**CONTENIDO:**



## 1. CONTROL DE FIRMAS:

| **Emitido Por:** | **Revisado Por:** | **Aprobado Por:** |
|---|---|---|
| Analista SST-SGC | Administrador de Infraestructura | Gerente General |
| **Fecha: DD-MM-AA** | **Fecha: DD-MM-AA** | **Fecha: DD-MM-AA** |
| 28-03-23 | 28-03-23 | 28-03-23 |
| **Firma:** | **Firma:** | **Firma:** |
| | | |

## 2. OBJETIVO:

- Identificar, medir, analizar y gestionar los riesgos asociados a la ciberseguridad, seguridad informática y seguridad de la información de MICROHOME y sus proyectos.

## 3. ALCANCE:

Esta política aplica a todos los activos de información, a todos los procesos de MICROHOME y también a sus partes interesadas internas y externas en el cumplimiento de los objetivos de la compañía, siendo un mecanismo de protección, prevención y control para los recursos de Tecnología e Informática de la compañía.

Esta Política abarca toda la información independientemente de la forma en la que se procese, quién acceda a ella, el medio que la contenga o el lugar en el que se encuentre, ya se trate de información impresa o almacenada electrónicamente

## 4. RESPONSABILIDADES:

- Es responsabilidad del Líder de infraestructura autorizado por la Directora de Servicios, informar la correcta aplicación de este procedimiento, así como de mantenerlo actualizado y verificar que se cumplan los requerimientos establecidos en el mismo informando a la directora de servicios cualquier novedad.

- Es responsabilidad del Analista SST-SGC verificar que el presente documento se ajuste a los requerimientos de la norma ISO 9001:2015 y que se encuentre identificado dentro del sistema de gestión de la calidad de MICROHOME S.A.S.

- Es responsabilidad de la Directora de servicios, cumplir y hacer cumplir los parámetros establecidos en el presente documento.

- Es responsabilidad de los colaboradores velar por la seguridad de los activos bajo su responsabilidad mediante las medidas que sean necesarias

- La Gerencia General, la Gerencia Administrativa y la Gerencia Comercial y Mercadeo son quienes aprueban esta política y son responsables de la autorización de sus modificaciones.

## 5. DEFINICIONES:

**Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, infraestructura, personas...) que tenga valor para la compañía.

**Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema de información o la Entidad

**Backup:** Una copia de seguridad, respaldo, copia de respaldo o copia de reserva en ciencias de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida.

**Ciberseguridad:** Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos

**Firewall (Muro de Fuego - Cortafuego):** Herramienta de seguridad que controla el tráfico de entrada/salida de una red

**Incidente de Seguridad:** Evento único o serie de eventos de seguridad de la información inesperados o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Ingenieria social:** conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales infecten sus computadoras con malware o abran enlaces a sitios infectados

**Seguridad de la información:** conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos

**Seguridad informática**: Disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático.

**Vulnerabilidad:** Debilidad de un activo o control que pone en riesgo la seguridad de la información y/o sus activos asociados, y que puede ser explotada por una o más amenazas.

## 6. DIAGRAMA DE FLUJO

**N/A**

## 7. GENERALIDADES

Para Microhome es fundamental acatar las recomendaciones de las mejores prácticas de Seguridad de la Información instauradas en el Estándar ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información puedan aplicar a nuestros procesos

### 7.1 IDENTIFICACIÓN Y CONTROL DE RIESGOS

Microhome cuenta con una matriz de identificación de riesgos (GC-MTZ-004) enfocada a seguridad de la información, donde se busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos, facilitando la toma de decisiones a todos los responsables.

### 7.2 COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de la compañía se compromete a garantizar que se establezca la política de seguridad de la información y sea compatible con la dirección estratégica de la organización.
Promoverá la organización las funciones y responsabilidades en el ámbito de seguridad de la información.

Facilitará los recursos adecuados para alcanzar los objetivos de seguridad de la información.
Impulsará la divulgación y la concientización de la Política de Seguridad de la Información entre los empleados.

Exigirá el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.

Considerará los riesgos de seguridad de la información en la toma de decisiones y promoverá la mejora continua.

### 7.3 SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Microhome debe asegurar que su personal recibe un nivel de formación y concientización adecuado en materia de Seguridad de la Información, especialmente en materia de confidencialidad y prevención de fugas de información. Así mismo, los empleados deberán ser informados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes, de manera que pueda garantizarse el cumplimiento de esta Política.
Por otro lado, los empleados tienen la obligación de obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de empleados o terceros no autorizados.

Se deberán tener en cuenta, al menos, los siguientes aspectos:

- Proceso para el manejo de dispositivos de alta criticidad conocidos
- Uso adecuado de dispositivos extraíbles
- Uso del correo electrónico
- Transmisión de información de forma oral
- Impresión de documentación
- Salida de documentación
- Uso de dispositivos móviles
- Uso de Internet
- Equipos desatendidos

### 7.4 DOCUMENTACIÓN SERVICIOS ADMINISTRADOS MICROHOME S.A.S.

**a) Correo.**

- La compañía cuenta con 99 cuentas de correo, 75 con capacidad de almacenamiento de 100 GB, 24 con capacidad de 50 GB de almacenamiento por cuenta en la nube y configuración por IMAP en cada uno de los equipos de usuario con almacenamiento local en archivo PST y copia de los correos que ingresan a la nube.
  Estos servicios se encuentran contratados con MICROSOFT 365 y se administran con una cuenta de correo electrónico asignada por el proveedor, bajo el control del administrador de infraestructura.

