1. OBJETIVOS

El estándar de seguridad informática (ESI) es un instrumento de la organización para concientizar y dar los lineamientos a sus colaboradores responsables de la correcta gestión de los activos de información a su cargo y así garantizar la confidencialidad, disponibilidad e integridad sobre cada uno de ellos.

- Mantener Homologada la información de la compañía contando con información actualizada, probada y libre de errores u problemas de seguridad.

- Homologar la configuración del firewall, en donde se garantice la denegación de accesos y de controlar aquellos que sean permitidos para el funcionamiento de algún aplicativo de la empresa.

- Mantener Homologada la información de la compañía en donde las herramientas de trabajo contengan los aplicativos requeridos para cada usuario protegiendo la seguridad de la información.

- Controlar que la información de la compañía, así como de proveedores y clientes se mantenga en absoluta confidencialidad, considerando que los dispositivos de almacenamiento, así como la papelería son considerados como activo importante para la protección del negocio.

Este estándar es un medio de comunicación para los dueños de los activos de información de seguridad de la información / Ciberseguridad y tecnología. El estándar establece el canal formal de actuación del personal, con relación a los recursos y servicios informáticos y que hace reconocer la información como uno de sus principales activos, así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Se establece la obligación de vigilancia del personal por el uso y limitaciones de los recursos y servicios informáticos críticos de la compañía.

2. ALCANCE

Todos los colaboradores contratados para *Integral Group Solution* (IGS) y lideres responsables de activos de información.

Todos aquellos proveedores internos o externos que intervengan en algún proyecto dentro de la compañía directa o indirectamente.

3. RESPONSABLES

La información depositada en este documento es de absoluto cumplimiento por cada uno de los empleados y proveedores de la compañía.

El líder de la Plataforma de Servicio de cada filial es el responsable de garantizar el cumplimiento de este estándar.

El incumplimiento de alguna directriz de este documento debe ser informado al Gerente Latam de infraestructura, vicepresidencia de tecnología y oficial de seguridad de la información quienes tomarán las medidas correctivas y de tratamiento.

4. DEFINICIONES Y ABREVIATURAS

N/A

5. CONTENIDO

5.1. ACTUALIZACIÓN SOFTWARE IGS

Reglas de actualización

Toda *Actualización de Software* deberá realizarse en ambiente de prueba.

- Si no se cuenta con un equipo físico de laboratorio, se deberá hacer las pruebas en un equipo virtual replicando lo que se tiene en producción.
- Una vez actualizado el software deberá presentar resultados y generar manual de actualización que deberá ser revisado y probado por el Gerente de infraestructura.
- Una vez se reciba el autorizado de actualización se procederá con las debidas precauciones.
- Respaldo completo del equipo a actualizar
- Contar con todo equipo y software requerido antes de proceder
- Realizar en horarios acordados de ventanas de tiempo y contar con un plan de contingencia.
- Una vez concluido enviar informe a Gerente a cargo.

5.2. CONFIGURACIÓN FIREWALL

Sistemas o Equipos

- Fortigate 60E / 60D

Configuración Inicial de equipamiento La configuración inicial es:

- Deny All
- Activar IDS y IPS
- Activar logs

Puertos de acceso especiales

- Comunicación VoIP (En caso de ser requerido)
- VPN
- Monitoreo externo
- VPN site to site (Previa autorización de conexión.)

Informe firewall semanal

El Gerente, jefe o encargado de sistemas deberá enviar en el informe semanal los resultados de la revisión del firewall según formato establecido.

5.3. CONFIGURACIÓN INICIAL LAS ESTACIONES DE TRABAJO.

1. Se deberá verificar en base al requerimiento del responsable de área que el equipo sea necesario y que tenga la autorización del Gerente a cargo quien validará con finanzas el presupuesto aprobado para cada área.

2. Obtener 3 cotizaciones.

3. Una vez adquirido el equipo se deberá revisar que cuente con el sistema Operativo Windows con licencia.

4. El nombre de cada dispositivo deberá formarse de la siguiente manera: IGSCOXX1234, siendo:

    - El Grupo de trabajo deberá formarse de la siguiente manera:
      IGSCO IGS (fijo) + Prefijo País (CO)

    - Tipo de equipo
        - PC (PC)

- Notebook (NB)
- Impresora (IMP)

- Número de dispositivo correlativo y no repetido en cada tipo de equipo.

5. Las IP's asignadas deberán ser asignadas por DHCP para que asigne IP automáticamente.
6. Instalar las impresoras correspondientes con clave de usuario de acuerdo al perfil de usuario.
7. En caso de haber sido solicitado y aprobado se instalará Office y se deberá actualizar el inventario de licencias de software
8. Los dispositivos de almacenamiento deberán ser bloqueados física y lógicamente.
    - Cable interno
    - BIOS

<u>Configuración de las estaciones de Telemarketing</u>

Hasta el punto 5 del listado anterior se mantiene para este sector, la diferencia radica en las condiciones de seguridad que necesitan estas máquinas de ventas.

- No instalar impresoras de red ni locales.
- No instalar aplicativos innecesarios, solo los de telefonía y navegación básica.
- Deshabilitar:
    - Consola.
    - Registro de Windows.
    - Task Manager
    - Unidades extraíbles USB.
    - Acceso a internet
    - Escritura en la raíz del disco local
    - Instalación de programas.
    - La cuenta local "TMK" debe ser del grupo Usuarios.

