Políticas y Generales:

Lineamientos generales de Seguridad de la Información y el uso de sistemas e infraestructura de TI.

COPIA NO CONTROLADA

1. Propósito

Este documento tiene como objetivos:

1.1 Establecer las pautas que deben aplicar todos los colaboradores de GBM para que el desempeño de sus labores no ponga en riesgo la seguridad de la información.

1.2 Establecer los lineamientos por los cuales se deben regir todos los terceros que tienen relación con los sistemas e infraestructura de TI, con el fin de no poner en riesgo la seguridad de la información.

1.3 Desarrollar los conocimientos necesarios en los colaboradores de GBM, con la finalidad de hacer conciencia de la importancia de la seguridad de la información para GBM.

2. Alcance

Los Lineamientos Generales de la Seguridad de la Información y el uso de sistemas e infraestructura de TI cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros, que laboren o tengan relación con GBM.

En caso de incumplimiento de estos lineamientos por parte de un colaborador, se procederá según lo definido en el documento PG-CCO-002 Conozca a GBM en la sección de incumplimientos y sanciones.

El incumplimiento a estos lineamientos por parte de proveedores y/o socios comerciales, se procederá según lo dispuesto en el respectivo contrato y/o NDA (Non Disclosure Agreement)

Los usuarios que atenten contra la seguridad de los sistemas e infraestructura podrán incurrir en un proceso disciplinario (Regido por el reglamento del Código de Ética), responsabilidad civil o penal de conformidad con la legislación vigente aplicable según sea el caso. GBM cooperará plenamente con la investigación de cualquier presunto delito o violación de la seguridad de sistemas o infraestructura, bajo la dirección de las autoridades competentes.

3. Políticas

3.1 Human Capital debe comunicar y capacitar acerca de la política PG-PSI-001 Lineamientos generales de Seguridad de la Información y el uso de sistemas e infraestructura de TI, como parte del proceso de ingreso a la organización.

3.2 El Information Security Manager y Management Information Systems (MIS) deben:

3.2.1 Revisar, como mínimo una vez al año, o cuando haya cambios significativos dentro de GBM, la PG-SDI-001 Política de Seguridad de la Información de GBM.

3.2.2 Revisar, como mínimo una vez al año o cuando haya cambios significativos dentro de GBM, el presente documento.

3.3 Cada colaborador se compromete a desempeñar sus funciones, acorde a la estrategia y los valores de la compañía, así como lo indicado en este documento y documentos asociados. La responsabilidad en caso de incumplimiento de los lineamientos establecidos para el uso de información, sistemas e Infraestructura de TI, es única y exclusivamente del colaborador, el cual estaría sujeto a las sanciones de acuerdo con el documento PG-CCO-003 Código de Ética.

3.4 **Autoridades y grupos de interés.**

GBM debe mantener contactos apropiados con las autoridades pertinentes, así como con grupos de interés y foros especializados en áreas de seguridad.

3.5 **Dispositivos Móviles y Teletrabajo.**

3.5.1 **Uso de dispositivos personales - Bring Your Own Device (BYOD).**

GBM permite a sus colaboradores el uso de dispositivos propios y de su elección para ejecutar sus funciones laborales. A excepción del equipo de cómputo, el cual es provisto por la organización.

GBM se reserva el derecho de revocar este privilegio si el usuario no cumple con estos lineamientos.

Para el uso de estos dispositivos, los colaboradores de GBM deben estar de acuerdo con los términos y condiciones especificados en el formulario FO-ATH-006 Declaración de Entendimiento Uso Equipo Cómputo (equipo personal) de lo contrario no podrán utilizarlos.

COPIA NO CONTROLADA

3.5.2 **Uso aceptable de dispositivos personales.**

La compañía define como uso de negocio aceptable, actividades que directa o indirectamente soporten el negocio de GBM.

Durante el horario laboral, la compañía define como uso personal aceptable, tiempo razonable y limitado para comunicaciones personales, lectura o recreación a discreción del Gerente inmediato del colaborador.

Fotografías, video y audio capturado y distribuido sin consentimiento de los involucrados o de GBM puede tener consecuencias legales.