**b) Servicio de Internet.**

- Servicio de internet contratado de 300 MB por fibra. Cuenta con un pool de direcciones IP's públicas, NAT configuradas en el firewall para estas direcciones.
- El Backup de conexión a internet se encuentra contratado con un proveedor diferente al del canal principal y cuenta con una capacidad 100 Megas por cobre.

**c) Servicio de telefonía.**

- Se contrata servicio de telefonía con los servicios de IP Trunking de ETB con 5 canales, No de arranque 3074010 /14 configurados en la planta telefónica. (SIP TRUNK)

**d) Página Web.**

La página web es www.microhome.com.co esta se encuentra contratada con Wordpress, el diseñador gráfico es el administrador de la página Web quien tiene los datos de acceso a este portal, la actualización y contenido de esta es administrado por el área de mercadeo quien realiza estudios y estadísticas de visitas y demás características del sitio.

El dominio utilizado para el envío de correos masivos promocionales es @novedadesmicrohome.com.co

**e) Servicio Puerta de enlace.**

- Se cuenta con un dispositivo firewall, actualmente se utiliza como enrutador.

**f) SWITCH.**

- La infraestructura de red de MICROHOME cuenta con 5 Switch de 24 puntos cada uno los cuales cuentan con configuración de ClearPass la cual hace conexión con el Directorio Activo, los puertos de los switches se habilitan por autenticación con el Directorio Activo.

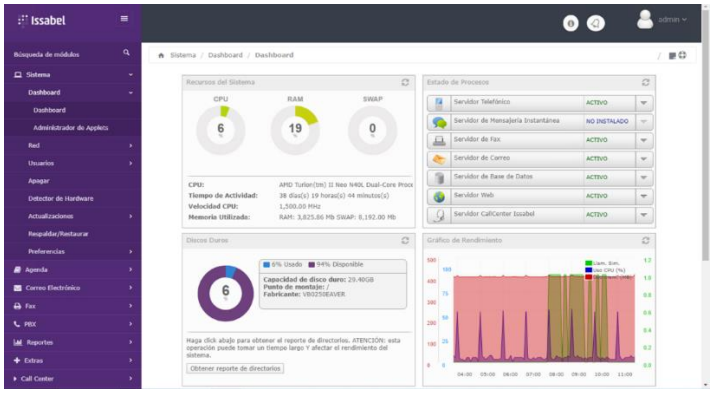
**g) SERVIDORES.**

- **SERVIDOR 1**
  Servidor de Dominio, DHCP, DNS

- **SERVIDOR 2**
  Servidor de virtualización en el cual se encuentran las máquinas virtuales de los servidores con las aplicaciones de Clear Pass, Worldoffice, Aranda, EMA, Adconnect e Impresión

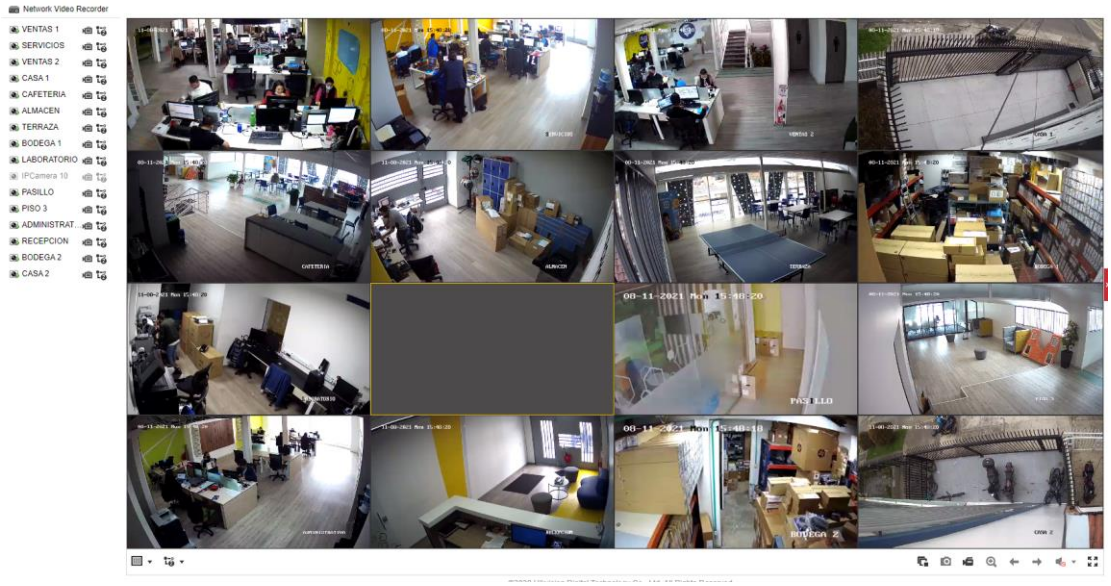
- **SERVIDOR 3**
  Servidor virtualizado en el servidor de virtualización en HYPERV, corresponde al aplicativo Aranda, cuenta con acceso remoto con direccionamiento público para fuera de la oficina y una IP privada para la oficina

- **SERVIDOR 4**
  Planta telefónica con sistema operativo Issabel, entrada 5 Troncales SIP manejo de PBX




