ÍNDICE

1. OBJETIVO

Establecer políticas de trabajo para Tecnología de la Información, con el fin de mantener la confiabilidad, disponibilidad e integridad de la información de la empresa.

2. ALCANCE

Las presentes políticas tienen como alcance todos los activos informáticos que hacen parte del alcance del marco de trabajo de Flores el Trigal S.A.S.

3. CONDICIONES GENERALES

Una de las funciones del área de Tecnología de la información es soportar toda la operación de la Empresa, fundamental para la custodia y administración adecuada de la información. Por esta razón, T.I debe hacer un esfuerzo especial en la administración de los activos informáticos para garantizar así, la seguridad de toda la información que en estos reside, se transporta o se respalda.

El tiempo de guarde del CCTV es de mínimo 15 días.

4. POLITICA SISTEMAS DE INFORMACION

Establecer las directrices de seguridad de la información necesarias para las diferentes actividades del área de Tecnología de la información, tiene como alcance todos los activos informáticos que hacen parte del alcance del marco de trabajo de Flores el Trigal S.A.S.

4.1. PLAN DE CAPACIDAD

Se deben revisar periódicamente Quien y cada cuanto las demandas de capacidad tecnológica y realizar proyecciones de los futuros requerimientos con el fin de garantizar la capacidad de procesamiento y almacenamiento de la información. Estas proyecciones deben tener en cuenta los nuevos requerimientos del negocio, los requerimientos de almacenamiento de información y las tendencias actuales para determinar un adecuado plan de crecimiento de los sistemas de información propiedad de Flores el Trigal.

4.1.1. Los custodios de los equipos deben verificar la utilización de los recursos del sistema, incluyendo procesadores, almacenamiento principal, almacenamiento de archivos, impresora, sistemas de comunicación y otros medios de entrada y salida. Éstos deben identificar las tendencias de uso, particularmente en relación con las aplicaciones comerciales o las herramientas de sistemas de información.

4.2. PROTECCION CONTRA EL CODIGO MALICIOSO

El software de antivirus debe estar instalado, habilitado y actualizado en todos los sistemas de la empresa como: equipos de escritorio, equipos portátiles o móviles y en todo equipo donde sea posible realizar la instalación del software. Debe garantizarse que se encuentren activos los registros de auditoría que este tipo de software genera.
El software de antivirus debe ser instalado, mantenido y actualizado por lo menos una vez a la semana en todos los equipos de cómputo y no debe ser removido o deshabilitado por parte de usuarios finales. Los cambios no autorizados sobre la configuración del sistema antivirus en un computador personal y/o equipo móvil están prohibidos.

4.2.1. No debe accederse a ningún medio de almacenamiento externo como Memorias USB, Discos Externos, etc., si este no ha sido explorado previamente con la versión más actualizada de software antivirus.

4.2.2. La exploración de código malicioso debe ser realizada como mínima una vez por semana en todas las estaciones de trabajo. Para equipos que no están conectados permanentemente (portátiles) debe realizarse como mínimo una vez por mes.

4.2.3. Los usuarios no deben abrir archivos adjuntos en los correos electrónicos si estos no son recibidos desde una fuente conocida. En caso de requerir el archivo enviado, debe explorarse con el antivirus para descartar la presencia de código malicioso. Si los colaboradores detectan un archivo adjunto sospechoso deben informar a los funcionarios de Sistemas, eliminarlo de su equipo y vaciar la papelera de reciclaje.

4.2.4. Los usuarios no deben visitar sitios de dudosa reputación o abrir enlaces a sitios web desconocidos enviados a través de correo electrónico.

4.2.5. Los usuarios, contratistas y terceros que tengan acceso a la red, no deben descargar ni instalar software o archivos de ninguna fuente desconocida o sospechosa o sistema externo. Todos los archivos y/o programas descargados de fuentes confiables a través de internet pero que no proceden de la empresa o Gr Chía, deben ser revisados con un software antivirus antes que sea ejecutado el programa o el archivo sea utilizado.

En caso de requerirse la restauración de archivos de una copia de respaldo en el ambiente de producción, estos deben ser explorados con la versión más actualizada de software antivirus.

4.2.6. Los equipos que no tienen un sistema antivirus o estén contaminados con virus, deben ser desconectados de la red de la empresa.