En todo momento, el colaborador es responsable del uso del dispositivo personal, en relación con:

- Almacenar o trasmitir material ilegal.
- Almacenar, reproducir o trasmitir pornografía.
- Acoso a terceros.
- Actividades comerciales diferentes a las de GBM.

Los colaboradores de GBM podrán usar sus dispositivos para acceder la siguiente información de la compañía: correo, calendario, contactos y documentos de oficina relacionados al negocio.

3.5.3 **Dispositivos y Soporte.**

Teléfonos inteligentes, Tabletas y Laptops son permitidas.

La conectividad es soportada por la unidad de Infraestructura Interna de MIS, en el caso de las oficinas ubicadas en Forum y Lindora. Para el soporte de oficinas de país, el soporte se realiza a través del Centro de Servicio del país.

En caso de problemas relacionados con el sistema operativo o Hardware de los dispositivos de uso personal, los colaboradores deben contactar al proveedor del dispositivo o al “carrier” para problemas relacionados con Sistema Operativo o problemas de Hardware.

En caso de que se requiera soporte en sitio para temas de conectividad, es la unidad de TSS (Technical Support Services), a través de su Centro de Servicio local, quien brinda la atención.

Los dispositivos provistos por la organización (ej: equipo de cómputo) deben ser presentados a los departamentos mencionados anteriormente para el aprovisionamiento correcto de aplicaciones de negocio como, por ejemplo: aplicaciones estándar (ej.: SAP GUI), exploradores (ej.: Microsoft Internet Explorer), software de oficina (ej.: Microsoft Office), herramientas de seguridad (ej.: OCS) y configuración al Dominio de GBM, antes de accesar la red.

COPIA NO CONTROLADA

3.5.4 **Reembolsos.**

GBM no reembolsará al colaborador ningún porcentaje del costo por el uso del dispositivo.

En términos generales, GBM no reembolsará al colaborador ningún porcentaje del costo por plan contratado de datos, voz o excedentes sobre el mismo, ni gastos por “roaming”, a menos que así esté establecido para la posición, o bien, sea aprobado a discreción del gerente del colaborador, previa autorización del Director de área o Gerente General.

3.5.5 **Seguridad.**

Con el objetivo de prevenir acceso no autorizado, los dispositivos deben estar protegidos por contraseña usando las características del dispositivo y que su robustez se acerque lo más posible a los requerimientos Corporativos.

La robustez de las contraseñas se especifica en los procedimientos PR-APM- 004 Accesos Lógicos- Perfil Usuario y PR-APM-003 Accesos Lógicos Perfil Administrador.

El dispositivo debe auto bloquearse con una contraseña o PIN si queda desatendido.

Teléfonos inteligentes, Tabletas o Laptops de uso estrictamente personal son permitidos únicamente en la red “GGuest”.

El dispositivo del colaborador podría ser remotamente “limpiado” (wiped) si:

- El dispositivo es perdido.
- El colaborador termina su relación laboral con GBM.
- Si se detecta incumplimiento de las Políticas Corporativas.
- Riesgo de virus o amenaza a la seguridad de la infraestructura de GBM.

3.5.6 **Generalidades sobre Riesgos/Obligaciones/Aviso Legal.**

Se espera de los colaboradores, en todo momento, el uso de los equipos conforme con la política de uso aceptable expresada anteriormente.

Aunque el Departamento de Infraestructura Interna de GBM tome todas las precauciones para prevenir pérdida de información personal en caso de una “limpieza” (wipe) remota, es responsabilidad total del colaborador tomar precauciones adicionales como respaldar su correo, calendario y contactos personales, etc.

GBM se reserva el derecho de desconectar los dispositivos o deshabilitar servicios sin notificación.

Es responsabilidad del colaborador reportar dispositivos perdidos o robados a GBM dentro de las próximas 24 horas siguientes al evento, los colaboradores son responsables de notificar al correspondiente carrier telefónico y a las instancias policiales según corresponda, inmediatamente después de la pérdida del dispositivo.

El colaborador es personalmente responsable de todos los costos asociados con su dispositivo.

