PLAN DE ACCESO REMOTO SEGURO

ÁREA METROPOLITANA DE BUCARAMANGA

AÑO 2020

ELABORADO POR: Área de apoyo tecnológico y de información, Gestión Corporativa

Contenido

Introducción

El presente proporciona al Área Metropolitana de Bucaramanga una serie de soluciones que permiten implementar, de forma ágil, acceso remoto a los recursos de una Organización minimizando el impacto en los recursos IT y optimizando el tiempo para su puesta en producción. El proceso, tipología y componentes utilizados en un despliegue específico de una organización dependerá de una serie de factores, entre los que se incluyen:

- Perfil de riesgo de la organización.
- Aspectos financieros.
- Legislación aplicable.
- Capacidad técnica de la organización.
- Arquitectura admitida por las capacidades técnicas de la organización.
- Modelos de propiedad permitidos

Cada dependencia del AMB es responsable de conocer y evaluar los factores que le son de aplicación previamente al diseño o replanteo del sistema, la reserva de recursos y la selección de componentes a incluir. La dependencia de TI que realiza el despliegue debe realizar un análisis del nivel de seguridad requerido para la información que se va a manejar en los puestos de trabajo remotos o móviles

Soluciones técnicas

La implementación de una solución de acceso remoto es un reto desde el punto de vista de la seguridad y la gestión para el Área Metropolitana de Bucaramanga. Las soluciones clásicas basadas en el despliegue de sistemas locales u on-premise requieren de capacidades, tanto de personal como de infraestructura, que no siempre están disponibles, Por otro lado, se adaptaran los sistemas de información actuales de la entidad para implementar un sistema de acceso remoto seguro que pueda desplegar los servicios que le sean necesarios. A continuación, se presentan dos (2) soluciones para la implementación de un sistema de acceso remoto seguro en función de las capacidades de la organización.

Sistema de información y Comunicación del AMB.

1. BPM INTEGRASOTF
2. SIIGO
3. PRESUPUESTO
4. BSCG CATASTRO
5. PÁGINA INSTITUCIONAL
6. SOFTWARE DE VALORIZACIÓN
7. APLICATIVOS WEB

Servicios disponibles para facilitar la comunicación en el AMB.

- Soporte Remoto Bajo ANS
- Conexiones Remotas (Anydesk, Teamviewer, Escritorio remoto de Windows)
- Líneas telefónicas fijas y celulares (Corporativas y personales)
- Aplicaciones de comunicación móvil (WhatsApp, Telegram)
- Servidores de carpeta en (BPM modulo Documentos)
- Cuentas corporativas y personales Gmail.
  (Acceso a carpetas compartidas en la Nube Drive)
  (Chat para reuniones y video Conferencias, Hangouts)
  (Comunicación de información)
  (Elaboración de formularios)
- Skype
- Dropbox
- We transfer

Dependencias u áreas de trabajo del AMB

1. Talento Humano: (Dirección, Secretaria General, Comunicaciones, Gestión Corporativa, , Archivo)
2. Control Interno
3. Contratación
4. Subdirección administrativa y financiera (Valorización)
5. Subdirección de Planeación e Infraestructura (Catastro)
6. Subdirección de Transporte
7. Subdirección Ambiental
8. Jurídica

Recomendaciones del uso de Los servicios

Correos electrónicos

Si se plantea un escenario en el que los funcionarios y contratistas del AMB, puedan acceder al sistema de correo electrónico corporativo desde equipos informáticos no gestionados por la organización a través de Internet, se recomienda reforzar la inspección de los correos electrónicos y gestionar toda la información de la entidad de una forma correcta. En este caso, pueden aumentarse las probabilidades de ser víctimas de ataques al poder tener implementadas medidas menos seguras en los ordenadores remotos y que en la organización se detectarían y tratarían al tener controlado el perímetro de seguridad, aspecto que en los equipos remotos no se puede garantizar. Es importante controlar los motores de antivirus e inspección de los buzones de correo electrónico hacia atrás en el tiempo de las personas que tengan tanto acceso remoto como acceso al correo electrónico corporativo. No se debería utilizar datos sensibles de la organización o información que legalmente deba ser protegida en equipos que no pertenezcan a la organización. Si los miembros de una organización deben enviarse correos internos, pero ya no se puede utilizar la red interna es conveniente usar mecanismos de cifra, como PGP (Pretty Good Privacy), para el cifrado de los correos y así mantener la confidencialidad y no repudio.

