Lineamiento de acceso a Centros De Datos GIM

La seguridad del Centro de Datos GIM representa la seguridad de la información, la cual es vital para la consecución de los objetivos organizacionales, continuidad del negocio y sus empresas contenidas.

El objetivo es implementar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del Centro de Datos GIM y es aplicable a todo el personal cuyas funciones laborales están orientadas a la administración y mantenimiento del mismo.

1. **Control de acceso al Centro de Datos.**

   a. **Personal autorizado**. Las siguientes personas están autorizadas a ingresar al Centro de Datos GIM, ya sea de manera física o remota:
   - Administrador de Base de Datos y/o Administrador de Sistemas.
   - Administrador o encargado de infraestructura, redes, comunicaciones y seguridad.
   - Coordinador TI. Monitoreo rutinario del Centro de Datos.
   - Gerente de TSI.
   - En caso de que las personas citadas no estén presentes (vacaciones, permisos, licencias) entonces la Gerencia y/o Coordinación autorizará TSI y/o habilitará de forma escrita el ingreso al data center de personal técnico alterno, hasta el retorno de los titulares.

   b. Acceso físico. Determinado sólo en los siguientes casos:
   - Actualizaciones a nivel de hardware.
   - Actualizaciones a nivel de software en caso de ser necesario.
   - Verificación del buen estado de funcionamiento de cada uno de los subsistemas (equipos) que integran el Centro de Datos GIM.
   - Revisión de bitácoras o logs de dispositivos que no pueden ser accedidos de manera remota.
   - Mantenimiento de la infraestructura de redes y comunicaciones.
   - Copias de respaldo del equipamiento de redes y comunicaciones y otros a los que no se puede acceder remotamente.

   c. Acceso remoto. Determinado para todos los casos en los que es posible establecer conexión remota con algún dispositivo del Centro de Datos GIM.

   d. Identificación y autenticación
   - Identificación. El usuario se dará a conocer ya sea para acceso físico o remoto. En el físico deberá tener la llave de acceso y/o teclear la contraseña de acceso que se le proporciono en el control de automático de acceso.

   e. Acceso de terceras personas. El grupo de terceras personas estará conformado por:
   - Técnicos especializados en servidores de alto rendimiento.
   - Técnicos especializados en redes, comunicaciones y seguridad.
   - Técnicos especializados en el sistema eléctrico.
   - Técnicos especializados en administración y mantenimiento de Centros de Datos.

- En todos los casos anteriores la Dirección de TSI, ó la Coordinación de TI autorizarán mediante plan de trabajo el acceso de técnicos foráneos especialistas al Centro de Datos GIM de la organización.

- Todo acceso de terceras personas deberá ser supervisado (acompañado) por personal técnico de TI de la organización.

- Bajo ninguna circunstancia, las terceras personas, podrán ingresar al data center portando dispositivos de almacenamiento masivo de información (discos duros externos o similares), cámaras fotográficas, videograbadoras.

- Bajo ninguna circunstancia las terceras personas podrán conectar a la red eléctrica equipos electrónicos foráneos en el Centro de Datos GIM, sin la autorización y supervisión de personal técnico de la organización (TI).

2. Registro de las actividades y acciones del personal en el Centro de Datos GIM

a. Bitácoras de acceso y/o sesiones en los sistemas operativos. Todos los servicios de registro de bitácoras de los servidores deben ser habilitados y configurados correctamente para registrar todas las actividades del personal autorizado, siempre y cuando la herramienta utilizada lo contenga y/o pueda ser utilizado para éste propósito.

b. Toda persona con acceso al Centro de Datos GIM deberá previamente llenar la Bitácora de ingreso, anotando en la misma las actividades a realizar y registrando el tiempo efectivo que permaneció en el Centro de Datos.

3.- Guías de Conducta en el Interior del Centro de Datos.

- No pueden hacer mal uso o abusar de la propiedad y equipos de la empresa.
- No podrán acosar físicamente, amenazar, intimidar o abusar a ninguna persona dentro del Centro de Datos GIM, incluyendo pero sin limitarse a empleados, agentes o invitados de la empresa, así como otros visitantes.
- Los abusos, las amenazas y todo tipo de comportamiento ofensivo por parte de los clientes, no será tolerado.
- La empresa puede negar la entrada o requerir la inmediata salida de cualquier persona que sea desordenada, no cumpla la presente política, deje de cumplir cualquier otra política de la empresa, así como sus procedimientos y requerimientos, una vez le sean informados.

Por favor leer y seguir los siguientes lineamientos, para que podamos mantener el Centro de Datos GIM como una unidad de primera clase.