- En caso de ser necesario se asignará una contraseña a la cuenta “TMK”.
- La cuenta “Administrador” tendrá una contraseña para la administración de la maquina local, que solo la usará tecnología.

Configuración de Acceso a Internet a las estaciones de trabajo.

- En caso de requerir acceso a una página no común, o que requiera un puerto en particular, se debe obtener aprobación de la Gerencia de Sistemas.
- El acceso a las redes sociales será monitoreado, debido a que puede interferir en el trabajo diario. Si es requerido se bloquearán.
- Los accesos a los correos públicos se inhabilitarán, pero cada usuario administrativo tiene una cuenta de correo personal corporativa configurada en el cliente de correo.

Configuración estándar de los Servidores

Usuarios

- Administrador / Root
- Contraseña alfanumérica, de 8 caracteres de longitud minimos.
- Usuario estándar
  - Contraseña alfanumérica de 8 caracteres mínimo
  - Cuenta requerida para conexiones vía RDP/VNC o Terminal.
  - Desde esta cuenta se puede elevar privilegios.
- Firewall interno.
  - Por default solo se abren los puertos necesarios para comunicación de aplicativos.
- Administración.
  - Cada servidor tiene una nomenclatura: **IGSCOSE0000**
  - Siendo SE0000: el prefijo SE (servidor), seguido de un numero de 4 dígitos único y correlativo.

  Los dispositivos deben quedan registrados en una planilla con su número de IP.

5.4. DIRECTIVAS DE CUENTAS Y CONTRASEÑAS

Directivas de cuenta

- Directivas de contraseñas

  - ✓ Cambio de contraseña en el primer Login
  - ✓ Longitud mínima de la contraseña: 8 caracteres
  - ✓ Requerimientos de construcción: Mínimo una mayúscula y dos números.
  - ✓ Forzar el historial de contraseñas: 4 contraseñas recordadas
  - ✓ Forzar el cambio de contraseña: cada 30 días
  - ✓ Historial de No uso de las ultimas 2 contraseñas

- Directiva de bloqueo de cuentas

  - ✓ Umbral de bloqueos de la cuenta: 5 intentos fallidos
  - ✓ Duración del bloqueo de cuenta:5 minutos
  - ✓ Restablecer la cuenta de bloqueos después de: 5 minutos
  - ✓ Cierre de sesión por inactividad después de 1 Minuto
  - ✓ Vencimiento automático de cuenta por inactividad: 3 meses

5.5. DESTRUCCIÓN DE LA INFORMACIÓN

Clasificación de información a destruir

1. Información de clientes (Base de datos, estrategias comerciales y cualquier información considerada o etiquetada como confidencial)
2. Base de datos del negocio en general
3. Listas, red, mapa de proveedores, Bases de datos, software, clientes y datos de contacto, información financiera, comercial y legal, métodos, procedimientos y políticas del negocio, información de sus empleados y colaboradores, y en general toda información que apoye el éxito del negocio

Procedimiento de destrucción

1. Informar la baja de dispositivos de almacenamiento al Gerente a cargo

2. La Gerencia de tecnologia asignara un recurso para la información a destruir.
3. Identificar la información que deberá ser destruida y clasificarla según inventario de documentación.
4. En caso de ser dispositivos de almacenamiento, Discos Duros, CD's, DVD's:
    - Triturar los DVD's/CD's; en caso de discos, romper la lógica, y si es posible abrirlos para que el contenido se borre.
    - Papel
        - Trituradora
5. Generar Reporte de información destruida.

5.6 DECÁLOGO DE SEGURIDAD

IGS considera la información, activos y colaboradores elementos fundamentales para el desarrollo de su negocio, en ese sentido vela por su protección y seguridad integral.

1. Toda Información referente al negocio, por ejemplo: las listas, red, mapa de proveedores, Bases de datos, software, clientes y datos de contacto, información financiera, comercial y legal, métodos, procedimientos y políticas del negocio, información de sus empleados y colaboradores, y en general toda información que tenga incumbencia en el desarrollo del negocio, son un activo de carácter confidencial y es propiedad intelectual de IGS quien se encarga de definir los roles y niveles de acceso a la misma.
2. Como cualquier activo, la información debe tener un dueño responsable asignado de acuerdo a los roles sobre los procesos, encargado de velar por su confidencialidad, adecuado uso y distribución. En su caso, tenga en cuenta que Usted no podrá

   realizar reproducciones de ninguna clase de la información. Usted solo se encuentra autorizado para la consulta con fines propios del negocio de IGS
3. Todo colaborador es responsable por velar por la seguridad de las personas, activos e información de la compañía. Por seguridad de la información, los colaboradores no podrán ingresar a las instalaciones de IGS cualquier dispositivo de almacenamiento conocido o por conocer, tales como y sin limitar, memorias USB, CD-RW, IPOD'S, Teléfonos Celulares.
4. Todo Colaborador está obligado a cumplir las políticas, normas y lineamientos de seguridad que dicte la compañía.

5. Los colaboradores que tienen acceso a la información confidencial del negocio tienen la responsabilidad de guardar absoluta reserva de la misma evitando su difusión verbal, electrónica o escrita a personal no autorizado en especial en actividades no laborales y/o sitios externos a las instalaciones de la compañía y deben emplear su perfil usuario y contraseña de forma personal e intransferible.