Para más información leer políticas de TIC del AMB: https://www.amb.gov.co/planes-institucionales-2020/

Salas de reuniones virtuales

Si se plantea un escenario en el que los usuarios puedan acceder a salas de reuniones/conferencias de forma virtual o telemática desde equipos informáticos no gestionados por la entidad a través de Internet, se debería revisar la seguridad o haberse aplicado los parches de seguridad correspondientes. Además, se debe tener un listado de servicios acordados para mantener reuniones de forma virtual, conocer las licencias de las que se disponen o si se van a utilizar herramientas gratuitas. En todos los casos conviene tener controlados los accesos a la red y sistemas del organismo, además de tener la posibilidad en los dispositivos perimetrales de habilitar reglas con fecha y hora de inicio y finalización. Cuando se inicien reuniones por medio de estos canales, se debe revisar que los asistentes son los invitados y no se tienen duplicados, personas no invitadas o desconocidas en la reunión. Se debe revisar si la reunión es grabada, que quede registro de las personas conectadas, donde se almacena y que personas pueden grabar la reunión dentro de la misma

Para más información leer políticas de TIC del AMB: https://www.amb.gov.co/planes-institucionales-2020/

Recomendaciones Genéricas

En el presente apartado se enumeran una serie de medidas genéricas de protección, algunas de las cuales serán desarrolladas en los anexos del presente documento.

• Tener instaladas las últimas actualizaciones del sistema operativo.
• Tener activados servicios de monitorización con alertas definidas.
• Revisar los registros y auditorías de las conexiones remotas.
• Tener habilitados canales de comunicación para reuniones mediante Internet.
• Restringir montar unidades mapeadas del organismo en equipos remotos inseguros.
• Evitar las opciones de "Split-Tunneling" en equipos inseguros o que no cumplan todas las medidas de seguridad.
• Revisar o tener más vigilados unidades para intercambiar información.
• Asegurar si los antivirus escanean los dispositivos USB conectados a los equipos remotos o si se bloquea el acceso de USB en dichos equipos.
• Tener listados telefónicos de fácil acceso para comunicarse con las diferentes personas.
•Tener listados de personas, direcciones IP, teléfonos, correos electrónicos corporativos y alternativos relacionados con el acceso a los sistemas de forma remota.
• Tener actualizado el listado de personas que pueden acceder remotamente a los equipos de la organización con la dirección IP de acceso y medio de conexión.

Procedimientos de actuación de las personas o equipos con acceso remoto

Se recomienda disponer, de forma diaria, los portátiles o equipos para acceder remotamente a los organismos por si se activa algún protocolo de actividad extraordinaria fuera de la oficina.

En estas situaciones conviene realizar pruebas de conectividad de los diferentes usuarios que pudieran utilizar el acceso remoto comprobando su funcionalidad y registrando las direcciones IP de acceso remoto, credenciales y accesos disponibles mediante la conexión remota. Si para tener acceso remoto se debe dejar el equipo del organismo encendido, asegurarse de las siguientes medidas:

• Tener actualizado el puesto de trabajo con los últimos parches de seguridad (Sistema operativo, herramientas de seguridad, aplicaciones, etc.).

• Cerrar todas las conexiones que no sean estrictamente necesarias.

• Cerrar todas las aplicaciones cuando no se estén utilizando.

• Realizar análisis programado de los antivirus (exhaustivos) a los puestos de trabajo, aunque los ordenadores no se reinicien.

• Aplicar las actualizaciones programadas en la Organización, para ello puede ser necesario apagar y encender los equipos de forma periódica.

• Prever mecanismos que permitan el reinicio de estas máquinas de forma remota y acceder por canales establecidos a las mismas desde fuera de la organización una vez se reiniciara el equipo. Se recomienda tener un listado de las direcciones IP de los posibles orígenes remotos de las conexiones.

Vulnerabilidades conocidas

A la hora de redactar el presente documento, Microsoft ha publicado un aviso de vulnerabilidad en el protocolo SAMBA, en su versión 3. En este sentido, se ha dado a conocer un posible escaneo con NMAP: https://gist.github.com/nikallass/40f3215e6294e94cde78ca60dbe07394

En estos casos, se recomiendan las siguientes acciones:

• Conocer, al menos, que equipos pueden estar afectados por la vulnerabilidad para conocer sobre que equipos se deben aplicar futuras medidas de mitigación o contención.

• La actualización de sistemas operativos y elementos que proporcionen acceso remoto para prevenir posibles incidentes de seguridad.