- **Servidor 5**
  Servidor virtualizado en HYPERV Servidor de aplicación contable WORLD OFFICE acceso remoto

- **NVR Cámaras:** NVR de cámaras con acceso local y remoto;




- **Servidor de impresión:** Servidor virtualizado en HYPERV con consola HP Access Control, Conectado con directorio activo para registrar colas de impresión a través del directorio activo

- **Clearpass:** Servidor virtualizado en **HYPER-VP** con la consola de acceso web para administración de ingreso de usuarios a la red


- **Servidor Documentos:** Servidor de almacenamiento de data.
- **EMA:** Servidor para control de equipos y acceso remoto por soporte, acceso remoto con acceso web: https://ema.novedadesmicrohome.com.co/#/

- **AZURE AD-CONNECT:** Servidor de conexión entre el AD y el tenant de office 365

**h) EQUIPOS.**

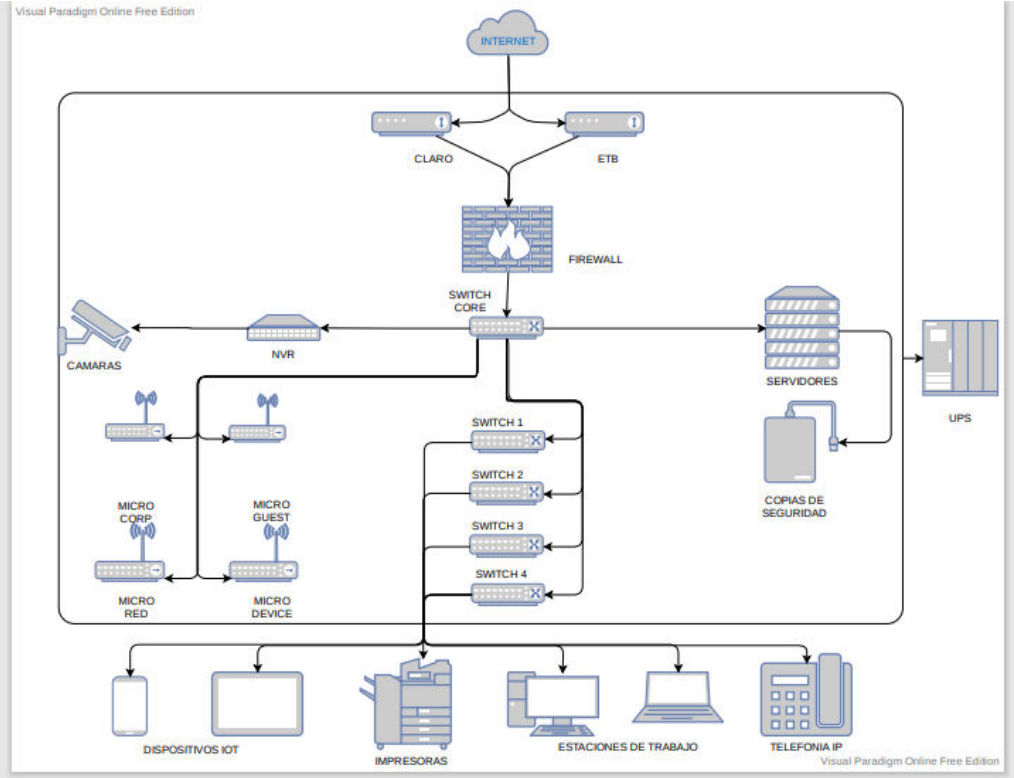
- Se cuenta con equipos configurados con Windows 10 Profesional, vinculados al dominio, con su un nombre predeterminado de acuerdo con el departamento asignado según corresponda, estos están direccionados por DHCP y configurados con software de acuerdo con al área de trabajo.

**i) RED WIFI.**

- Contamos con red WiFi dentro del dominio llamada: MICROCORP, MICROGUEST, MICRORED Y MICRO_DEVICE ubicadas en el segundo piso.

**j) TOPOLOGIA DE LA RED**

- La red LAN de Microhome se encuentra distribuida de la siguiente forma: Firewall con conexión al Switch principal y de allí se despliega una cascada a los 4 switches de borde, del Switch core se realiza la conexión a los servidores y los demás puertos son de conectividad para los AP Microcorp y Microguest.




## 8. GESTIÓN DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN

Se deberán realizar copias de seguridad de la información, del software y del sistema y se deberán verificar periódicamente. Para ello, se deberán realizar copias de seguridad de aplicaciones, ficheros y bases de datos con una periodicidad definida en el numeral 8.1 del presente documento.

Las copias de seguridad deberán recibir las mismas protecciones de seguridad que los datos originales, asegurándose su correcta conservación, así como los controles de acceso adecuados.