6. Los colaboradores del negocio que tienen acceso a los sistemas de información y a las herramientas que permiten distribución de la misma como: correo, carpetas compartidas en red, fax, fotocopiadora, impresión, correo electrónico, etc. deben usar estos medios con máxima prudencia y total responsabilidad evitando enviar información sin autorización a destinatarios no autorizados.

7. Los colaboradores de IGS son contratados invocando el principio de confianza en el personal y como tal deben abstenerse de acceder a información a la que no han sido autorizados así como distribuir información a personas no autorizadas.

8. Los colaboradores de IGS que tienen a cargo la custodia de información del negocio representada en medios verbales, escritos y/o electrónicos debe garantizar que estos activos reposan en personal confiable y ambientes físicos y/o lógicos seguros, exigiendo los elementos que considere necesarios para salvaguardar los activos de información.

9. IGS facilita los mecanismos que garanticen la seguridad integral de las personas, activos e información, incluyendo planes de contingencia y establece los planes que permitan la Continuidad de la operación de la empresa en caso de falla mayor o desastre.

10. IGS deberá de forma permanente mantener actualizados los roles de los colaboradores dentro de la compañía que garanticen que el acceso a la información esta monitoreado por un dueño del activo y un grupo de usuarios que acceden a él sin causar riesgos a la confidencialidad, integridad y disponibilidad de los activos de información.

5.7 BUEN USO DEL CORREO ELECTRÓNICO

IGS pone a disposición de sus colabores la herramienta de correo electrónico con el fin de apoyar el intercambio y difusión apropiada de la información relacionada exclusivamente con el negocio. El correo electrónico es de propiedad exclusiva de IGS y el empleado es

consciente que la Compañía o la empresa podrá hacer verificaciones en los correos electrónicos, con el fin de evaluar la aplicación de la política de confidencialidad.

A. *Responsabilidades de los usuarios:*

1. Utilizar los servicios de forma responsable y racional para uso de las labores inherentes a su cargo.
2. Este servicio es personal e intransferible. No facilitar su cuenta de correo a otra persona.
3. Acceder al correo desde fuera de la oficina sólo si ha sido autorizado.
4. Enviar mensajes tomando las debidas precauciones cuando éste contiene información confidencial activando las opciones de codificación y firma electrónica.
5. Verificar que los destinatarios de sus correos sean los indicados para evitar que llegue información a personas equivocadas.
6. Firmar el correo, indicando: nombre, apellido, cargo, área, teléfono.
7. Evitar las opciones de “responder a todos” y/o “cadena de mails” a menos que sea realmente necesario.
8. Eliminar los anexos cuando responde sus correos.
9. Enviar correos breves y concretos a las personas estrictamente necesarias, ya que esto exige un alto consumo de recursos de red.
10. Evitar la distribución masiva de los mensajes que contienen anexos.
11. Hacer uso de Directorios compartidos ó si es información de interés general, divulgarla a través del mail Corporativo.
12. No difundir las cadenas de mails, masivos o "bola de nieve".
13. Cuando se vaya a retirar de su puesto de trabajo, aún de forma momentánea, desconectar la sesión de correo con el fin de evitar accesos de personas no

    autorizadas a su buzón.
14. Activar el ausente de oficina cuando se presente esta condición.
15. Utilizar racionalmente el espacio de almacenamiento asignado y activar el archivado local.

16. Eliminar sin abrir, los correos cuyo remitente o asunto sea sospechoso, para evitar el ataque de virus o hackers. Informar sobre cualquier señal de correos que puedan tener posible presencia de virus.

17. No abrir ni difundir mensajes con “Alertas de Seguridad” a menos que provengan del área de Gerencia de tecnologia.

18. No leer ni remitir mensajes que no le correspondan por destinatario, área o nivel jerárquico en la organización, Informar a quien envió el mensaje sobre el error de destinatario.

19. Cambiar o solicitar el cambio periódicamente de la contraseña.

20. No emplear desde la red privada correos en servidores públicos como Hotmail, Yahoo, este último a menos que se emplee como un método de contingencia por fallas en el servidor principal, etc.

21. Uso responsable de las listas de correos, no responder correos informativos corporativos a menos que sea necesario.

B. *Responsabilidades de los Jefes directos, Gerentes, Directores o responsables de usuarios para con el correo de sus colaboradores:*

1. Para los colaboradores cuyos cargos no tienen definido el uso del correo electrónico, el jefe debe autorizar con el mayor criterio el uso de la herramienta y solicitarla directamente a la Gerencia de tecnología.

2. Autorizar el acceso a un buzón por parte de un tercero en casos especiales.

3. Con el mayor criterio, autorizar el ingreso de sus colaboradores al correo desde fuera de la oficina.

4. Supervisar el cumplimiento de las políticas y buenas prácticas de uso de la herramienta.

5. Coordinar con la Gerencia de tecnología la difusión de correos de interés general en forma masiva y distribuirlos bajo el criterio y políticas de la Compañía.

6. Informar a la Gerencia de tecnología cuando se requiera copiar o guardar correos de algún colaborador que se ha retirado de la compañía o ha cambiado de cargo.

7. Informar a la Gerencia de tecnología, cualquier novedad en cuanto al retiro o traslado de usuarios, indicando qué debe hacerse con el correo de la persona que deja de usar la herramienta.

8. Dar a conocer masivamente y fomentar las políticas y buenas prácticas acerca del correo electrónico.

9. Revisar la conducta del empleado al infringir derechos de autor, propiedad intelectual o industrial, envío de información obscena, pornográfica, injuriosa, calumniosa o que se constituya en una amenaza a la integridad de las personas y aliente conductas que puedan traducirse en ofensas o puedan comprometer la seguridad y confidencialidad de la información de IGS.