Proceso de Comunicación y trabajo Remoto

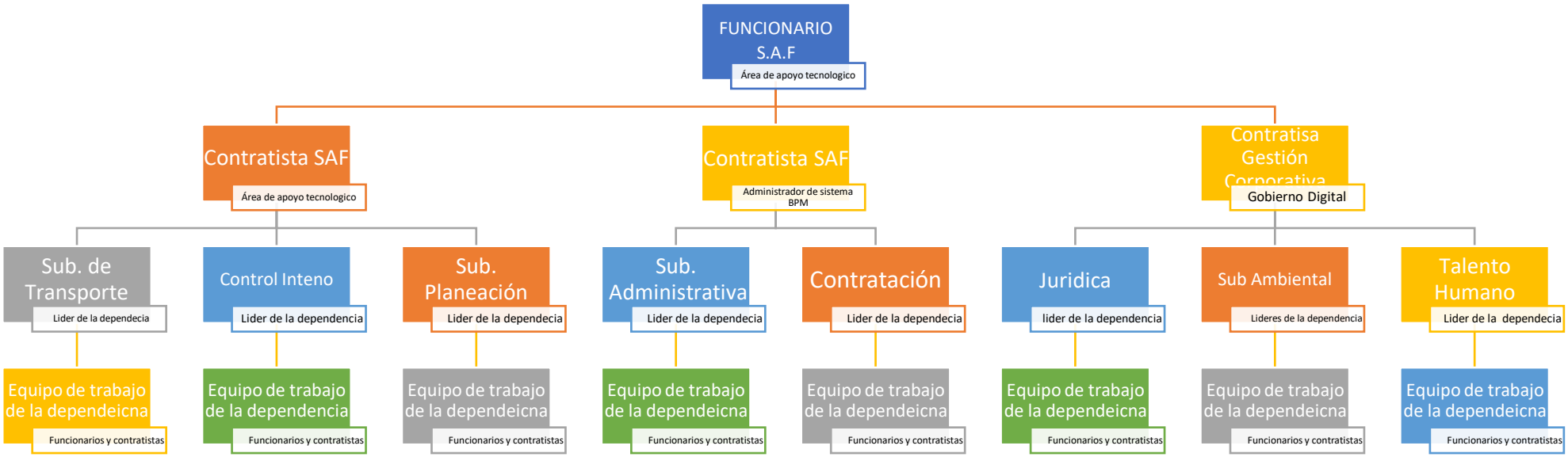
Con base a un plan de contingencia de prevención y salud bajo y el decreto de emergencia sanitaria Nacional, La entidad opta por implementar y ejecutar trabajos de forma remota que implican a "funcionarios y contratistas" del AMB; aplicando el modelo de trabajo en casa con el fin de evitar desplazamientos dentro de la ciudad y permanecer en sitios seguros.

Por directriz de la dirección institucional del AMB se ha delegado a un grupo de funcionarios y contratistas facilitadores con conocimientos en el área de TI y servicio al cliente capaces de comunicarse con los líderes por dependencia quienes son los encargados de comunicar a sus equipos de trabajo las actividades a ejecutar diariamente, para esto la entidad ha definido 5 pilares del trabajo remoto seguro para proteger la información las cuales son:

1. **Gestión de Roles y funciones dentro del AMB** (funcionario y contratista): La información solo debe ser accesible para los perfiles de usuario que realmente necesitan visualizarla y modificarla. Para el resto, debería estar **restringida**.
2. **Control de dispositivos**: Teniendo en cuenta la amplia variedad de dispositivos en el mercado, es importante restringir el acceso solamente a aquellos en los cuales se aplican las herramientas de seguridad adecuadas.
3. **Protección Contra códigos Maliciosos**: Para garantizar que los datos no sean afectados por códigos maliciosos, todos los dispositivos utilizados por el empleado deben contar con soluciones de seguridad que detecten proactivamente este tipo de amenazas.
4. **Monitoreo de tráfico de la Red**: Dado que hay dispositivos que están ingresando a la red por fuera del perímetro físico de la oficina, es necesario hacer un seguimiento de qué tipo de tráfico generan. Por ejemplo, a dónde tratan de acceder, si hay intentos recurrentes y fallidos de ingreso a servidores o si generan algún tipo de **tráfico inapropiado**, como la descarga de archivos desconocidos.
5. **Concientización de los funcionarios y contratistas del AMB:** La educación debe ser un pilar importante para que todos los usuarios sean **conscientes de los riesgos** a los cuales pueden verse expuestos y cuáles son los cuidados que deben tener al ingresar dispositivos ajenos a la compañía.

El personal encargado de ti y servicio al cliente, tiene como función mantener la disponibilidad, confiabilidad e integridad de los sistemas de información del área metropolitana, y hará uso de herramientas de telecomunicaciones ya mencionadas para coordinar y ejecutar sus actividades dentro de este plan de contingencia.

En la siguiente grafica "Mapa1" se define el proceso de comunicación y trabajo remoto del AMB.



Mapa. 1 Organigrama de Trabajo Remoto

Ámbito

Toda conexión de acceso remota:

- Colaboradores (funcionarios y Contratistas) conectado en forma externa.
- Proveedores conectados en forma externa.
- Clientes conectados vía canales de comunicación específicos

Roles y Responsabilidades

- Subdirección Financiera (funcionarios y contratistas área de apoyo tecnológico de la información, Contratista apoyo Herramientas y aplicativos del sistema)
- Gestión Corporativa (contratistas Gobierno digital y transparencia)
- Líderes de cada Dependencia