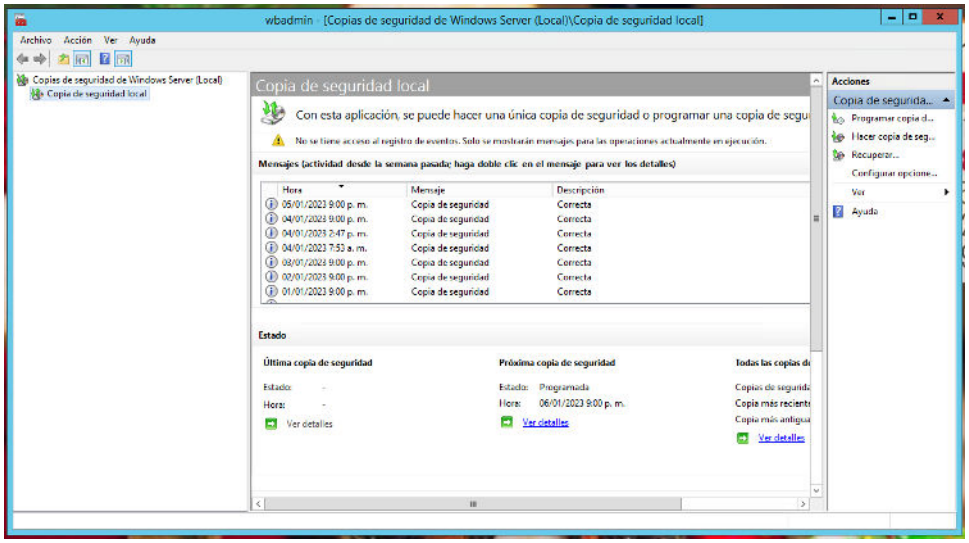
Se deberán realizar pruebas de restauración de las copias de seguridad disponibles y de los procesos de restauración definidos, a fin de garantizar el funcionamiento correcto de los procesos. Estas se realizarán de forma periódica y quedarán documentadas de acuerdo con el GG-DG-009 Plan de continuidad del Negocio

Se deberá garantizar que existe una copia de seguridad adicional de la información, de forma que se garantice su integridad ante la necesidad de recuperación frente a posibles incidencias de seguridad asociadas, por ejemplo, a Ransomware (Secuestro de datos)

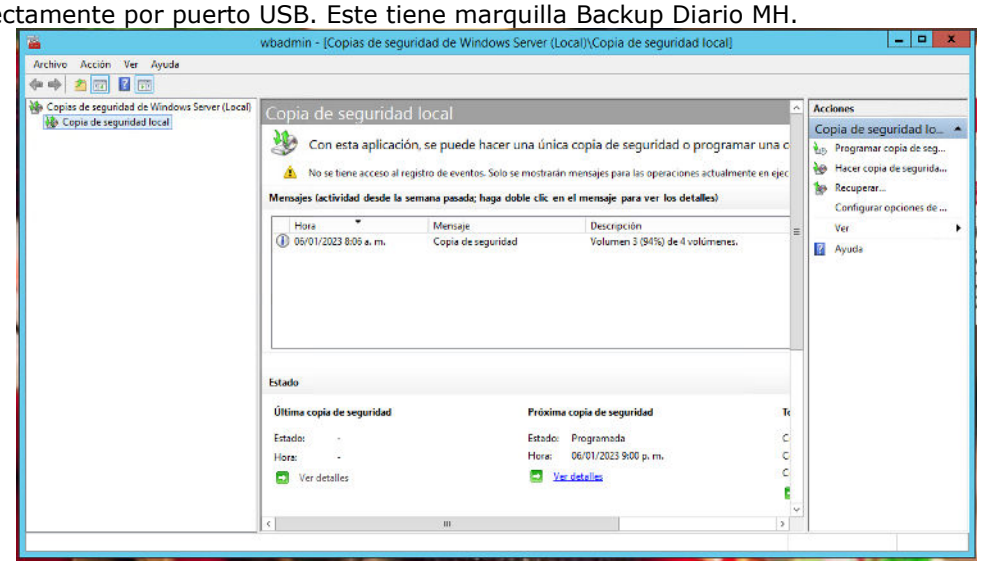
### 8.1 PROCEDIMIENTO DE BACKUP.

El procedimiento de Backup está configurado de la siguiente manera:

- **DCMH001:** Backup del servidor de dominio DCMH001 configurado para realizarse todos los días miércoles a las 9:00 PM se realiza Backup completo del servidor. Estado de sistema, y se guarda en una partición del Disco Duro.