El colaborador asume total responsabilidad con los riesgos incluyendo, pero no limitados a, pérdida total o parcial de información corporativa y personal debido a problemas de Sistema Operativo, errores, “bugs”, virus, “malware”, y/o fallas de software, hardware, o errores de programación que dejen el equipo inutilizable.

GBM libera su responsabilidad ante cualquier daño derivado del uso de la red y sistemas internos de GBM.

GBM se reserva el derecho de tomar acciones disciplinarias apropiadas por el no cumplimiento con esta política.

COPIA NO CONTROLADA

3.5.7 **Uso de dispositivos propiedad de GBM.**

Se entiende por dispositivos propiedad de GBM aquellos que se brindan al colaborador y están destinados a dar uso a los Sistemas Internos de la compañía y ser apoyo al colaborador en el cumplimiento de las responsabilidades laborales asignadas, de acuerdo con su cargo.

Todo colaborador de GBM antes de recibir el equipo debe firmar el formulario FO-ATH-004 Declaración de Entendimiento Uso Equipo Cómputo (asignado por GBM).

La modificación de sistemas operativos, instalaciones o modificaciones a las especificaciones de los equipos deben ser solicitados a la unidad de Infraestructura Interna, o bien, al Taller de Servicio de cada país, por medio de una solicitud de servicio formal a través del Service Desk.

3.5.8 **Home Office.**

En los países que ha adoptado la práctica de Home Office, GBM permite a sus colaboradores la realización de teletrabajo, siempre y cuando sus funciones apliquen y en coordinación con su jefe directo, por lo tanto, el colaborador debe firmar los documentos requeridos de acuerdo con PG-ATP-002 Política de regulación de Home Office.

3.6 **Sanciones.**

GBM establece las sanciones de acuerdo con el documento PG-CCO-003 Código de Ética y la PG-EDP-001 Política para el proceso disciplinario de colaboradores.

3.7 **Capacitación.**

Todo nuevo ingreso debe cumplir con el programa de inducción de GBM, de acuerdo con el procedimiento PR-DTO-003 Inducción General y el PR-DTO-006 Inducción a la Posición. Además, realizar la lectura íntegra de estos lineamientos, la PG-SDI-001 Política de seguridad de la Información de GBM y sus instrucciones relacionadas, así como, ser capacitado en el uso de las herramientas informáticas de trabajo.

3.8 **Gestión de Accesos.**

Los requisitos de seguridad para el control de acceso deben establecerse como parte de la recopilación de requisitos de sistemas y servicios nuevos o significativamente modificados, y deben incorporarse en el diseño resultante.

Además de los requisitos específicos de seguridad, se deben utilizar una serie de principios generales al diseñar controles de acceso para sistemas y servicios de GBM, entre ellos:

• Defensa en profundidad: la seguridad no debe depender de ningún control individual sino ser la suma de varios controles complementarios.

• Privilegio mínimo: el enfoque predeterminado debe ser asumir que no se requiere acceso, en lugar de suponer que sí.

• Necesidad de saber: el acceso solo se otorga a la información requerida para desempeñar el rol.

• Necesidad de uso: los usuarios solo podrán acceder a las instalaciones físicas y lógicas necesarias para su rol.

COPIA NO CONTROLADA

3.8.1 **Red interna de GBM y uso de internet.**

Se define como acceso a la red aquellas conexiones a internet o sistemas internos para cumplir las responsabilidades laborales asignadas, a todas aquellas búsquedas de información que apoyen de alguna forma la realización de las funciones específicamente definidas para cada puesto.

Desde las oficinas de GBM es posible hacer uso de la red de Internet, ésta es una herramienta con capacidad limitada que debe ser usada con racionalidad. Su mal uso va en detrimento de la calidad del servicio.

- **Acceso a redes sociales, portales de contenido “streaming” y herramientas peer-to-peer (P2P).**

  Es permitido sólo para actividades laborales que por su naturaleza lo requieran:

  - Redes Sociales.
  - Sitios de entretenimiento o contenido similar.
  - Sistemas de búsqueda y obtención de archivos de música, videos o archivos comerciales con derechos reservados.
  - Sistemas de compartición de archivos peer-to-peer (P2P)
  - Radio Emisoras y Canales de Televisión cuya transmisión sea vía Internet.