10. Establecer y divulgar las sanciones establecidas en caso de incumplimiento de las políticas.

C. *Responsabilidades de Sistemas:*

1. Efectuar la administración, control y auditoría de los servicios que preste con relación al correo.

2. Emitir informes de incidentes a las direcciones de las áreas afectadas, con copia a la Gerencia de tecnología y seguridad de la información.

3. Emitir y coordinar la difusión de las buenas prácticas en el uso del correo.

4. Asignar los nombres de buzones de correo de acuerdo al estándar vigente de la compañia (primer letra del nombre más apellido)@igroupsolution.com

5. Asignar las cuentas con la cuota de almacenamiento estándar ó según solicitud de las Personas autorizadas. (Default 10 Mb)

6. Mantener en total reserva las listas de correo. No entregarla a terceros.

7. Mantener durante 1 mes, una copia de seguridad de la bases de datos del correo de los colaboradores que han salido de la compañía o han sido trasladados a otra área o cargo, a menos que el jefe del colaborador le haga una solicitud especial.

D. *Responsables de su aplicación*

Son responsables de su aplicación todos los colaboradores de IGS y terceros especialmente autorizados para el uso del correo de la Compañía.

Basados en el establecimiento de estas políticas y los valores Corporativos de IGS, es expectativa de la compañía, el apoyo y cumplimiento de la presente política por cada una de las personas responsables, tal como se especifica también en los contratos de trabajo con los colaboradores y los acuerdos de confidencialidad con terceros.

5.8 BUEN USO DE CONTRASEÑAS

IGS habilita el acceso a sus aplicativos y servicios para apoyar el desarrollo de los procesos y el manejo apropiado de su información, utilizando solicitudes formales para todo lo que tenga que ver con solicitud de asignación o actualización de usuarios, autorizaciones y contraseñas, teniendo en cuenta las siguientes responsabilidades:

A. *Responsabilidades de los usuarios:*

1. Utilizar sus usuarios y contraseñas de forma responsable.
2. El usuario asignado a cualquier aplicativo o servicio es de uso estrictamente personal e intransferible y de carácter exclusivo para ejercer labores inherentes a su cargo. Para el caso de terceros, este servicio se rige bajo las cláusulas de confidencialidad del contrato pactado con IGS
3. Cuando se vaya a retirar de su puesto de trabajo de forma momentánea, deberá salir o bloquear el acceso a los sistemas en los que esté trabajando.
4. Informar al administrador del sistema sobre cualquier irregularidad o acceso al cual considere que usted no debería tener permiso por efectos de proceso o de confidencialidad de la información.
5. Cambiar las contraseñas frecuentemente.
6. Debe ser precavido con la protección (custodia) de las contraseñas. No deben dejarlas escritas o visibles a otras personas.
7. Si tiene PC portátil, debe tener contraseña de prendido (solicitar a la Gerencia de tecnología), para bloquear el acceso a la información del disco duro en caso de robo o pérdida y debe de tener un candado de seguridad, una copia el usuario y otra el

Gerente a cargo.

8. Si requiere cambio de contraseña, en caso de olvido o bloqueo, debe solicitarlo personalmente. Ningún usuario está autorizado a pedir cambios de contraseña a nombre de otro usuario.

9. Cambiar la contraseña, cuando ha sido revelada o cambiada por terceros por motivos de fuerza mayor, tan pronto se haya superado la situación de excepción.

B. *Responsabilidades de los Jefes inmediatos o responsables de usuarios.*

1. Los jefes inmediatos deben asegurarse que cada colaborador tenga las autorizaciones requeridas de acuerdo a sus funciones. Asimismo son responsables de que el colaborador deje de tener dichas autorizaciones cuando se produce algún cambio en sus funciones.

2. En caso de reemplazos por traslado, vacaciones, incapacidad o casos especiales, el jefe inmediato debe solicitar un nuevo perfil de usuario para la persona que asumirá el cargo. Por ningún motivo se debe continuar usando el perfil del usuario ausente.

3. Los Jefes inmediatos deben autorizar a un colaborador para que pueda acceder a los sistemas del negocio desde fuera de la oficina, en casos excepcionales y si el aplicativo lo permite.

4. Supervisar el cumplimiento de las políticas y de las buenas prácticas

asociadas. C. *Responsabilidades de Sistemas:*

1. Los administradores de seguridad (plataformas, aplicativos o servicios) del área de Sistemas, deben garantizar la administración, control y auditoria de asignación y uso de perfiles de usuario y suministrar registros de utilización de los mismos en caso de ser necesario.

2. Los administradores de seguridad y/o de red deben mantener en total reserva su contraseña. Sólo su jefe inmediato debe tener copia de ésta en sobre cerrado y lugar seguro. Si la contraseña es revelada por motivos de fuerza mayor debe ser cambiada inmediatamente superada la situación.

3. Establecer los estándares para definiciones de nombres de usuarios y forma de registrar la información básica de los usuarios, con el fin de unificar mantener y facilitar la administración.

4. Emitir informes de incidentes en asuntos de contraseñas a las direcciones de las áreas afectadas con copia a la Gerencia de tecnología y seguridad de la información.

5. Informar a los jefes inmediatos en caso de detectar préstamos de contraseñas con copia a la Gerencia de tecnología.

6. En caso de terceros que presten soporte, se debe reportar y llevar un estricto control de los accesos a los sistemas, en especial los de producción con previa firma de contrato de confidencialidad.