4.2.7. Ningún usuario debe escribir, generar, compilar, copiar, recolectar, propagar, ejecutar o tratar de introducir código malicioso diseñado para auto-replicarse, dañar o de alguna manera entorpecer el desempeño de cualquier computador, red o activo de información de la empresa.

4.2.8. Cualquier colaborador que sospeche que ha sido infectado por software malicioso (Virus, spyware, etc.), debe inmediatamente desconectarlo de la red y contactar a los funcionarios de Sistemas. En ningún caso el colaborador debe intentar remover el código malicioso por su propia cuenta.

4.3. COPIAS RESPALDO

4.3.1. Debe respaldarse periódicamente toda la información confidencial, sensible y/o crítica contenida en los sistemas de computación y las redes de la empresa.

4.3.2. El área de Tecnologías de la Información debe proveer la infraestructura de copias de respaldo adecuada que permita recuperar los datos y software en caso de un desastre o falla en los medios de almacenamiento.

4.3.3. Las copias de respaldo y los procesos de almacenamiento y recuperación deben ser consistentes con los Planes de Continuidad del Negocio.

4.3.4. La frecuencia y el tipo de copias de respaldo deben determinarse de acuerdo con la importancia de la información y el riesgo aceptable calificado por el dueño de la información.

4.3.5. Las copias de respaldo deben ser realizadas en medios confiables y deben ser almacenadas en un sitio seguro lejano de los sistemas en producción. Para la realización de copias de respaldo no deben utilizarse servicios gratuitos disponibles en Internet o servicios en la nube sin estar respaldados por un contrato formal de prestación de servicios.

4.4. SEGURIDAD DE REDES

4.4.1. La gestión de la red debe realizarse de forma segura a través de protocolos y procedimientos confiables, que garanticen la confidencialidad, integridad y disponibilidad de la información que se encuentra en la red o en uno de sus elementos o hace tránsito por esta.

4.4.2. Todos los dispositivos de red deben pasar por un procedimiento de aseguramiento basado en las recomendaciones del fabricante, estándares de la industria y requisitos del negocio antes de su entrada a producción.
Todos los dispositivos de red de la empresa deben poseer una contraseña única u otros mecanismos de control de acceso. La gestión de los dispositivos de red debe realizarse si estos lo permiten a través de protocolos seguros como lo son SSH, IPSEC, SSL.

4.4.3. El tráfico entrante y saliente a través de todos los dispositivos de red debe ser limitado a través de listas de acceso u otro tipo de controles permitiendo solo el autorizado de acuerdo con los requerimientos del negocio. Cualquier otro tráfico que no se encuentre explícitamente permitido debe ser bloqueado.

4.4.4. Si el uso de servicios inseguros (FTP, Telnet, rlogin, etc.) es permitido debido a requerimientos del negocio o limitantes técnicos en los sistemas, deben implementarse controles compensatorios que permitan reducir el riesgo de su uso.
Deben utilizarse dominios lógicos (VLAN), firewalls o segmentos físicos para segmentar los diferentes flujos de tráfico que viajen desde y hacia los diferentes sistemas que componen la topología de red de la empresa.

4.4.5. Cualquier servidor de producción o sistema conectado a una red pública IP o red no confiable, debe ser ubicado en una zona desmilitarizada (DMZ) separada de las redes internas de cualquiera del clúster de Empresas en la cual el tráfico público es restringido por los enrutadores y/o Firewalls.
Las conexiones directas desde internet hacia un Sistema en Producción deben pasar a través de un Firewall o enrutador que filtre las conexiones.

4.5. FIREWALLS E IPS

4.5.1. Todos los firewalls conectados a cualquier red pública (Internet) deben ser configurados de tal forma que cada servicio por defecto se encuentre deshabilitado (Principio de negación Predeterminada).

4.5.2. Los privilegios para modificar las configuraciones, conexiones y los servicios sustentados por los Firewalls e IPS se deben restringir a unas pocas personas con adiestramiento técnico y con necesidad de dichos privilegios.

4.6. DISPONIBILIDAD DE LA INFRAESTRUCTURA

Todo dispositivo conectado a la infraestructura de la empresa debe ser sincronizado a través de un servidor centralizado de “Network Time Protocol” que sincronice todos los equipos de la red interna. Debe asegurarse la disponibilidad de la infraestructura de red lo más cercano al 100% del tiempo durante las 24 horas del día, los siete días de la semana a través de la utilización de arquitecturas de alta disponibilidad y mecanismos a prueba de fallos. Los tiempos de caída deben minimizarse a través de alertas de eventos en tiempo real durante las 24 horas del día. Los enlaces de comunicación críticos deben ser diseñados para permitir la comunicación a través de múltiples rutas físicas.