- **Archivos de uso personal (audio, video y fotos).**

  Para los casos de uso de archivos personales, los mismos deben cumplir con las siguientes condiciones:

  - No se permite respaldar archivos de uso personal en los servidores de GBM.
  - No se permite trasladar archivos de uso personal por la red entre equipos de GBM.
  - No se permite comercializar o utilizar aplicaciones que violen los derechos de propiedad intelectual.

- **Exploradores de Internet.**

  Las herramientas colaborativas y Sistemas Corporativos han sido desarrollados y probados con Microsoft Internet Explorer®, Safari y Google Chrome, la funcionalidad de los sistemas puede variar según el aplicativo que se utilice.

COPIA NO CONTROLADA

- **Monitoreo de la red y el uso de Internet.**

  GBM monitorea mediante dispositivos el tráfico de la red con el objetivo de asegurar la calidad de los servicios que sustentan las operaciones críticas del negocio. Controles adicionales serán autorizados por el Gerente General de cada país.

  GBM se reserva el derecho de monitoreo de sitios de internet que consulten los usuarios desde la intranet de la organización.

- **Mensajería Instantánea.**

  Las herramientas de mensajería instantánea oficiales de GBM son Webex Teams y Microsoft Teams. El uso de otras herramientas de mensajería instantánea (ej.: Skype®, Yahoo! Messenger®, Google Talk®, etc.) es de uso discrecional y debe ser utilizada racionalmente.

- **Excepciones de Mensajería Instantánea.**

  Se prohíbe el uso de cualquier tipo de mensajería instantánea en los equipos que estén ubicados en la red de los Centros de Impresión, con excepción de mensajería instantánea interna Webex Teams y Microsoft Teams.

- **Aspectos generales del uso de Internet.**

  El usuario es consciente de que GBM no puede conocer el contenido de la información que circula a través de su red y, por lo tanto, exime a GBM de toda responsabilidad en relación con el contenido de los mensajes transmitidos a través de ella.

  El usuario final de Internet debe hacer uso de las herramientas de seguridad provistas para evitar que la información accedida contenga virus que ponga en riesgo los bienes o servicios de la organización.

- **Usos no permitidos de la Internet.**

  En términos generales otras actividades Web que no están permitidas son las siguientes:

  - Descargar contenido ofensivo.
  - Amenazas o comportamiento violento.
  - Actividades ilegales.
  - Solicitudes comerciales (no relacionadas con la empresa).
  - Acceso, descarga, envío y/o transferencia de material con contenido pornográfico, sexista, homofóbico, racista, xenófobo, antisemita u otros potencialmente ofensivos.

  El uso no permitido de internet según se ha definido en esta sección, conllevará la aplicación de una sanción en forma inmediata. La empresa aplicará una política de cero tolerancias en este tema en particular.

- **Excepciones en el uso de Internet.**

  Los equipos relacionados directamente con el servicio de Impresión no deben tener acceso a la navegación por Internet.

- **Acceso a red para terceros.**

  La clave para la red “Gguest”, debe ser modificada y entregada bi-mensualmente por el Telecom Support Group, al General Services Receptionist, el cual la custodiará.

  Los consultores, proveedores externos o las visitas de GBM, únicamente se les brindará la clave de acceso para conectarse a la Red “Gguest”.

3.8.2 **Correo electrónico.**

Todo colaborador regular de GBM dispondrá de una cuenta de correo electrónico activa dentro del dominio @gbm.net, cualquier excepción debe contar con una justificación por escrito y ser aprobada por el MIS Manager.

Esta cuenta puede ser utilizada desde cualquier equipo con acceso a Internet. La titularidad de la cuenta pertenece a GBM. La vigencia de la cuenta comprende el periodo que inicia el primer día laboral y finaliza con la terminación del contrato.

Algunos usuarios externos dispondrán de una cuenta de correo electrónico, según solicitud del área responsable de su contratación, dentro del dominio @EXT.gbm.net.