7. Mantener en total reserva los usuarios y contraseñas con copia a la Gerencia de tecnología.

8. Configurar (activar) un protector de pantalla con contraseña en los PC's de los usuarios con copia de la contraseña al área de sistemas.

9. Reportar Semanalmente a la Gerencia de tecnología las actividades sobresalientes, problemas, errores, fallas en sistemas, Bases de Datos, comunicaciones, seguridad, etc.
10. Llevar una bitácora de eventos por Hardware, Software y Comunicaciones diaria que será revisada en cualquier momento por Gerente de tecnología.

D. *Responsables de su aplicación*

Son responsables de su aplicación todos los colaboradores de IGS y aquellos terceros a quienes se les ha autorizado el acceso a uno o varios aplicativos y servicios de IGS, por medio de la asignación de un usuario y contraseña respectiva.

Basados en el establecimiento de estas políticas y los valores Corporativos de IGS, es expectativa de la compañía, el apoyo y cumplimiento de la presente política o estandar por cada una de las personas definidas como responsables aquí, tal como se especifica también en los contratos de trabajo con los colaboradores y los acuerdos de confidencialidad con terceros

Dentro de las medidas de seguridad existentes se establece que el cambio de contraseñas de id's funcionales (Administrador, Root, Admin, etc.…) en Servidores, equipos de comunicación, telefonía y Seguridad, competen al Gerente de Sistemas, por ningún motivo se permitirá el cambio de contraseñas a alguien distinto a menos que tenga una indicación formal y documentada de Dirección, dichas contraseñas serán resguardadas en la compañía.

5.9 BUENAS PRÁCTICAS EN EL USO DE ACCESO REMOTO

1. Indicar a que servicio específico está autorizado ingresar.

2. El área de Sistemas debe garantizar la administración, control y auditoria de buen uso de este servicio y suministrar logs de uso del mismo en caso de ser requerido por una acción de auditoría. Así mismo los Administradores de plataformas de los servicios autorizados a acceder vía acceso remoto deben mantener logs del sistema a los accesos de este tipo sobre los sistemas del negocio.

3. La administración de usuarios en tecnología debe garantizar cambio frecuente de contraseña, perfil diferente al de esta, claves complejas y desactivación por no uso.

4. Las personas de terceros autorizadas a recibir este servicio deberán diligenciar el acuerdo de buen uso del servicio de acceso remoto para terceros amparado bajo las cláusulas de confidencialidad pactadas en el contrato vigente con estas firmas. En el formato se debe indicar a que servicio específico está autorizado ingresar.

5. En caso de que este servicio deba ser retirado a un usuario que ya lo percibe por traslado, cambio de funciones, retiro, etc. El Gerente de área debe informar la novedad a la Gerencia de tecnología para deshabilitar el servicio.

6. Si termina la vigencia de un contrato con un tercero, de inmediato el jefe responsable del servicio debe enviar la novedad a tecnología.

5.10 ALMACENAMIENTO DE ARCHIVOS CON INFORMACIÓN DEL NEGOCIO

1. Toda carpeta compartida para almacenar información de un área en particular o un grupo de trabajo y/o proyecto debe tener un dueño quien será el responsable por solicitar este servicio al área de sistemas.

2. La lista de usuarios autorizados a acceder esta carpeta y el rol de acceso (Lectura, escritura, etc.) debe ser solicitado al área de tecnología indicando la novedad: Incorporar un usuario, cambiarle su rol sobre la carpeta o retirarle el acceso a la misma. Es responsabilidad del jefe inmediato anunciar con anticipación rotación de personal por ingresos, traslados o retiros.

3. La Gerencia de tecnologia debe garantizar que no haya carpetas de dominio público, salvo las autorizadas.

4. Todo archivo (xls, doc, zip, ppt, etc...) almacenado en disco interno de su Pc y/o en carpetas compartidas de la red y que contenga información sensible del negocio debe ser almacenado con contraseña para evitar accesos no autorizados o fuga de información y entregar dicha clave a la Gerencia de tecnología.

5. Todo archivo almacenado en carpetas compartidas de red, el área de tecnología le tomará copia de seguridad de acuerdo a las políticas definidas en la toma de backups.

6. Todo archivo que repose sin ser modificado por un espacio mayor a 3 meses en las carpetas compartidas será respaldado por el área de tecnología al dispositivo instalado en la filial (DVD's, CD's; cintas) y eliminado del acceso compartido para optimizar el uso de los recursos. (Esto con autorización del dueño del activo de información).

7. Los administradores de servidores de archivos deben guardar total confidencialidad acerca de la información almacenada en los discos de red de los usuarios y en ningún caso podrán acceder a esta información, salvo previa consulta y aprobación del Gerente.

8. El usuario no está autorizado para compartir carpetas de su disco interno de su Pc.

9. El usuario de PC debe coordinar con sistemas la copia de seguridad que requiera de sus archivos locales para garantizar la disponibilidad de esta información ante daño y o robo de equipos en especial portátiles.

10. En ningún disco local o de red el usuario podrá guardar y/o descargar información que no corresponda a las labores inherentes a su cargo. En especial Software y/o archivos bajados de Internet como mp3, juegos, fotografías, videos etc... que incluso pueden contener peligrosos virus. El área de sistemas podrá auditar en cualquier momento el cumplimiento de esta medida.