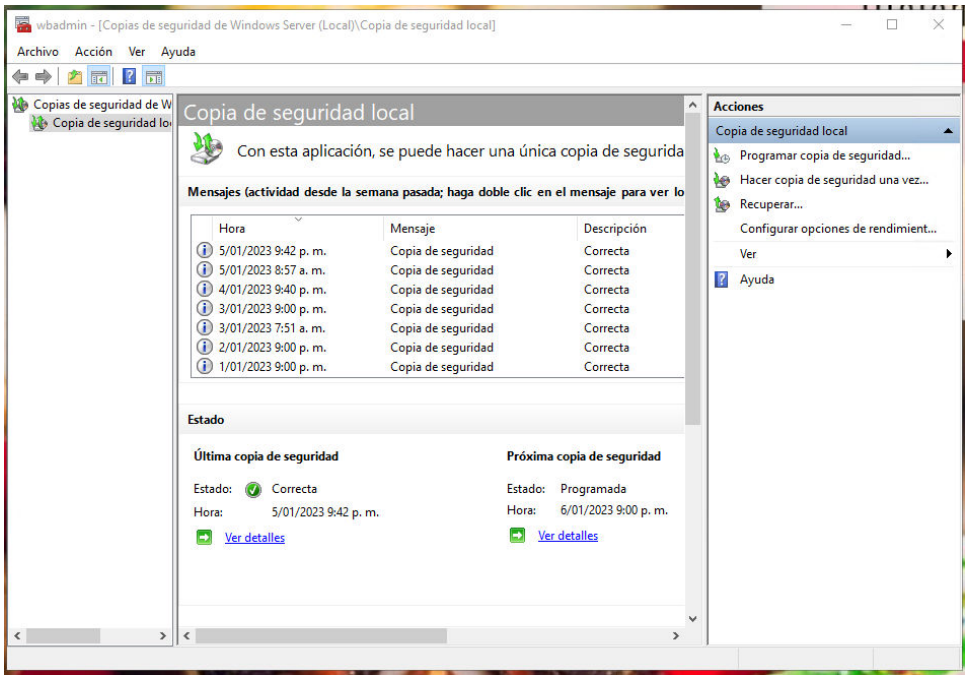



- **MHARCHIVO**: Backup del servidor de Archivo MHARCHIVO configurado para realizarse de lunes a viernes a las 9:00PM, se realiza Backup completo la unidad D y B donde se encuentra ubicados todas las carpetas de usuario personales y públicas, Docunet, Escaneo y DB almacenadas en este servidor. este es guardado en unidad de disco externa con conexión directamente por puerto USB. Este tiene marquilla Backup Diario MH.




**MHHYPER-VP**: Backup del servidor de Archivo MHHYPER-VP configurado para realizarse de lunes a domingo a las 9:00PM, se realiza Backup completo del servidor, en el cual se encuentra los servidores virtualizados y copias de bases de datos de los aplicativos que usa la compañía. este

es guardado en unidad de disco externa con conexión directamente por puerto USB. Este tiene marquilla Backup Diario MH




- **Backup Diario:** El líder de infraestructura Autorizado por la Directora de Servicios o quien designe la Coordinadora HelpDesk, es el responsable de entregar copias de seguridad todos los días a la Gerencia General en caso de su ausencia a la Gerencia Comercial y de Mercadeo y a la Gerencia administrativa, si ninguno de ellos se encuentra en Microhome la entrega se realizará a la Directora de Servicios y/o a la Coordinadora HelpDesk; se disponen de discos USB los cuales se intercambian todos los días y se deja registro en el Formato de Backup Diario (GG-FO-005), la copia almacenada corresponde al servidor MHARCHIVO.

- **Backup Mensual:** El líder de infraestructura Autorizado por la Directora de Servicios o quien designe la Coordinadora HelpDesk, es el responsable de entregar disco duro con las copias realizadas en cada uno de los servidores dejando evidencia en el formato GG-FO-004 al área de Recursos, quien posteriormente lo entregará a la coordinación de Recursos Humanos, quien posteriormente lo entregará a la Gerencia General en caso de su ausencia a la Gerencia Comercial y de Mercadeo y/o a la Gerencia Administrativa. Estas copias se realizan los 5 primeros días hábiles de cada mes; por seguridad se almacenan fuera de Microhome.

- **Backup Semestral:** El líder de infraestructura Autorizado por la Directora de Servicios o quien designe la Coordinadora HelpDesk, es el responsable de entregar disco duro con las copias realizadas en cada uno de los servidores dejando evidencia en el formato GG-FO-004 a la coordinación de Recursos Humanos, quien posteriormente lo entregará a la Gerencia General en caso de su ausencia a la Gerencia Comercial y de Mercadeo y/o a la Gerencia Administrativa. Estas copias se realizan los 7 primeros días hábiles del mes de Julio y Enero del año en curso; por seguridad se almacenan fuera de Microhome.

## 9. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información es de aplicación obligatoria para todo el personal de Microhome cualquiera que sea su situación contractual o la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Los propietarios de los activos de información son responsables de la clasificación, mantenimiento y actualización de los mismos, así como de documentar y mantener actualizada la información de acuerdo a sus funciones y competencias en general tienen la responsabilidad de mantener integra, confidencial y disponible el activo de información.

### 9.1 ANTIVIRUS

Todos los sistemas, servidores, computadores y portátiles deben tener el software de antivirus instalado y funcionando, las opciones de alertas en el antivirus se deben implementar de manera que se tenga una notificación oportuna de cualquier virus encontrado y la acción correctiva correspondiente.

Los Empleados de Microhome tienen estrictamente prohibido introducir, desarrollar o distribuir intencionalmente virus hacia dentro o fuera de la infraestructura de información y telecomunicaciones interna o hacia dentro o fuera de la infraestructura de clientes o proveedores

### 9.2 NAVEGACIÓN EN INTERNET Y CORREO ELECTRÓNICO

Está prohibido transmitir, mostrar mensajes, imágenes o información de cualquier tipo de material ilegal, amenazante, obsceno, pornográfico, acosador, difamatorio, calumnioso, ofensivo o escandaloso en Internet o Intranet.

Está prohibida cualquier descarga, distribución o modificación de los recursos legalmente protegidos a través de Internet o Intranet Microhome sin la debida autorización
Microhome cuenta con un portal cautivo para visitantes, se realiza a través del registro en la red y la autorización de ingreso la brinda el líder de infraestructura.

Los colaboradores de Microhome deben prestar el mayor cuidado en la transmisión de información confidencial o reservada para evitar la divulgación no autorizada.

### 9.3 CONTROL DE ACCESO A LA RED Y PROTECCIÓN DE LA INFORMACIÓN

Todos los sistemas de información deben contar con un sistema de control de acceso a los mismos. Asimismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas.