4.7. CONEXIONES A REDES EXTERNAS

4.7.1. Debe mantenerse un inventario actualizado de todas las conexiones hacia redes externas.

4.7.2. Esta documentación debe ser considerada como confidencial. La documentación solo debe ser accesible para el personal del área de TI y por parte de auditorías externas.

4.8. ASEGURAMIENTO DE ACTIVOS

4.8.1. Todo activo informático de la empresa, debe pasar por un proceso de aseguramiento con el fin de garantizar la seguridad de la información en función de su disponibilidad, confidencialidad e integridad y de acuerdo con la sensibilidad de la información que en estos reside, procesa, comparta o transporta. Este aseguramiento debe realizarse antes de instalar el activo en producción. El proceso de aseguramiento debe contemplar como mínimo, pero no limitarse a las siguientes actividades:

- ✓ Instalación de los últimos paquetes, parches y actualizaciones de sistema operativo, seguridad, aplicación o bases de datos de acuerdo con lo publicado por el fabricante del sistema.
- ✓ Eliminación de servicios, puertos, cuentas, privilegios, scripts, drivers, subsistemas, sistemas de archivos, servicios web innecesarios.
- ✓ Cambio de contraseñas por defecto generadas por los procesos de instalación del sistema.
- ✓ Cambio en los nombres de las cuentas por defecto generadas por los procesos de instalación del sistema.
- ✓ Instalación del programa antivirus autorizado por GR CHIA.
- ✓ En caso de que el sistema lo permita debe activarse el Firewall Personal que posee el Sistema Operativo.

- ✓ Activación de disco duro como primer medio de arranque.
- ✓ Activación de protector de pantalla protegido con contraseña.
- ✓ Bloqueo de acceso al sistema de cuentas tipo invitado, genéricas o vacías (“null”).

4.8.2. Para aplicaciones web deben garantizarse adicionalmente las siguientes actividades:

- ✓ Validación de parámetros de entrada para evitar que usuarios puedan modificar comandos y consultas que generen ataques tipo inyección (Por ejemplo “SQL Injection”).
- ✓ Validación de parámetros de entrada para evitar que la aplicación acepte archivos o nombres de archivos por parte de los usuarios.

4.8.3. Se debe realizar un aseguramiento continuado de los activos de la empresa con una periodicidad no mayor a seis (6) meses. Este proceso debe ser el resultado de actividades como los análisis de riegos, escaneo de vulnerabilidades y auditorías internas y externas.

4.9. COMPUTACIÓN MÓVIL

4.9.1. Los equipos portátiles (computadores, celulares, tabletas, etc.), no deben ser usados como herramientas de negocio de la empresa, a menos que hayan sido configurados con los controles necesarios para garantizar la seguridad de la información.

4.9.2. Los requerimientos de seguridad mínimos que deben establecerse para el uso y operación de equipos móviles propiedad de la empresa o de terceros dentro de las instalaciones son:

- ✓ Todos los dispositivos móviles pertenecientes a la empresa con permiso para conectarse a la red deben tener un único identificador como: IP estática, dirección MAC, etc.
- ✓ Dispositivos que no son propiedad de la empresa, pueden ser sujetos en cualquier instante de revisión y auditoria para garantizar que no tengan software malicioso que pueda afectar la seguridad de los activos.
- ✓ El responsable del área T.I debe tener una lista actualizada con los datos de contacto (Nombre y teléfonos) de los funcionarios que tienen asignados dispositivos móviles.
- ✓ Los derechos de acceso a la red no pueden ser transferidos a otra persona aun si esa persona está usando un dispositivo de cómputo autorizado.