5.11 USO DE PCS, MEDIOS DE ALMACENAMIENTO

1. Las computadoras como activos de la compañía que contienen información del negocio deben tener asignado un responsable quien debe velar por el buen uso del recurso y la confidencialidad de la información allí contenida y/o compartida. Dispositivos de almacenamiento auxiliares como cámaras digitales, celulares, discos removibles, periféricos de almacenamiento USB, computadoras de mano o agendas electrónicas no se encuentran autorizadas para el ingreso a la compañía salvo autorización expresa y escrita de su Jefe Inmediato.

2. NO está autorizado salvar información de la compañía en equipos de propiedad de los colaboradores o visitantes. La información propiedad de IGS solo puede ser almacenada en dispositivos autorizados por la misma. Casos particulares deben ser revisados con tecnología de los países y reportar esto al área de Sistemas.

3. El Jefe de área es responsable de asignar el dueño de la máquina que deben ser solicitadas al área de Sistemas con la relación del SW que requiere el puesto de trabajo y las debidas aprobaciones. Sistemas configurará el Hardware que sea necesario y que cumpla con las funciones asignadas a esa máquina. Dispositivos de almacenamiento auxiliares deben recibir el mismo tratamiento.

4. El contenido de la información almacenada por el usuario en el PC o dispositivos auxiliares asignados bajo su responsabilidad debe ser exclusivamente de las labores inherentes a su cargo.

5. Ningún usuario podrá retirar y/o enviar información de IGS en medios de almacenamiento auxiliar o magnéticos, escritos y/o servicios de mensajería o transferencia electrónica sin estar debidamente autorizado por escrito por su Jefe Directo, Gerente a cargo.

.

6. Sistemas debe entregar los Pc´s y en especial los portátiles con las claves de encendido, de disco duro y del protector de pantalla activadas para garantizar la confidencialidad de la información en caso de pérdida y/o robo. Debe el usuario activar su contraseña para el refrescador de pantalla para cuando se ausente de su puesto de trabajo por lapsos pequeños de tiempo. Para ausencias prolongadas o salidas de oficina el PC debe quedar apagado.

7. El retiro de portátiles de las instalaciones debe obedecer exclusivamente a labores inherentes al cargo y con la debida autorización de su jefe inmediato y siempre que exista cifrado de disco y un respaldo de su información en las instalaciones de la Empresa.
8. El uso de las unidades grabadoras de CD-RW no será masivo y debe estar centralizado en lo posible en las áreas de Sistemas. El usuario que requiera de este servicio esporádicamente deberá ser aprobado por su Jefe directo que garantice que la información a grabar en CD/DVD está debidamente autorizada.

9. El área de Sistemas debe ejercer estricto control en el uso de medios que permitan la reproducción de información (grabador CD, DVD, Cinta, etc.).

10. En lo posible toda computadora debe tener desactivada toda unidad de, USB o CD-RW a excepción de los puestos en que los usuarios por procesos requieran de este dispositivo previa solicitud del Gerente Responsable.

11. Sistemas debe velar por que el antivirus este activo en toda Pc y actualizado. Si el usuario detecta que no está actualizado o este opera mal debe reportarlo de inmediato al área de tecnología con copia al oficial de seguridad de la información.

12. No está permitido que un tercero conecte su Pc o laptop a la red corporativa de IGS, por cualquiera de los medios disponibles como: la red LAN ethernet, Radiofrecuencia, wireless, RAS o VPN. En caso de ser estrictamente necesario esta actividad deberá ser coordinada y realizada con el área de Sistemas para definir y controlar este acceso así como el estado de virus del Pc del visitante. Esta norma aplica de Igual forma para equipos de propiedad de los empleados y se debe mantener un registro del evento.

13. El área de administración debe registrar el ingreso y retiro de equipos de cómputo de visitantes o de empleados indicándoles a sus portadores la norma anterior.

14. Todo retiro de computadoras, reportes, medios magnéticos, etc. deben ser autorizados por escrito por su jefe inmediato y las áreas de sistemas y administrativa, explicando las razones del retiro y registrándolo en la bitácora o mesa de servicio.

15. IGS proveerá de una cadena de seguridad (de ser posible) para el equipo portátil, así como deberá mantener todos los equipos asegurados.

5.12 POLÍTICAS EN EL USO DE LAS IMPRESORAS

1. Toda funcionario de IGS debe comprometerse con la tendencia del "0 papel", es decir, que el envió de documentos a imprimir debe ser absolutamente justificado.
2. Todo funcionario de IGS debe comprometerse con la confidencialidad que se debe guardar con la información del negocio evitando su exposición y/o fuga en los sitios de impresión.
3. Todo archivo enviado a la impresora que contenga información sensible del negocio debe ser retirado de la bandeja de salida de forma inmediata por el usuario dueño del reporte.
4. El área de Sistemas velara por el buen uso del recurso, cuya responsabilidad principal será recolectar al fin del día las impresiones que han sido abandonadas en la máquina para efectuar una Auditoria y generar un reporte al Gerente con el número de hojas abandonadas, el tipo de Información impresa y pasar esta papelería a destrucción.
5. El usuario apoyado por el área de Sistemas debe configurar sus impresiones usando la calidad de impresión adecuada y por ambas caras para optimizar el uso de los recursos de tóner y papel.
6. Los archivos que envíe el usuario a impresión deben contener exclusivamente información relacionada con labores inherentes a su cargo.