El control de acceso se entenderá desde la perspectiva tanto lógica (enfocado a sistemas de la información) como física.

Microhome asume una serie de requisitos de negocio para el control de acceso, que serán, al menos, los siguientes:

La cuenta de red y la contraseña son los elementos con los cuales un usuario es validado en la red y obtiene acceso a los recursos de tecnología de Microhome

Los usuarios deberán ser únicos y no podrán ser compartidos. Asimismo, los privilegios de los usuarios serán inicialmente asignados mediante el principio de mínimo privilegio

El líder de infraestructura es quien se encarga de la creación y el mantenimiento de cuentas de dominio y aplicaciones; su composición, complejidad de contraseña y deshabilitación de cuentas cuando ya no son requeridas.

La instalación, activación y gestión de los puntos de red es responsabilidad del Área de Servicios

**9.3.1 DERECHOS DE ACCESO**

Implementar controles de acceso que garanticen que a los usuarios sólo se les otorguen privilegios y derechos necesarios para desempeñar su función.

Los derechos de acceso deberán ser establecidos en función de:

- Control de acceso basado en roles: deberán establecerse perfiles o roles de acceso por aplicación y/o sistemas para poder asignar los mismos a los diferentes usuarios.
- Necesidad de saber: Solo se permitirá el acceso a un recurso cuando exista una necesidad legítima para el desarrollo de la actividad.
- Privilegios mínimos: los permisos otorgados a los usuarios deberán ser los mínimos.
- Segregación de funciones: deberá asegurarse una correcta segregación de funciones para desarrollar y asignar derechos de acceso.

Asimismo, ningún usuario deberá poder acceder por sí mismo a un sistema de información controlado sin la aprobación del responsable del propio usuario (o de la persona designada).

**9.3.2 IDENTIDADES PRIVILEGIADAS**

La asignación y uso de derechos de acceso privilegiado deberá estar restringida y controlada. El acceso privilegiado es el acceso a sistemas como administrador o con un rol que ofrezca la posibilidad de modificar la configuración del sistema.

La asignación de derechos de acceso privilegiado deberá ser controlada a través de un proceso formal de autorización de acuerdo con las políticas de control de acceso. Deberán considerarse, al menos, los siguientes requisitos:

Deberán identificarse los derechos de acceso privilegiados asociados a cada sistema o proceso (por ejemplo, sistema operativo, sistema de gestión de base de datos o aplicación), así como los usuarios a los que estos les deberán ser asignados.

La asignación de derechos de acceso privilegiados deberá realizarse en base a las necesidades de uso, basándose en el mínimo privilegio y necesidad de saber. Deberá definirse un proceso de autorización que incluya un registro de los privilegios asignados. No deberán concederse derechos de acceso privilegiado hasta que el proceso de autorización se complete.

Se deberán establecer procedimientos y mecanismos que aseguren la confidencialidad de la información secreta de autenticación para los usuarios genéricos de administración (por ejemplo, modificación frecuente de contraseña mecanismos de compartición de la contraseña seguros, etc.).

## 9.4 CONTROL DE ACCESO LÓGICO

### 9.4.1 POLÍTICA DE CONTRASEÑAS

Microhome establece una Política de contraseñas adecuada y alineada con las buenas prácticas en seguridad. A través de esta se definen los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña.

Los estándares que rigen la complejidad, seguridad y composición de las cuentas y contraseñas de dominio son totalmente administrados y controlados a través de una política del directorio activo.

A continuación, se describe las reglas generales respecto a las contraseñas de usuarios Microhome:

- Deben tener un mínimo de 8 caracteres y deben tener caracteres de por lo menos tres de las siguientes cuatro clases

    a. Letras minúsculas (por ejemplo, abcdef… z)
    b. Letras mayúsculas (por ejemplo, ABCDEF… Z)
    c. Números (por ejemplo 01234… 9)
    d. Caracteres NO-alfanuméricos, tales como los símbolos de puntuación (por ejemplo ¿:!@.. ).

- No pueden ser iguales a las cuentas o a ninguna parte o la totalidad del nombre del usuario

- El sistema solicitará automáticamente el cambio de contraseña a cada usuario.

### 9.4.2 ENTREGA DE CONTRASEÑAS Y USUARIOS

- Se realiza entrega de un dispositivo de almacenamiento en sobre sellado donde se encuentran todas las contraseñas de acceso a servidores, servicios, monitoreo de cámaras y demás requeridas para su acceso o administración, este se entrega a la Gerencia General y a la Gerencia Comercial y mercadeo o a la Gerencia administrativa , será actualizado y cambiado con intervalos de 6 meses.

## 9.5 LINEAMIENTO DE ESCRITORIO Y PANTALLA LIMPIA

Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

- Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del usuario), como de forma automatizada mediante la configuración del bloqueo de pantalla.

- Se deberá dejar recogido el entorno de trabajo al finalizar la jornada. Esto incluye la necesidad de que todo documento o soporte de información quede fuera de la vista, guardando bajo llave los que por su clasificación sean confidenciales o secretos

- Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

- La información clasificada, cuando se imprima, debe ser retirada inmediatamente de las impresoras.

### 9.6 GESTIÓN DE ACTIVOS

Se deberán tener identificados e inventariados los activos de información necesarios para la prestación de los procesos de negocio, por lo tanto se deberá mantener actualizado el inventario de activos.

