RGC ACTIVA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Calle 103B No.49B-41
PBX: (60 1) 742 7695
Bogotá, D.C. - Colombia
rgc@rgc.com.co / www.rgc.com.co

RGC ACTIVA

CONTENIDO

OBJETIVO

Las políticas de la Seguridad de la Información buscan establecer controles administrativos y operativos que regulen de manera eficaz el acceso de los empleados a la información en RGC Activa SAS, estableciendo lineamientos reglamentarios, orientados a proteger todos los activos de información y la tecnología utilizada para su procesamiento, frente a las amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

ALCANCE

La política aplica en todos los ámbitos de RGC Activa SAS, empleados, proveedores, contratistas, demás partes interesadas, que tengan acceso a información a través de los documentos, equipos de cómputo e infraestructura tecnológica, para el manejo de información en el Proceso de desarrollo, relacionados con seguridad y privacidad de la información.

DEFINICIONES

ACTIVOS DE INFORMACIÓN: Es un recurso o elemento que contiene información, que tiene valor para la organización debido a que es usado o interviene en alguna función directa o indirecta para RGC Activa SAS.

ACUERDO DE CONFIDENCIALIDAD: Es un documento en los que los empleados de RGC Activa SAS., o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la compañía, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

AUTENTICACIÓN: Es el procedimiento de comprobación de la identidad de un empleado o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

CANALES DE COMUNICACIONES: Corresponde al medio utilizado para la transmisión de información.

CENTRO DE CÓMPUTO: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medio ambientales adecuadas.

CIFRADO: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

CLAVES O CONTRASEÑAS: Corresponden a una serie de caracteres pertenecientes a un usuario con un login, usado con fines de identificar al empleado para la aprobación de ejecución de tareas.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CORREO ELECTRÓNICO: Es un servicio que permite la transmisión de mensajes electrónicos.

CRIPTOGRAFÍA: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

DERECHOS DE AUTOR: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

DISPONIBILIDAD: Propiedad que determina que la información sea accesible y utilizable a solicitud de una entidad autorizada.

EQUIPOS DE CÓMPUTO: Es un elemento tecnológico tangible con un propósito específico en las labores de oficina, por ejemplo: computador, la impresora, el escáner, etc.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Son las acciones que violan las disposiciones del presente manual o las políticas, las cuales pueden generar una pérdida a los activos de información enfocado a la afectación de la Confidencialidad, Integridad y Disponibilidad.

EXTERNOS O TERCEROS: Toda compañía o persona que presta un servicio para la realización de funciones especiales diferentes a las del fondo (Ejemplo: Personal de vigilancia, personal de mantenimiento, personal de aseo, Revisoría, contraloría, etc.).

HACKING ÉTICO: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

INCIDENTE INFORMÁTICO: Evento adverso, real o potencial que tiende a generar afectación a la seguridad de los sistemas de información o a las redes inesperado o no deseado. Generalmente derivado de un análisis previo de riesgos inexistente o deficiente, puede ser derivado de la ausencia de un control y tiene probabilidad de afectar las políticas de seguridad.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

LICENCIA DE SOFTWARE: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

MEDIDAS DE SEGURIDAD: Son las medidas de seguridad para proteger la información sensible y confidencial de RGC Activa SAS

MEDIO REMOVIBLE: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs, BDs, y unidades de almacenamiento USB, entre otras.

NORMA ISO 27001:2013: Es la versión del año 2013 de la norma ISO 27001 que “proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información.”

NORMA ISO 27002:2013: Es la versión del año 2013 de la norma ISO 27002 que "está diseñada para que las organizaciones la usen como un marco de referencia para seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información".

PARTE INTERESADA: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada. [Fuente: ISO 31000].

PERFILES DE USUARIO: son grupos que concentran varios empleados con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los empleados cobijados dentro de él.

POLÍTICA: Declaración general de principios que presenta la posición de la administración para un área de control definida. Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que aborden situaciones concretas.

Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías, las políticas deben ser pocas (es decir un número pequeño), deben ser apoyadas y aprobadas por las directivas de la Institución y deben ofrecer direccionamientos a toda la Entidad o a un conjunto importante de dependencias. Por definición, las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

PROPIEDAD INTELECTUAL: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

PROPIETARIO DE LA INFORMACIÓN: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

RECURSOS TECNOLÓGICOS: Son todos los elementos informáticos de los que dispone LA COMPAÑÍA para su aprovechamiento como apoyo en las funciones requeridas para la gestión del fondo.