- ✓ El dispositivo Móvil debe tener siempre instalado y operando un programa de antivirus aprobado por GR CHIA. El programa debe estar configurado con protección en tiempo real y recepción diaria de actualizaciones.
- ✓ El dispositivo Móvil debe tener siempre instalado y operando un Firewall Personal aprobado por GR CHIA, configurado con protección en tiempo real. El Firewall debe estar activo siempre que el dispositivo se conecte a redes no confiables incluyendo redes inalámbricas o IP públicas.
- ✓ Todas las contraseñas por defecto en los dispositivos móviles deben ser cambiadas antes de ser entregados a los funcionarios.
- ✓ Los equipos móviles de cualquiera de la empresa, así como su información nunca debe ser dejada en lugares públicos sin el debido cuidado. Las características de “suspensión” o “hibernación”, no deberían ser utilizadas cuando se encuentra el equipo portátil fuera de las instalaciones.
- ✓ Cuando un empleado utilice un avión para transportarse a otra locación, siempre debe cargar el equipo portátil como equipaje de mano y nunca debe ser enviado como equipaje en las bodegas del avión.
- ✓ Cualquier pérdida de un equipo portátil debe ser reportada de manera inmediata a la autoridad local y deben tomarse todas las medidas necesarias para recuperar la información del equipo.
- ✓ Los equipos móviles de cualquiera de la empresa son solo para el uso de los funcionarios. Familiares y terceras partes no deberían hacer uso de estos.
- ✓ No debe instalarse software no aprobado en los equipos móviles o portátiles de la empresa.
- ✓ Cualquier actividad de copia de respaldo que se realice sobre un equipo portátil o móvil, debe seguir los lineamientos estipulados en la Política de Copias de Respaldo.
- ✓ El uso de dispositivos móviles que no son propiedad de la empresa dentro de la red e instalaciones debe ser autorizado por el responsable del área de T.I.

4.10. REDES WIRELESS

4.10.1. La conexión de un Punto de Acceso o el uso de tecnologías inalámbricas no deben ser permitidas si no se realiza un análisis de riesgo para entender las amenazas y la probabilidad de que estas puedan ser explotadas y el impacto potencial sobre el negocio en caso de hacerse realidad un ataque.

4.10.2. Los siguientes son requerimientos básicos para garantizar la seguridad en las redes inalámbricas:

- ✓ Se deben utilizar las últimas versiones de los protocolos de comunicación y seguridad para las redes utilizadas en la empresa.
- ✓ El personal involucrado en la configuración, implementación y verificación de redes inalámbricas debe ser adecuadamente entrenado en esta tecnología y conocer donde pueden reportar la perdida y/o robo de un dispositivo inalámbrico.
- ✓ Todos los dispositivos inalámbricos deber ser revisados de forma regular y sus configuraciones deben ser auditadas.
- ✓ Cualquier dispositivo de conexión inalámbrica no autorizado dentro de la red de la empresa, debe ser removido inmediatamente.

4.10.3. Todos los Puntos de acceso inalámbrico (APs) deben ser situados en aéreas físicas protegidas tales como techos o paredes que no sean accesibles a personas.

4.10.4. La información que haya sido clasificada como confidencial y que vaya a ser transferida a través de una red inalámbrica, debe ser cifrada usando algoritmos fuertes no propietarios (Ej. 128 bits o superior) y que de los cuales no se conozca vulnerabilidades que puedan ser fácilmente explotadas (Ej., WPA2 en modo empresarial usando autenticación 802.1x y cifrado AES, combinación recomendada). En caso de utilizar WPA2 en modo personal, el “passphrase” debe tener un mínimo de 8 caracteres y debe estar acompañado de un cifrado AES.

4.10.5. Los equipos inalámbricos podrán estar disponibles para los funcionarios, contratistas y visitantes siempre y cuando se cumpla con la presente política. Cualquier Punto de Acceso (AP) conectado a la red de la empresa debe ser registrado y aprobado.

5. POLITICA PARA EL CONTROL DE ACCESO

Establecer las reglas para proteger los activos de información contra el acceso no autorizado y garantizar un ambiente de seguridad adecuado que solo permita el acceso a los mismos por los usuarios autorizados de la empresa sin comprometer la seguridad de los recursos informáticos, aplica a todos los activos informáticos de la empresa que cuenten con sistemas de control de acceso.

5.1. El acceso a los activos de información de la empresa siempre debe estar autorizado formalmente por el responsable designado. Esta autorización debe contemplar la clasificación que se haya realizado al activo de información y debe limitarse a aquellas personas que lo necesiten de acuerdo con su rol y función desempeñada dentro la empresa, siempre conservando el principio del menor privilegio posible. El acceso debe ser configurado de forma predeterminada para bloquear a los usuarios no autorizados.