7. Sistemas deberá garantizar a través de estadísticas el uso de este recurso y mediante auditorias periódicas, el buen uso del mismo.

5.13 BUENAS PRÁCTICAS EN EL USO DE INTERNET

1. El acceso a Internet es un servicio controlado, autorizado y auditado y sólo tendrán acceso a los servicios quienes a través de solicitud escrita indicando el uso que se dará a esta herramienta y bajo la responsabilidad del Jefe inmediato (primer aprobador) y del Gerente del área (segundo Aprobador) obtengan la correspondiente autorización

2. Es responsabilidad del usuario NO difundir ni facilitar su usuario y contraseña a otra persona. Esta clave es personal e intransferible.

3. Es responsabilidad del usuario utilizar los servicios de forma racional y para uso exclusivo de las labores inherentes a su cargo.

4. La información consultada en cualquier horario de trabajo a través de Internet debe apoyar directamente las funciones relacionadas con el campo de responsabilidad laboral del usuario y o servir como herramienta para desempeñar sus funciones.

5. Es responsabilidad del usuario verificar que siempre esté activo el antivirus y de revisar la Información que baje de Internet a su máquina a través del correo o del navegador antes de ser abierta y/o distribuida.

6. Es responsabilidad del usuario NO difundir información que NO apoye directamente actividades laborales.

7. Es responsabilidad del usuario NO navegar por sitios no deseados o de dudosa calidad registrados por el ICRA (Internet Content Rating Association l). http://www.icra.org/about/

8. Es responsabilidad del usuario consultar al área de Sistemas en cualquier actividad que involucre bajar freeware, shareware (software libre, demostraciones temporales) y/o software licenciable para pruebas, evaluaciones, demostraciones. Cualquier instalación de este tipo sin el Visto Bueno mencionado, no está autorizado debido a que las leyes que hoy rigen el licenciamiento de software son de estricto cumplimiento por parte de la compañía. cualquier acción de este tipo que sea emprendida contra la empresa por esta condición mencionada será responsabilidad del usuario.

9. Es responsabilidad del usuario reportar de inmediato al área de sistemas cualquier anomalía que detecte en el uso de esta herramienta.

10. Es responsabilidad del usuario cuando se retire por un período de tiempo considerable de su puesto de trabajo, estando conectado a la red, desconectar la sesión con el fin de evitar accesos de personas no autorizadas.

11. Es responsabilidad del área de sistemas brindar la administración, control y auditoria de los servicios que preste con relación a Internet así como de emitir reportes del uso que las personas autorizadas del área le estén dando a estas herramientas registrando básicamente: tiempo de uso, páginas visitadas, etc... con el fin de tomar las acciones necesarias para garantizar la seguridad, buen uso del servicio y el mejor desempeño de los recursos

12. En cualquier momento la Gerencia de tecnología junto con el oficial de seguridad de la información podrá auditar cualquier equipo de la compañía para verificar que los citados puntos anteriores no sean violados.

5.14 RESPALDO Y RECUPERACION DE LA INFORMACION

INTEGRAL GROUP SOLUTION SAS establece las siguientes normas para su aplicación:

El proceso de respaldo se realiza a través de procesos bash.

Composición:
Bases de datos servicios:
Base de datos a respaldar: cogestion.sql,
Formato de almacenamiento: cogestion_aaaammdd_hhmm.sql.gz

Base de datos venta. :
Base de datos a respaldar: asterisk.sql,
Formato de almacenamiento: asteriskco_aaaammdd_hhmm.sql.gz

Audios de grabaciones de servicios.
https://IP/grabacionesCAT/igsco/cliente/
user: pass:

Audios de grabaciones de venta.
https://IP/grabacionesTMK/igsco/cliente/
user: pass:

Frecuencia

El respaldo de datos es completamente automático y continuo, en forma diaria, a través de procedimientos programados entre los servidores destino origen mediante relaciones de confianza establecidos entre ellos..

Ejemplo Script de respaldo:

```
#!/bin/sh
echo 'Iniciando backup .....'
cd /backups/bases
fecha=`/bin/date +%Y%m%d_%H%M`
/usr/bin/mysqldump -u msadminbd -pxxxxxxx -hIP --opt co > cogestion_$fecha.sql &&
      echo
      'Empaquetando'
      gzip -f
      cogestion_$fecha.s
      ql  rm
      cogestion_$fecha.s
      ql &&
echo 'Backup Finalizado Satisfactoriamente
```

Seguro

La conexión entre los servidores se realiza a través de llaves RSA, las bases de datos se encuentran cifradas y/o protegidas con contraseña.

Remoto

Los datos deben quedar alojados en los servidores de respaldo fuera de la empresa, en este caso quedan en servidores en un centro de datos alterno.
Adicionalmente tenemos un respaldo en NAS que se almacena en el centro de datos de la oficina.

Mantenimiento y prueba de respaldos.

Mensualmente se realiza la prueba de los archivos de respaldo, simulando el procedimiento de recuperación y puesta en marcha de un sistema de pruebas, se verifica el acceso a los datos y la integridad de los mismos.

5.15 ACCESO A REDES

INTEGRAL GROUP SOLUTION, tiene sus redes distribuidas, para los accesos al personal interno y externo, así mismo existen redes a las que está restringido su ingreso sin permiso previo por el área de TI. Los usuarios y contraseñas para el ingreso al sistema son personales e intransferibles y es responsabilidad de cada empleado el uso de la misma.