RED: Es un conjunto computadoras y/o dispositivos interconectados mediante cables, señales, ondas o cualquier otro medio de transporte de datos, que comparten recursos.

REGISTROS DE AUDITORÍA: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la compañía. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

RESPONSABLE POR EL ACTIVO DE INFORMACIÓN: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

RIESGO: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes

(económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización) [Fuente: ISO 31000].

SISTEMA DE GESTIÓN: Conjunto de elementos que interactúan y se interrelacionan para establecer políticas y objetivos y los procesos para alcanzar dichos objetivos.

SOFTWARE: Es el término usado para nombrar a los programas y/o aplicaciones que hacen posible que el usuario pueda interactuar con el computador.

SEGURIDAD DE LA INFORMACIÓN: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información

SISTEMA DE INFORMACIÓN: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por RGC Activa SAS., o de origen externo ya sea adquirido por la compañía como un producto estándar de mercado o desarrollado para las necesidades de ésta.

SOFTWARE MALICIOSO: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

VULNERABILIDAD: Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

GENERALIDADES

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de RGC Activa SAS. con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Empresa y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

RGC Activa SAS, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.

- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de RGC Activa SAS
- Garantizar la continuidad del negocio frente a incidentes.

Esta política cimenta las bases de los objetivos del Sistema de Gestión de Seguridad de la Información junto con las políticas adjuntas, y alineadas con el alcance del SGSI, fortalecerán la cultura interna en Seguridad y permitirán identificar y proteger los activos de información mediante la asignación de roles y responsabilidades, que contribuirán a desarrollar, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI), garantizando métodos de continuidad ante incidentes que se presenten en la empresa.

Esta política será sometida a revisiones con periodicidad de una vez al año por parte de la Gerencia, o a cambios si existiesen a nivel de objetivos, en el mapa organizacional u otro suceso que pudiese afectar su propósito, tal que sea ajustada a los requerimientos apropiados.

DEBERES

En el presente documento se exponen las diferentes políticas de uso y protección de la información y elementos tecnológicos. Son complemento a la Política General de Seguridad de la Información de RGC Activa SAS y representan su visión en cuanto a la protección de sus activos de información y los de sus partes interesadas.
Por tanto, las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

COMPROMISO DEL EQUIPO DIRECTIVO

El equipo directivo de RGC Activa SAS., aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la compañía.

El equipo directivo de la compañía demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la compañía.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

RGC Activa S.A.S, establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

NORMAS QUE RIGEN PARA LA ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Normas dirigidas a: EQUIPO DIRECTIVO DE RGC ACTIVA SAS

El equipo directivo de RGC Activa SAS., debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

- El equipo directivo debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.

- El equipo directivo debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.

- El equipo directivo de RGC Activa SAS., deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la compañía.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- El Comité de Seguridad de la Información debe actualizar y presentar ante la El equipo directivo las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.

- El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

- El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

- El Comité de Seguridad debe liderar la generación de lineamientos para gestionar la seguridad de la información de RGC Activa SAS. y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

- El Comité de Seguridad debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

- El Comité de Seguridad debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de RGC Activa SAS., a fin de determinar si las políticas, procesos,

procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

- El Comité de Seguridad debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

- El Comité de Seguridad debe informar a las áreas responsables los hallazgos de las auditorías.

Normas dirigidas a: GERENCIA DE TI

- La Gerencia de Tecnología debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la compañía. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para RGC Activa SAS., tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

A continuación, se establecen las políticas de seguridad que soportan el SGSI de RGC Activa SAS.:

POLÍTICA PARA EL USO ADECUADO DE LOS ACTIVOS

El acceso a los documentos en formatos físicos y digitales mientras dure su ciclo de vida, estará determinado a la idoneidad del área o dependencia específica, y a los permisos determinados por los niveles de acceso determinados por la gerencia de RGC Activa SAS

Para el manejo de documentos cargados en la nube de la compañía, la gerencia establecerá lo parámetros para asignación de privilegios de acceso a los empleados conforme a sus funciones y competencias.