COPIA NO CONTROLADA

- **Responsabilidad del usuario en el uso de cuenta de correo electrónico.**

  Es responsabilidad del colaborador, contratista, proveedor, socio comercial, consultor, entre otros hacer buen uso de su cuenta, entendiendo buen uso como:

  - Leer diariamente su correo y borrar o archivar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo (INBOX).

  - El uso de un lenguaje apropiado en sus comunicaciones.

  - El respetar las reglas de "Conducta" corporativas para las comunicaciones.

  - No permitir que segundas personas hagan uso de su cuenta.

- **Monitoreo de mensajes de correo electrónico enviados o recibidos.**

  Todo el tráfico de correo electrónico de GBM es analizado por sistemas automáticos de Anti-Spam, Antivirus y control de imágenes pornográficas. Todo mensaje catalogado en estas categorías es eliminado y se envían reportes semanales al administrador del correo Corporativo para tomar las acciones respectivas.

- **Prohibiciones de uso del correo electrónico.**

  Está prohibido el uso del correo electrónico para los siguientes casos:

  - El uso de la cuenta para fines comerciales diferentes a GBM.

  - El enviar o contestar cadenas de correo.

  - Enviar SPAM de información (correo basura), o enviar anexos (attachments) que pudieran contener información nociva u ofensiva para otro usuario como virus o pornografía.

COPIA NO CONTROLADA

- **Software.**

  - Se prohíbe el uso de software para el cual no exista una licencia de uso válido a título personal o a nombre de GBM.

  - Se prohíbe copiar programas de computadora adquiridos por GBM.

  - GBM se reserva el derecho de auditar el uso de Software sin previo aviso al usuario final.

  - Trimestralmente se genera el reporte del software instalado en las herramientas de usuario final utilizando la plataforma de SCCM (System Center Configuration Manager).

  - La revisión incluirá software sin licencia que esté en el dominio de GBM.

  - Está prohibido el uso de programas utilitarios privilegiados, que almacenen o administren información de acceso lógico. En caso de requerirlo para las funciones del puesto, el colaborador debe solicitar la autorización al jefe inmediato y al Manager Information System Management y debe quedar documentado por medio de correo electrónico.

  - No está permitido la instalación de software que corresponden a las siguientes categorías:

    - VPN para cambiar la ubicación (país)
    - Aplicativos P2P (peer-to-peer) - Torrents
    - Aplicativos de Streaming de Video/Película
    - Aplicativos de “Mineo de Criptomoneda”
    - Juegos de Computadora
    - Aplicaciones de Apuestas

  - Cuando se identifique un uso inadecuado, la unidad de Internal Infraestructure le notifica al usuario indicándole que debe proceder con la desinstalación del software respectivo en las próximas 48 horas hábiles. En caso de no acatar la medida, se le notificará al Gerente del colaborador para que le solicite tomar acción en un lapso de 24 horas hábiles. De no tomarse las medidas indicadas se informará a Human Capital para que proceda con las sanciones respectivas.

3.8.3 **Acceso físico.**

Las ubicaciones y los perímetros de las áreas seguras de GBM se deben definir y controlar a través de sus respectivos procedimientos de gestión de accesos físicos. En general se deben ubicar estas áreas para evitar el acceso o la visibilidad al público o personas no autorizadas. Si es posible, deben estar físicamente separados de las áreas públicas y no compartirse con terceros.

Para garantizar la seguridad de los sistemas de GBM y con el fin de proteger y resguardar los activos de TI, se prohíbe el ingreso a los edificios de GBM de personas no autorizadas.

La información específica de algunos sectores seguros de GBM se detallan en las instrucciones:

- IN-SDI-001 Gestión de accesos Físicos al Centro de Servicio.
- IN-SDI-002 Gestión Accesos Físicos al Service Desk Regional.
- IN-SDI-003 Gestión de Accesos Físicos al Centro de Monitoreo.
- IN-SDI-004 Gestión de Accesos Físicos a los Data Center.
- IN-SDI-005 Gestión de Accesos Físicos al Servicio de Printing.
- IN-SDI-006 Gestión de Accesos Físicos al Centro de Cómputo.

