donde corresponde el servicio

FCA

deberá ser responsable del mismo, validando el trabajo realizado durante todo el proceso y asistiendo al proveedor.

- Los proveedores deben de regirse por las responsabilidades estipuladas en los contratos, para tratar los riesgos de seguridad de la información asociados con los servicios de tecnologías de la información y comunicaciones y los productos de la cadena de suministro contratados con los mismos.
- Todos los cambios a la provisión del servicio estipulada en el contrato celebrado, incluyendo el mantenimiento o mejora de las políticas de seguridad existentes, procedimientos y controles, deben ser administrados adecuadamente, tomando en cuenta la criticidad de los sistemas y procesos dentro del alcance del SGSI, que se vean involucrados en dicho cambio y evaluar el riesgo que implica realizar el cambio.

Validado por:		Aprobado por:	Versión	Página
Edgar Santos R.	Elaine Cruz		01	Página 3 de 3
Involucrados en el Proceso		Director de TIC		

*Los espacios en blanco serán cerrados con N/A.