Aquellos empleados que hagan uso de información catalogada como confidencial, deberán firmar un “acuerdo de confidencialidad”, donde se comprometan a no divulgar y utilizar la información respetando los niveles establecidos para su clasificación; y violación a lo establecido en este acuerdo será considerado de manera inmediata como una falta grave y tratada como un “incidente de seguridad”.

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Los activos de información de RGC Activa SAS, serán sometidos a un proceso de identificación y posterior clasificación con el fin de establecer las opciones de protección necesarias.

La escala de clasificación de la información considerará el valor de la misma para la compañía, por lo que los controles serán más estrictos para la información de mayor valor con el fin de evitar su pérdida. En caso de una difusión, se evaluarán las razones por las cuales se deban o no realizar.

Toda información debe tener asignado un propietario, quien será la persona encargada de propender por su clasificación.

CLASIFICACIÓN	OBSERVACIONES	NIVEL DE PROTECCIÓN
Confidencial	Información propia de RGC Activa SAS acceso a sistemas de información, manuales operativos, configuración de controles, llaves criptográficas e información de cumplimiento de la ley,	Alto
Restringida	Información clasificada de clientes y empleados que solo debe ser accedida por personal autorizado para ello, previa autorización del dueño del proceso.	
Interno	Información que no debe ser conocido por el público en general y es sólo de interés de los empleados.	Medio
Público	Información de interés de personal externo a la compañía.	Bajo

POLÍTICA DE USO DEL CORREO ELECTRÓNICO

RGC Activa SAS., entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre empleados y terceros, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de la información y de quienes emplean esta herramienta.

- RGC Activa SAS podrá realizar, y sin previo aviso, auditorías sobre el uso adecuado de este recurso.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada trabajador en apoyo al objetivo misional de RGC Activa SAS.

- Las cuentas de correo corporativo se crearán, suspenderán y/o eliminarán previa solicitud escrita del dueño del proceso y el área de Talento Humano, donde se indique nombres y apellidos del empleado y proyecto al que ingresa o sale y fecha de retiro o ingreso.

- Los empleados deberán utilizar este recurso específicamente con fines corporativos absteniéndose de registrarlo en formularios de cualquier tipo de página sin la autorización explicita de la compañía.

- Se debe evitar enviar información personal o de RGC Activa SAS a buzones de proveedores gratuitos o sin autorización (Gmail, Hotmail, Yahoo, etc.…)

- Se prohíbe enviar o reenviar cadenas de correo, SPAM, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

- El envío de información **CONFIDENCIAL,** se realizará por medios seguros según el procedimiento establecido por la compañía.
- Los mensajes con remitente desconocido y sospechosos deberán ser reportados al área e infraestructura y ser considerados spam.
- Todos los mensajes enviados deberán respetar el estándar de formato e imagen corporativa definido por RGC Activa SAS y deberán conservar en todos los casos el mensaje legal corporativo.
- En caso que un empleado tome vacaciones o presente ausencia por un tiempo considerable, deberá informar al administrador para dejar un mensaje de tipo informativo, o redireccionar los correos a otra cuenta que su superior directo autorice.
- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún trabajador de la compañía, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Se prohíbe el envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

RGC ACTIVA

POLÍTICA DE USO DE LOS RECURSOS TECNOLÓGICOS

RGC Activa SAS establece las normas para el uso de recursos tecnológicos como parte de las herramientas de trabajo para uso de sus empleados y de todo tercero autorizado para hacerlo. Su uso queda sujeto a las siguientes condiciones:

- La utilización de los recursos tecnológicos deberá hacerse exclusivamente para fines comerciales operativos sin salirse del contexto de la razón social de la compañía.
- Los empleados de RGC Activa SAS son quienes cuentan con derechos exclusivos de los recursos y son responsables de su utilización y del uso de la información que contengan conforme a la Política para el Uso Adecuado de los Activos. Dichos derechos serán revocados en el momento de la terminación de su contrato o por orden de la Gerencia General.
- Los equipos de cómputo deberán ajustarse con el estándar para contraseñas establecido.
- Los computadores deben contar con un antivirus debidamente licenciado.
- Los computadores no se deben dejar manipular por personas externas a RGC Activa SAS
- Está prohibida la utilización de programas externos para interferir con las sesiones de los computadores.
- Los empleados deberán poner en conocimiento a su superior en caso de conectar medios de almacenamiento removibles de terceros no autorizados, tales como CD's, DVD's, memorias USB y discos duros externos.
- La instalación de cualquier tipo de software en los equipos de cómputo de RGC Activa SAS debe ser solicitado a Infraestructura bajo requerimiento de las necesidades laborales y con la autorización del superior inmediato.
- Los empleados que no pertenezcan al área de Infraestructura no deben realizar cambios relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla.
- Cualquier conexión remota al equipo deberá ser informada, supervisada y autorizada por El Área de Infraestructura.
- Los empleados tienen la responsabilidad de las impresiones que se envíen, y deberán recoger las que fueron impresas. Está prohibido dejar impresiones erróneas sobre la mesa, puestos de trabajo de las personas cercanas a ella, ni en la impresora.
- El uso negligente de los recursos informáticos que causen daño parcial o total a la información de la compañía será causal de terminación de contrato y dependiendo del caso, de sanciones jurídicas.
- El área de Infraestructura será responsable de verificar los controles necesarios para asegurar que sólo los empleados autorizados puedan hacer uso de los medios de almacenamiento removibles.

- Todo empleado se compromete a asegurar física y lógicamente el dispositivo o medio de almacenamiento removible y será responsable en caso de poner en riesgo la información de RGC Activa SAS

POLÍTICA DE ESCRITORIO Y PANTALLA DESPEJADA

Esta política establece buenas prácticas para el orden y la limpieza en los puestos de trabajo de los empleados de RGC Activa SAS y da cumplimiento a directrices de Seguridad de la Información que están enmarcadas, y manejan los activos de la compañía que estén a cargo de un propietario de un activo de la Información, por lo cual se dan las siguientes directrices:

- Los empleados tienen la responsabilidad de mantener sus puestos de trabajo limpios y ordenados, manteniendo los implementos necesarios para cumplir con las funciones inherentes a su cargo.
- Las comidas y bebidas se consumirán en los lugares destinados para ello.
- Las pantallas de los computadores deberán estar ubicadas de manera que personal externo a la compañía no tenga visibilidad directa.
- Cuando finalice la jornada laboral, los empleados deberán almacenar los documentos con información sensible en los lugares determinados para ello.
- La pantalla de los computadores deberá ser configurada para bloquearse a los 15 minutos de inactividad y debe requerir autenticación para desbloquearse.
- En los puestos de trabajo de los empleados deben existir medidas de seguridad física y digital tendientes a la protección de la información que impidan el acceso libre por parte de personas externas.
- Los empleados no deberán dejar desatendidos sus dispositivos móviles.
- Queda prohibido el almacenamiento de contraseñas en notas autoadhesivas o autoguardadas en los exploradores.
- Todo empleado de RGC Activa SAS está en obligación de informar cualquier incumplimiento a esta política o cuando considere que no se está cumpliendo con la confidencialidad, integridad y disponibilidad de la información.

POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Esta política brinda un marco de referencia para el control de acceso físico a las instalaciones y las áreas donde se almacena información sensible y donde se encuentren computadores con información crítica e infraestructura que soporta la operación de RGC Activa SAS

- Se prohíbe el acceso de los visitantes a las instalaciones de RGC Activa SAS por fuera de los horarios laborales establecidos, o a menos que haya un empleado que lo apruebe, quien será responsable por el visitante durante su permanencia en las instalaciones de RGC Activa SAS
- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.
- La oficina cuenta con extintores de polvo químico seco (Solkaflam), los cuales serán utilizados exclusivamente en caso de una emergencia.
- Todas las áreas de procesamiento de información clasificado como confidencial o restringido deben contar con protecciones a nivel físico y deben cubrir las necesidades en cuanto a controles de entrada físicos y protección contra amenazas ambientales. Sus correspondientes controles deben ser de acuerdo a la necesidad de aseguramiento, clasificación y valoración de los activos de información establecidos por los responsables.
- Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado. El equipo deberá estar protegido contra fallas de energía (fuentes de corriente reguladas) y otras interrupciones causadas por fallas en el soporte de los servicios públicos (Proveedor de internet alterno UNE). El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la intercepción, interferencia o daños. Los equipos de cómputo deben tener un correcto mantenimiento (dos mantenimientos preventivos por año a excepción cuando sean equipos nuevos a los cuales se les realizara la primera vez a los dos años y mantenimientos correctivos cuando se requiera) para asegurar su continua disponibilidad e integridad.
- Se deben identificar las salidas de emergencia y asignar a un brigadista, quien deberá conocer el plan de emergencias del edificio.
- Se prohíbe abandonar en las impresoras información Confidencial, una vez se haya impreso.
- Los equipos, la información o el software no se sacarán de las instalaciones de la empresa sin la previa autorización del área administrativa. Se aplicará seguridad a los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

- Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando un computador este desatendido deberá bloquearse la pantalla.

- Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.

Normas dirigidas a: DIRECCIÓN DE INFRAESTRUCTURA

Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios del área de Infraestructura autorizados; no obstante, los visitantes siempre deberán estar

acompañados de un trabajador de dicha dirección durante su visita al centro de cómputo o los centros de cableado.

El Área de Infraestructura debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la recepción de cada sede, de forma visible como se indica en el procedimiento “acceso centro de cómputo”.

El Área de Infraestructura debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un trabajador autorizado.

El Área de Infraestructura debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

El Área de Infraestructura debe velar porque los recursos de la plataforma tecnológica de RGC Activa SAS ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

El Área de Infraestructura debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

El Área de Infraestructura debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: GERENTES, COORDINADORES, JEFES DE PROYECTO Y LIDERES DE EQUIPO

Los Lideres de equipo de la Oficina que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en sus áreas.

Los Gerentes, Coordinadores y Jefes de Proyecto de la Oficina que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.

Normas dirigidas a: TODOS LOS EMPLEADOS

Los ingresos y egresos de personal a las instalaciones de RGC Activa SAS., deben ser registrados; por consiguiente, los empleados, contratistas, proveedores y terceros deben cumplir completamente con los controles físicos implantados.

Los empleados deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la compañía; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

Aquellos empleados o terceros a los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

Los funcionarios de RGC Activa SAS, contratistas, proveedores y terceros no deben intentar ingresar a áreas a las cuales no tengan autorización.

POLÍTICA DE AUTENTICACIÓN Y CONTRASEÑAS

PROPÓSITO: El propósito de esta política es establecer un estándar de generación de contraseñas seguras, la protección de dichas contraseñas y su frecuencia de cambio.

POLÍTICA: Los empleados de RGC Activa SAS deberán seguir las siguientes políticas para garantizar un adecuado control de acceso y uso de las contraseñas de acceso de computadores, sistemas de información y otros relacionados que puedan poner en riesgo la Seguridad de la Información.

- Todas las contraseñas de nivel de sistema (Usuarios de Windows, Correo Electrónico, Bases de Datos, etc.), deben ser cambiadas al menos cada tres meses.
- Los propietarios de los activos de la información serán las personas responsables de clasificar la información, determinar los controles de acceso, autenticación y utilización que se van a implementar, aprobar o denegar la solicitud de asignación de privilegios de acceso a su información y su revisión correspondiente.

- Las contraseñas son de uso personal de cada uno de los empleados de RGC Activa SAS y por ningún motivo deberán ser utilizadas por personas diferentes.
- Todas las contraseñas utilizadas deben cumplir con las condiciones descritas a continuación:
    - Mayúsculas
    - Minúsculas
    - Números
    - Caracteres especiales (e.g. #$%&/ (“! ;),
    - Para correo longitud mínima de 8 caracteres
    - Para contraseñas de cuentas de sistema y gestionadas por infraestructura, longitud mínima de 20 caracteres.
    - Para cuentas de usuarios de servidores generados por infraestructura, longitud de 10 caracteres alfanuméricos.
- Al momento de crear una contraseña no se debe incluir información personal como, por ejemplo: Nombres de Familiares, Mascotas, Meses, Ciudades, Equipos, Programas de televisión, Libros, Password, 123456, Gwerty, Asdfg, etc.…, tampoco debe estar compuesta de palabras de diccionario.
- Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico, mensajería instantánea, SMS, redes sociales o por ningún otro medio, ni con otros empleados, contratistas, proveedores y terceros.
- Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.
- RGC Activa SAS definirá e implantará controles para proteger la información propia y de sus clientes contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos.
- La solicitud de acceso a los servicios de red será autorizada por el coordinador o líder encargado, así como el nivel de acceso a la información contenida en la nube empresarial.
- El usuario debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que le sean asignados.
- Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- Cada usuario de los portales o sitios de uso de los tokens debe acceder desde su dispositivo asignado, al igual que la cuenta de usuario y la contraseña de acceso.
- Los empleados, contratistas, proveedores y terceros que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la compañía deben acogerse a lineamientos para la configuración de contraseñas implantados por la compañía.
- La dirección de Infraestructura debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- La dirección de Infraestructura debe validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a