Cuando se requiere proporcionar acceso al público y/o aceptar entregas para un área segura, esto debe segregarse en la medida de lo posible con una interfaz controlada con el perímetro seguro y los procedimientos respectivos de gestión de accesos físicos, y el personal de entrega no debería tener acceso al área segura.

3.8.4 **Manejo de la identidad de los usuarios, contraseñas y roles en los sistemas de información de uso interno.**

El manejo de la identidad de los usuarios, contraseñas y roles se gestiona según lo indicado en los documentos PR-APM-004 Accesos Lógicos- Perfil Usuario y PR-APM-003 Accesos Lógicos- Perfil Administrador.

3.8.5 **Monitoreo de Servidores y Equipos de comunicación.**

El monitoreo de equipos principales está integrado de forma automática con el Centro de Monitoreo, con el objetivo de una atención oportuna en caso de ser necesario.

3.8.6 **Pantalla y escritorios limpios.**

Este apartado se rige según lo indicado en la PG-CCO-004 Política de Escritorios Limpios y el Formulario FO-CCO-001 Inspección de Escritorios Limpios.

COPIA NO CONTROLADA

3.9 **Infraestructura tecnológica propiedad del cliente.**

En el caso de que la infraestructura tecnológica utilizada por el colaborador pertenezca a un cliente, GBM se compromete a cumplir las medidas y controles de seguridad implementados por el cliente, con el fin de colaborar con la protección de la información.

El colaborador de GBM que preste servicio y tenga acceso a sistemas informáticos, tanto de forma remota como en las premisas del cliente, se compromete a:

a) Utilizar dichos sistemas con el único fin de realizar los trabajos objeto del servicio que se presta.
b) No utilizar dichos sistemas para procesar datos o desarrollar programas, que no formen parte del alcance del servicio.
c) No compartir el acceso con terceras personas.
d) No desactivar ningún programa de seguridad o intentar obtener datos diferentes a los estrictamente necesarios para realizar sus actividades bajo el servicio prestado.
e) Mantener toda la información a la que pudiera tener acceso en calidad de confidencial, incluidos los set de credenciales de acceso a los sistemas propiedad de EL CLIENTE.

3.10 **Clasificación de la información.**

3.10.1 **Pública.**

La información valiosa en poder de GBM se encuentra disponible para el público a través de métodos de publicación establecidos. Dichos elementos de información no necesitan clasificación y no requieren que se les asigne un propietario formal o inventariado.

3.10.2 **Interna.**

Para la información que GBM no publica libremente, parte de esta puede utilizarse para uso interno. Esta es típicamente información que es de naturaleza relativamente privada, ya sea para un individuo o para la organización y, aunque su pérdida o divulgación es poco probable que tenga consecuencias significativas, sería indeseable.

3.10.3**Restringida.**

La información de esta categoría es de alto nivel restrictivo, y si la información clasificada en esta categoría se divulgara a personas no autorizadas, GBM podría enfrentarse a posibles consecuencias legales y podría impactar de manera negativa su imagen en el mercado.

3.10.4**Confidencial.**

La información en esta categoría es restringida y altamente sensible, y está destinada a ser utilizada por un grupo específico de personas con una necesidad legítima de acceso para llevar a cabo sus funciones laborales. Si se revela fuera de GBM sin previa autorización del propietario, se expondría en un impacto definitivo legal, contractual o de imagen.

COPIA NO CONTROLADA

3.11 **Confidencialidad.**

Con el objetivo de mantener la información confidencial y de la no divulgación, entre los colaboradores de GBM, se debe firmar o aceptar una vez al año y antes de iniciar sus labores el formulario FO-ATH-005 Convenio de Información Confidencial.

De igual forma, en el objetivo de mantener la información confidencial y de la no divulgación, con los terceros, se solicita que se firme el formulario FO-LEG-014 Acuerdo de Confidencialidad.

Para todos los efectos, la información debe ser tratada como se indica en el documento PG-CCO-002 Conozca GBM en el apartado de “Política y uso de la información confidencial”.