Además, para cada activo o elemento de información deberá existir un responsable o propietario, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido. Se deberán actualizar de manera periódica las configuraciones de los activos para permitir el seguimiento de estos y facilitar una correcta actualización de la información.

### 9.7 GESTIÓN DE DISPOSITIVOS BYOD O DISPOSITIVOS PERSONALES

Al permitir la política conocida como BYOD (Bring Your Own Device), lo que significa que los empleados utilizan sus recursos o dispositivos móviles personales para acceder a recursos o la información.Adicionalmente, los usuarios deberán tener en cuenta una serie de requisitos establecidos en esta Política

- Se deberán aplicar las mismas medidas y configuraciones de seguridad a los dispositivos BYOD que tratan información igual que al resto de dispositivos de la compañía.

- El usuario será responsable de los equipos BYOD

- Cualquier incidencia que pueda afectar a la confidencialidad, integridad o disponibilidad de estos dispositivos debe ser reportada al responsable de seguridad.

### 9.8 TRABAJO REMOTO Y TRABAJO EN CASA

Los servicios de conexión a plataformas web estarán destinados exclusivamente a personal que cuente con usuario dentro del dominio de la compañía. Su uso por parte de cualquier otro tipo de colaborador requerirá autorización del responsable.

El equipo utilizado para la conexión en la modalidad de trabajo en remoto podrá ser propiedad del empleado para acceso a plataformas web. En caso de acceso a aplicativos internos deberá ser proporcionado por la compañía, con el fin de que se cumplan los siguientes requerimientos de seguridad:

1. Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones de seguridad.
2. Software antivirus instalado Licencia Original.
3. Software de firewall/cortafuegos personal instalado.

El teletrabajo desde un equipo propio del trabajador requerirá de todas las medidas de seguridad oportunas, con el objetivo de que el trabajo en remoto no suponga una amenaza para la seguridad de la información. Además, se podrán establecer medidas de seguridad adicionales a las existentes para asegurar de una manera más fiable la conexión segura en remoto.

### 9.9 PREVENCIÓN DE FUGAS DE INFORMACIÓN

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.

Se deberán analizar los vectores de fuga de información, en función de las condiciones y operativa de trabajo Para ello, se deberán identificar los activos cuya fuga supone mayor riesgo para cada sociedad, basándose en la criticidad del activo y el nivel de clasificación que la información tenga. Además, se deberán identificar las posibles vías de robo, pérdida o fuga de cada uno de los activos

## 10. REGISTROS

FORMATO ENTREGA DE BACKUP A GERENCIA GENERAL (GG-FO-004)
FORMATO DE BACKUP DIARIO (GG-FO-005)
MATRIZ GESTION DE RIESGOS (GC-MTZ-004)
PLAN DE CONTINUIDAD DEL NEGOCIO (GG-DG-009)

## 11. CONTROL DE CAMBIOS:

| VER | FECHA | MODIFICACIÓN |
|---|---|---|
| 1 | 02-01-2013 | El documento no se encontraba en el SGC |
| 2 | 23-08-2014 | • Se cambia logo en este documento.<br>• Se Actualiza el documento como lo indica el procedimiento de control de documentos.<br>• Se revisa el proceso actual para aplicarlo en el documento. |
| 3 | 26-10-2015 | • Se realiza actualización de todo el documento<br>• Se crea el formato GG-FO-004 ENTREGA DE BACKUP A GERENCIA GENERAL<br>• Se incluye las actividades para Creación de carpetas o asignación de permisos a carpetas existentes o restricciones y Solicitud permisos usuarios Nuevos. |
| 4 | 15-07-2016 | • Punto 3: Se agregan los datos del proveedor de Internet de Backup.<br>• Punto 5: Se cambian los datos del proveedor de la página web por los datos del proveedor nuevo y su administración<br>• Punto 6: Se realiza el cambio del servicio de firewall por puerta de enlace se describe el funcionamiento.<br>• Punto 8: Se realiza cambio de IP servidor MHAPLICACIONES se agrega imagen de configuración.<br>• Punto 8: Se eliminan datos SERVMHCAM se remplazan por los datos del DVR.<br>• Punto 8: Se eliminan datos servidor MHCRM se remplazan por los del servidor CRMMH.<br>• Punto 8: Se agregan datos del servidor MHTMG<br>• Punto 12: Se cambia la descripción de la topología de red se cambia imagen.<br>• Punto 13: Se realiza cambio de procedimiento de Backup de todos los servidores.<br>• Punto 13: Se elimina servidor MHCRM se agrega servidor MHTMG. |
| 5 | 11-11-2016 | • Punto 3 Se actualiza IP de las conexiones remotas<br>• Punto 5 Se actualiza definición de MHARCHIVO (se incluye NSIS) |