5. NORMAS

INTEGRAL GROUP SOLUTION SAS establece las siguientes normas para su aplicación:

a. Manejo de usuarios y accesos al sistema

Para cada empleado el acceso al sistema será por medio de un usuario y una contraseña inicial la cual deberá ser cambiada por el empleado de forma inmediata. El área de TI se encargará de gestionar los usuarios y entradas al sistema, también configurará los permisos dependiendo de la gestión a realizar por el empleado enmarcada en la matriz de roles y perfiles del área de tecnología.

El área de talento humano deberá informar al área de TI los empleados que ingresan y salen para hacer la respectiva gestión de creación y cancelación de los accesos al sistema.

b. Autorización al Acceso a redes

Todos los equipos de cómputo están conectados a la red por medio de cable y el servicio de WIFI solo tiene acceso el personal autorizado y los visitantes deberán registrarse en un red de visitas que contiene restricciones adicionales, y solo bajo autorización se registrará su “mac address” vía firewall para tener ciertos permisos.

Los métodos de acceso a las aplicaciones para el personal remoto de la empresa, debe ser única y exclusivamente por medio de los datos asignados en su dispositivo de trabajo, esto quiere decir que está prohibido conectar el dispositivo a cualquier red de WIFI, cada usuario tendrá acceso a la información que corresponde del área a la cual fue contratada.

5.15 TRANSFERENCIA DE INFORMACIÓN

para mitigar el riesgo de fuga o pérdida de información restringida en actividades de transferencia de información, establece controles

- Control en el transporte de Información en discos duros: En el caso de transporte de información restringida en discos duros se debe realizar espacios cifrados en el disco.
- Control en el envío de información a través de correo electrónico: Se debe evitar enviar información restringida a través de correo electrónico.
- Establecimiento de acuerdos de confidencialidad de la información con clientes, proveedores y personal donde se establece la responsabilidad legal y consecuencias.
- No se deben dejar mensajes en buzones de voz que puedan reproducirse o copiarse por personas no autorizadas.

La información de **INTEGRAL GROUP SOLUTION** y de sus clientes no debe ser almacenada en dispositivos móviles o de almacenamiento externo, en el caso que sea necesario, deberá cifrarse la información.

5.16 PROTECCIÓN DE INFORMACIÓN DIGITAL MEDIANTE CIFRADO.

se identifican los escenarios en donde los controles de cifrado de información son aplicables. De manera extensiva, en aquellos casos en donde sea aplicable la protección de información por medio del cifrado, también se deben especificar las responsabilidades respecto al manejo adecuado de las llaves o mecanismos de cifrado utilizados.

a. Se hace explicita la implementación de métodos de cifrado de datos en las telecomunicaciones que se establezcan bidireccionalmente con terceras partes, según sea acordado en los procedimientos de transferencia de información, preferiblemente haciendo uso de redes virtuales privadas (VPN) y transferencia segura de archivos (FTPS).
b. En concordancia con los mecanismos y procedimientos de cifrado de la información que son implementados en la empresa, la gestión de llaves de cifrado, que son utilizadas en los diversos niveles y escenarios identificados para la protección de la información se expresa en el procedimiento vigente para la protección digital de la información.

c. Las llaves o claves de cifrado de la información deben ser “de uso restringido”, es decir que solamente los empleados autorizados conocerán el contenido y ubicación de esta información en cada uno de los procesos de la empresa y áreas críticas en donde sean utilizadas las herramientas de cifrado.

5.17 ESCRITORIO LIMPIO Y PANTALLA DESPEJADA.

escritorio limpio

Todo empleado o funcionario es responsable por el cumplimiento de las normas y estándares contenidos en este documento, además, tiene la obligación de informar, a través a TI si observan incumplimiento de esta política por parte de otras personas, o informar al área de seguridad de la información en caso de que se esté exponiendo la confidencialidad, integridad y disponibilidad de la información. La omisión de esta norma se considera incumplimiento de las obligaciones laborales por parte del trabajador.

Pasos para crear una política de escritorio limpio. A fin de promocionar una política de escritorio limpio, recomendamos la organización de la oficina siguiendo estos pasos para dar el mejor ejemplo:

PLANIFIQUE por la mañana. Conserve sobre su escritorio sólo las cosas que necesita para su día de trabajo. Comience cada día con algunos minutos de planificación de manera que pueda organizar los documentos que necesita para el trabajo inmediato. Archive cualquier otra carpeta o documento.

PROTEJA la información siempre que abandone su escritorio. De tener que abandonar su escritorio para asistir a reuniones o tomarse un descanso, verifique si hay información sensible sobre su escritorio y colóquela dentro de una carpeta o fuera de su escritorio. Asegúrese de activar el protector de pantalla con protección de contraseña de su computadora.

PRESERVE Y GUARDE todo al final del día. Cuando abandone su escritorio al final del día, no deje documentos sobre el. A fin de conservar la seguridad de la información, tanto de su cliente como del empleado, es fundamental que archive sus documentos o los guarde bajo llave. Si adquiere el hábito de despejar la superficie de su escritorio todos los días antes de irse, usted disfrutará los beneficios adicionales de la productividad resultantes de una oficina limpia a primera hora de la mañana

6. ANEXO.

N/A

Control de Cambios

Revisión	Ítem Modificado	Objeto de la Modificación
Rev. 00	Creación del documento	
Rev. 01	Revisión del Documento	

Giovanni Perea	Mario Pomares	Russell Aparicio
Elaboró/Controló	**Revisó**	**Aprobó**