3.12 **Respaldo de información.**

GBM mantendrá la custodia y disponibilidad de la información crítica del negocio en condiciones normales de la operación y ante eventos de desastre según la instrucción IN-EPC-012 Respaldo y Recuperación de Datos.

El colaborador es responsable de almacenar toda la información relacionada a sus labores, en los sitios que la organización ha autorizado: One Drive y SharePoint.

3.13 **Gestión de Incidentes y Solicitudes de Servicio.**

Los canales autorizados para la atención de Incidentes y Solicitudes de Servicio relacionados a dispositivos y sistemas es el Service Desk (Ext. 3911), mediante el correo support@gbm.net y a través del Portal de Autoservicio de Control Desk (solo aplica para Solicitudes de servicio).

Lo anterior de acuerdo con los procedimientos PR-GIN-001 Gestión de Incidentes y PR-GRQ-001 Gestión de Solicitudes de Servicio.

3.14 **Continuidad de negocio.**

GBM se compromete con sus clientes, accionistas, proveedores y colaboradores a mantener un Sistema de Gestión de Continuidad de Negocio, capaz de identificar los riesgos a los que se enfrenta la organización, y que pueden causar una interrupción de la operación normal del negocio.

Lo anterior se gestiona a través de los siguientes documentos:

- PG-EPC-001 Política del Sistema de Continuidad de Negocio de GBM.
- PR-EPC-001 Continuidad de negocio - Conocimiento de la Organización.
- PR-EPC-003 Continuidad de Negocio - Estrategias y Planes de Continuidad.

- PR-EPC-004 Continuidad de Negocio- Pruebas, Indicadores y Mejora continua.
- PR-EPC-002 Continuidad de Negocio. Acciones de Contención.

3.15 **Control de Seguridad.**

La gerencia de MIS y el TSS Field Manager de cada país, o las personas que éstos deleguen, son responsables de monitorear la ejecución y cumplimiento de las actividades descritas en esta sección.

- **Vigilancia y Monitoreo**.

Los mecanismos de vigilancia y monitoreo mínimos que deben existir en los centros de Cómputo son:

- Video vigilancia.
- Tarjetas electrónicas de acceso o en su defecto llaves de acceso.
- Bitácora digital o física de eventos dentro del centro de cómputo.
- Monitor de Temperatura.

COPIA NO CONTROLADA

3.16 **Retención de Información.**

GBM mantendrá la información financiera y de capital humano por el período de tiempo legal que se requiera en cada país donde GBM opera.

3.17 **Mantenimiento de Activos de Infraestructura.**

Es responsabilidad de las unidades de Support, DataCenter y SmartOps, brindar los servicios de mantenimiento correctivo y preventivo según los acuerdos de servicio internos (OLA's) establecidos con el departamento de MIS.

La Gerencia de MIS es la responsable de asegurar el cumplimiento de los servicios de mantenimiento según los OLA´S adquiridos.

Como activos de infraestructura se entiende:

- Servidores
- Equipo activo de comunicaciones (routers, switches, firewalls)
- Computadores de Escritorio y Portátiles
- Equipos de Video Conferencia
- Teléfonos
- Equipos auxiliares para salas de conferencias (Video beams, Pizarras electrónicas)

Fin del Documento

Políticas y Generales

Lineamientos Generales de Seguridad de la Información y el uso de sistemas e infraestructura de TI

PG-PSI-001

Fecha de Publicación	**21/oct/2021 17:02**			Versión	**14**
Fecha de Elaboración	**21/oct/2021 16:28**	Frecuencia de Vigencia	**12 Meses**	Vigencia del Documento	**21/oct/2022 17:02**
Emisor	**JACKELINE SILVA CARMONA**				
Puesto	**BUSINESS PROCESSES ANALYST**				

COPIA NO CONTROLADA

Firmas

Paso	Participante	Puesto	Fecha
Aprobación Business Process	JACKELINE SILVA CARMONA	BUSINESS PROCESSES ANALYST	21/oct/2021 16:32
Aprobación Dueño de Proceso	MARIA GABRIELA ROYO FERRUFINO		21/oct/2021 17:02