5.2. La empresa se reserva el derecho a bloquear, ocultar, negar o desconectar cualquier acceso a sus redes de cómputo en cualquier momento y sin previo aviso si este no ha sido previamente aprobado por el responsable designado al activo de información.

5.3. Para otorgar acceso a los sistemas de información soportados en servidores y de más equipos de cómputo, se emite desde el Área de SI de GR CHIA, allí se realizará la creación de una cuenta de usuario para cada funcionario o colaborador para el sistema de información que sea necesario. Asociado a cada cuenta de usuario se establecerá una clave (contraseña) de acceso que se asignará y la cual deberá ser de uso exclusivo y personal del funcionario o colaborador a quien le sea asignada.

5.4. De acuerdo con lo anterior, los sistemas deben proporcionar un método preciso para identificar a un usuario a través de una contraseña en un sistema de directorio y deben manejar un mecanismo fuerte de credenciales u otro mecanismo de autenticación y autorización.

5.5. Todo activo de información utilizado para el almacenamiento y/o procesamiento de información, debe utilizar un módulo de control de accesos que tenga como mínimo las siguientes funcionalidades:

- ✓ Restricción de acceso en tiempo real al sistema de acuerdo con la clasificación de la información y privilegios asignados.
- ✓ Restricción de funcionalidades del sistema, permitiendo el acceso solamente a menús, opciones o funciones requeridas para desempeñar sus responsabilidades dentro de la compañía.
- ✓ Número máximo de 10 intentos consecutivos fallidos al inicio de sesión antes que la cuenta sea bloqueada. Si una cuenta es bloqueada, solo es posible desbloquearla a través de actividades ejecutadas por el custodio o administrador del activo o de forma automática si el sistema lo permite.
- ✓ Restricción para la ejecución de comandos y utilitarios a nivel de sistema operativo. Estos deben ser restringidos de acuerdo con el perfil y permisos que hayan sido asignados.

5.6. Los usuarios son responsables de todas las actividades que sean realizadas con su identificación de usuario de red o aplicación.

5.7. Los usuarios deben finalizar sus sesiones en los sistemas multiusuario (servidores) si se van a ausentar por un tiempo prolongado.

5.8. Los permisos de acceso, lectura, escritura, modificación, actualización o borrado de activos de información, deben ser establecidos por los responsables designados de los activos. Las reglas de acceso deben ser establecidas de manera que se restrinja

a los usuarios desempeñar funciones incompatibles a su rol. La existencia de ciertos privilegios no significa que un usuario pueda estar autorizado para usarlos.

5.9. Todo usuario o sistema que establezcan conexiones remotas con los sistemas de información del SISTEMA ubicados en la red interna deben ser previamente autenticados por un Firewall o Terminador de VPN que emplee un proceso de autenticación fuerte. Los colaboradores de la empresa, contratistas y terceros no deben establecer conexiones desde redes externas hacia sistemas de información internos del sistema a menos que estos hayan sido aprobados formalmente por el responsable del área T.I.

5.10. Cuando el acceso de un tercero de la empresa no es más requerido para propósitos del negocio, el responsable del tercero debe realizar el proceso de solicitud de eliminación de cuenta y privilegios de los sistemas de información. El responsable del activo debe informar inmediatamente al custodio y/o responsable del activo para eliminar o desactivar la conexión.

5.11. Cuando un usuario es retirado de la empresa, todos los privilegios de sistema y acceso deben ser inmediatamente finalizados. La información entregada a estos usuarios debe ser devuelta o destruida. Toda información generada por los usuarios de los sistemas de información de la empresa es propiedad de la compañía y debe ser retornada a esta.

5.12. CONTRASEÑAS

Los usuarios deben seleccionar contraseñas fuertes que sean difíciles de deducir, lo cual significa que las mismas no deben estar relacionadas con la vida personal o el trabajo del usuario, como, por ejemplo, el número de placa de un automóvil, el nombre del cónyuge o fragmentos de una dirección, ni palabras incluidas en diccionarios o alguna parte gramatical tales como nombres propios, lugares, términos técnicos y jerga. Estas contraseñas deben cumplir con las siguientes características:

- ✓ Combinan letras minúsculas y mayúsculas, números y caracteres especiales
- ✓ No deben tener una secuencia básica de caracteres.
- ✓ Deben ser cambiadas cada vez que el usuario lo considere necesario debido al nivel de confidencialidad de la información que maneja.
- ✓ El área de Sistemas programará un cambio obligatorio de contraseñas dos veces al año

Los usuarios no deben construir contraseñas que sean idénticas o similares a las empleadas con anterioridad y deben abstenerse de usar contraseñas que hayan utilizado anteriormente. Las contraseñas no deben anotarse y dejarse en lugares o medios donde personas no autorizadas puedan descubrirlas.