| | | |
|---|---|---|
| | | • Punto 8 Cambio nombre servidor MHAPLICACIONES a MHARANDA y su dirección IP y se actualiza imagen. Se incluye el servidor MHRMD y su descripción.<br>• Punto 9 Se elimina descripción de uso del fax (ya no se usa)<br>• Punto 11 Se actualiza la descripción de redes inalámbricas<br>• Punto 13 Se incluye programación de backup del servidor MHARANDA con su descripción; se actualiza programación y descripción de backup del servidor MHARCHIVO; se actualiza descripción de backup MHAPLICATIVO; se incluye servidor de BACKUP con su descripción; se incluye descripción de backup diario y mensual.Se incluye FORMATO DE BACKUP DIARIO (GG-FO-005) |
| 6 | 15-11-2017 | Se modifica cargo Jefe de Servicios a Directora de Servicios<br>Se modifica Servidor de Impresoras por MHANTCON<br>Se modifica Topología de la Red<br>Se ajustan formatos correspondientes a la realización de cada uno de los Backup<br>Se adicionan responsables de realización de Backup diario y mensual<br>Se adicionan responsables de recibir discos duros en caso de ausencia del Gerente General |
| 7 | 01-07-2019 | Se adiciona en usuario correo de oscar.perez@microhome.com.co en documentación servicios administrados Microhome Ltda.<br>Se modifican direcciones en Servicio de Internet<br>Se modifica número de canales en servicio de telefonía y modificación de servidor<br>Se modifica IP publica para MH ARANDA<br>Se elimina IP publica 186.154.195.75 MHAPLICATIVO<br>Se modifica dirección IP e IP local DVR CAMARAS<br>Se elimina servidor MHRMD<br>Se adiciona IP en MHANTCON<br>Se elimina Impresora HP Color 2600 asignada a ventas<br>Se elimina WIFI ubicado fuera del dominio LAB-MH<br>Se adiciona Backup MHANTCON<br>Se elimina servidor de Backup<br>Se elimina las entregas todos los viernes de las evidencias de copias de seguridad<br>Se adiciona Backup Semestral |
| 8 | 16-04-2020 | Se modifica la configuración en el Fortigate.<br>190.147.53.133/186.30.168.148 a 192.168.1.2 Fortigate<br>186.30.163.146 a 192.168.1.26 NVR Cámaras<br>186.30.163.150 a 192.168.1.10 ARANDA<br>186.30.163.149 a 192.168.1.25 Word Office<br>186.30.163.145 Puerta de enlace Navegación para acceso a internet<br>Backup de conexión a internet se encuentra contratado con Claro servicio My pymes de 100 Megas por cobre. Cuenta con la dirección publica 190.147.53.133/24<br>servicios de IP Trunking de ETB con 5 canales No de arranque 3074010 /14<br>Servidor de aplicación contable WORLD OFFICE acceso remoto por IP publica **186.30.163.149**<br>Servidor de cámaras para acceso local y remoto; vía web por la dirección IP **186.30.163.146** NAT en Fortigate con IP local **192.168.1.26**<br>Servidor con la aplicación de Clear Pass para el control de acceso a la red. Ip local 192.168.1.13<br>Servidor de aplicación de cotizaciones para consumo interno y de clientes. IP local 192.168.1.15.<br>Contamos con red WiFi dentro del dominio llamada: MICROCORP y MICROGUEST ubicadas en el segundo piso.<br>**MHNSIS**: Backup del servidor. |
| 9 | 01-12-2021 | Se ajusta cargo Analista SST-SGC<br>Se adicionan definiciones al documento<br>Se actualiza información referente a las cuentas de correo<br>Se actualiza información de servicio contratado para registro MX<br>Actualización De MB contratados para servicio de internet por ETB de 50 a 300 MB<br>Actualización De la información de la página web contratada actualmente con wordpress<br>Actualización información de switch |

| | | |
|---|---|---|
| | | Se eliminan servidores MHARCHIVO, MHTMG, MHRMD<br>Se adiciona en servidores CPPM-VM-x86_64-6.7.0.101814-HYPERV<br>Actualización nombres de equipos PCMH0XX y LTMH0XX y configuración de Windows en los equipos<br>Se adicionan las redes WIFI MICRORED Y MICRO_DEVICE<br>Actualización del Diagrama de topología de la red<br>Se elimina backup de MHTMG y se adiciona el backup de MHHYPER:<br>Se ajusta cargo de técnico de mantenimiento por líder de infraestructura<br>Se elimina la carpeta DOCUNET en la Red<br>En el numeral 9 se ajustan las contraseñas requeridas por Gerencia. |
| 10 | 06/01/2023 | Se actualiza alcance de la política de seguridad de la información<br>Se incluyen definiciones adicionales<br>Se actualizan datos de servicio de internet, correo electrónico (cantidad de cuentas)<br>Se actualiza MHAPLICATIVO por MHWO<br>Se actualiza MHHYPE por MHHYPER-VP<br>Se actualiza MHANTCON Por MHPRINT<br>Actualización MHARCHIVO<br>Se ajusta la periodicidad de ejecución de backups<br>Se adiciona numeral Lineamientos de Seguridad de la información<br>La entrega del backup mensual y semestral se hará inicialmente al área de Recursos Humanos. |
| 11 | 28-03-2023 | Actualización objetivo y alcance del documento<br>Se incluyen definiciones Ciberseguridad, Seguridad informática, Ingenieria social<br>Se incluye responsabilidad de los colaboradores y las Gerencias<br>Se incluye los items 7.1 IDENTIFICACIÓN Y CONTROL DE RIESGOS, 7.2 COMPROMISO DE LA ALTA DIRECCIÓN, 7.3 SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN<br>Se eliminan datos sensibles de la compañía<br>Se incluyen lineamientos de seguridad de la información: Trabajo remoto, gestión de dispositivos byod o dispositivos personales |