5.13. ESCRITORIOS LIMPIOS

A menos que la información esté siendo utilizada por personal autorizado, los escritorios deben mantenerse limpios y libres de información expuesta. La información confidencial, crítica y/o sensible debe mantenerse bajo llave para lo cual la empresa, proveerá los medios de almacenamiento seguros.
En horario diferente al normal de trabajo, todos los colaboradores deben despejar sus escritorios y áreas de trabajo, de tal manera que todos los datos valiosos o sensibles se encuentren almacenados bajo llave.
Los usuarios no deben dejar desatendidos sus puestos de trabajo o terminales sin salir del sistema, se debe invocar un protector de pantalla y/o bloquear la sesión.
Debe configurarse de forma obligatoria en todos los servidores, terminales y estaciones de trabajo el protector de pantalla protegido con contraseña.
Es prohibido que los colaboradores, contratistas y terceros modifiquen las opciones del protector de pantalla establecidos por la empresa para sus servidores, estaciones de trabajo y terminales.

6. POLITICA DE GESTION DE INCIDENTES

Establecer las directrices para garantizar que los incidentes que afecten la seguridad de la información de la empresa sean reportados de manera oportuna y sean manejados de forma eficaz para minimizar su impacto en el negocio, aplica a todos los activos de información que hacen parte del alcance del marco de trabajo de la empresa.
La Gestión de Incidentes de Seguridad es crítica para proteger la información en la empresa, estableciendo y preparando una respuesta clara y oportuna, así como también estableciendo las responsabilidades y los procedimientos para el reporte y manejo oportuno de cada evento.

6.1. GESTION DE INCIDENTES

6.1.1. Es responsabilidad de cada funcionario, contratista, consultor o tercero, reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas que pueden afectar la confidencialidad, integridad y disponibilidad de los activos e información de la empresa.

6.1.2. SOLUCIÓN:

Si se sospecha que un activo informático ha sido comprometido por un atacante, este debe ser inmediatamente desconectado de todas las redes de la empresa y se deben ejecutar todas las acciones necesarias para garantizar que quede adecuadamente protegido antes de ser conectado nuevamente.

7. USO DE REDES SOCIALES

7.1. Las redes sociales no deben ser utilizadas de una manera que se incumpla con las Políticas de Seguridad de la información, el Reglamento Interno de Trabajo del sistema de empresas, el Código de Ética y Conducta, cualquier otra política del sistema de empresas, así como las leyes y regulaciones aplicables para este tema.

7.2. Los colaboradores del sistema de empresas tienen prohibido usar las redes sociales para: Infringir las prácticas y políticas de confidencialidad y los derechos de propiedad de la organización.

- Usar redes sociales en detrimento de la organización, sus colaboradores y/o terceros relacionados.
- Vulnerar los recursos de Tecnologías de la Información de la organización, los sistemas de seguridad de la información y cualquier procedimiento relevante.
- Infringir las políticas de privacidad de la organización y cualquier otra norma ética o ley aplicable.

7.3. Los colaboradores del sistema de empresas deben recordar que la actividad de las redes sociales es pública y permanente, que todo lo escrito en línea puede ser investigado hasta llegar a su autor.

7.4. Los colaboradores del sistema de empresas tienen libertad de expresar sus opiniones y participar en redes sociales. Sin embargo, con relación a la organización, los colaboradores deben cumplir con los siguientes lineamientos:

- No divulgar ninguna información confidencial de la organización.
- No divulgar ninguna información sobre la organización, un cliente o proveedor específico a menos que el área jurídica de la organización haya otorgado una autorización por escrito o dicha información esté disponible públicamente.
- No utilizar el logotipo de cualquiera de las empresas del sistema, sus marcas comerciales y otras marcas registradas, así como otra propiedad intelectual, a menos que esté autorizado por el área jurídica de la organización.
- No publicar videos, imágenes o cualquier otra reproducción escrita y/o en audio de los espacios físicos, eventos, oficinas, equipos, productos, clientes, proveedores o visitantes que violen de alguna manera la confidencialidad o privacidad de las empresas del sistema o de terceros.
- No utilizar las direcciones de correo electrónico corporativo para registrarse en redes sociales, blogs u otras herramientas en línea utilizadas para uso personal.
- Los colaboradores no están autorizados para hablar en nombre de alguna de las empresas del sistema o declarar que se ha otorgado dicha autorización. La organización no validará ni aprobará ningún contenido aportado por colaboradores que no estén autorizados formalmente por la gerencia de alguna de las empresas del sistema para hacerlo.

- Si un colaborador es contactado a través de redes sociales o cualquier medio de comunicación social para dar comentarios acerca de la organización, dicho colaborador deberá dirigir la consulta a la gerencia de la empresa y no podrá dar ninguna respuesta sin su aprobación por escrito.
- Los colaboradores que expresen su opinión sobre asuntos relacionados con los negocios del sistema de empresas deben dejar claro a los lectores en cualquier comunicación que discuta o mencione a alguna empresa del sistema, que las opiniones expresadas son solo del colaborador y no representan las opiniones de la organización.
- Los colaboradores deben aplicar su buen criterio con lo que publican y recordar que todo lo que diga puede reflejarse en la organización, incluso si incluye una exoneración de responsabilidad. La organización incentiva el actuar con profesionalismo, precisión y honestidad en las redes sociales y cualquier otro tipo de comunicaciones.
- Los colaboradores deben abstenerse de hacer declaraciones difamatorias y/o usar lenguaje malicioso, despectivo, vulgar, obsceno, amenazante y/o acosador acerca de cualquiera de las empresas del sistema, sus productos y servicios, compañeros de trabajo, gerencia, socios, clientes, proveedores y competidores, entre otros.
- Los colaboradores deben respetar la privacidad de los demás. No publicar información personal identificable o información personal confidencial sobre otros colaboradores, gerencia, socios, clientes, proveedores, competidores y/o de terceros, sin el consentimiento previo por escrito de esa persona.

7.5. Se aclara que esta política no pretende prohibir a los colaboradores ejercer sus derechos protegidos por las leyes aplicables.

7.6. Se debe tener en cuenta que cada empresa del sistema es propietaria de todas las cuentas de redes sociales utilizadas en su nombre con fines comerciales o social recluiting, incluida toda la información de inicio de sesión, las contraseñas y el contenido asociado a cada cuenta, como seguidores y contactos. Cada empresa del sistema posee toda esa información y contenido con independencia del colaborador que abra la cuenta o la use, y conservará toda esa información y contenido, independientemente de la desvinculación de la relación contractual de cualquier colaborador con las empresas del sistema.

7.7. Los colaboradores están sujetos a obligaciones de confidencialidad en virtud de los acuerdos de no divulgación, así como las políticas o procedimientos internos de la organización. Por lo tanto, los colaboradores deben tratar la información confidencial, los secretos comerciales y la propiedad intelectual de cualquiera de las empresas como información confidencial, y deben abstenerse de divulgarla a través de las redes sociales o a terceras partes.

8. CONTROL DE CAMBIOS

N°	CONTROL DE CAMBIOS		FECHA	APROBÓ
1	Emisión de la política		2019-10	Gerente
	Se realiza revisión de la Política de Tecnologías de la Información no se generan cambios.		2022-11	Gerente
2	Se complementa la política. numeral 7 Uso de Redes Sociales.		2023-08	Gerente
N°	**DESCRIPCIÓN DEL CAMBIO**	**REVISÓ**	**FECHA**	**APROBÓ**
3	En revisión anual se realiza actualización de **NUMERAL 8. CONTROL DE CAMBIOS:** En la tabla de descripción de cambios se adicionan las casillas de revisó y aprobó. Se elimina el pie de página, el cual contenía la misma información, este cambio se realiza debido a la actualización del estándar cero. No se generan cambios en la política.	Jefe SST y/o Analista SST Analista SIG	2024-08	Director Gestión Humana
4	Se realiza actualización de la matriz adicionando el tiempo de guarde del CCTV, mínimo 15 días	Jefe SST y/o Analista SST Analista SIG	2025-03	Director Gestión Humana