los empleados administradores; así mismo, debe verificar que el cambio de contraseña de los empleados administradores acoja el procedimiento definido para tal fin.

Como base del correcto manejo de claves y contraseñas se presentan una serie de recomendaciones para el manejo correcto de las mismas:

- Siempre utilice contraseñas diferentes para los servicios de la compañía y sus cuentas personales no relacionadas al ámbito laboral.
- Las contraseñas nunca deben estar escritas en texto plano (jamás archivos llamados claves.txt y en el escritorio).
- Evite utilizar la opción de recordar contraseña en navegadores y programas internos.
- Bloquee su equipo cuando se levante del puesto de trabajo.
- No comparta sus contraseñas con ningún tercero, incluso si este pertenece a la organización.
- No revele las contraseñas por medios de comunicación desprotegidos como correo, mensajería instantánea, SMS, etc.

POLÍTICA DE COPIAS DE RESPALDO

RGC Activa SAS., certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo del área de Infraestructura, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la compañía velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Es responsabilidad de los usuarios de la plataforma tecnológica de RGC Activa SAS., identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación

Se debe realizar Backup en los servidores del disco del sistema una vez al día y una vez cada semana mes para almacenarla en bucket de RGC Activa SAS. Las bases de datos de RGC Activa SAS tienen backup de la siguiente manera, un backup full cada domingo semanal, un diferencial diario de lunes a sábado y un transaccional cada hora. Las backups fulles se deben almacenar todas sus versiones, las backups diferenciales de deben almacenar las ultimas dos semanas y las backups transaccionales se deben almacenar el ultimo día. Estas backups se deben almacenar en un volumen exclusivo en el servidor, en On Premises y en almacenamiento Cloud. ésta se debe resguarda al menos 3 veces, 1 de ellas en el mismo en donde se realiza Snapshot a los discos duros de tarea critica en los servidores ubicados en AWS.

Ciclo de almacenamiento de información

Frecuencia de respaldo

• Los sistemas críticos de la compañía, datos financieros, contables y de nómina, son respaldados diariamente a través de una tarea automática en la plataforma cloud C2, adicional se implementó respaldo en Glacier Deep archive.
• Los archivos de usuario y documentos de trabajo serán almacenados en el Sharepoint correspondiente al área o unidad de negocio, (no está autorizado el almacenamiento de información en los perfiles locales de los equipos).
Mecanismo de respaldo de la información que se procesa

- Se cuenta con modalidad de backup 3 - 2 – 1 para bases de datos, esto significa que se tiene almacenada en tres sitios diferentes

1. Mismo servidor (retención 15 días)
2. AWS Amazon S3 (180 días de retención y posterior a esto 5 años en AWS Glacier deep archive o de común acuerdo con el cliente)
3. NAS Onpremise (retención 15 días)

Soportes: Retención 180 días AWS S3 e indefinido o de común acuerdo con el cliente en AWS Glacier.
Adicional se cuenta con snapshoots diarios de los discos duros de los servidores productivos con una retención de 3 días
La herramienta empleada para realizar el backup de base de datos SQLServerBooster, para los soportes se emplea el ciclo de vida de la herramienta AWS S3 de Amazon.
Los tipos de backup son:

Full: Semanalmente todos los domingos
Diferencial: Diario cada 24 horas
Transaccional: Cada hora

Retención de copias de respaldo

• Documentos Contables y Financieros: Las copias de respaldo que contengan información contable y financiera deben conservarse por un período mínimo de 10 años, en cumplimiento con el Código de Comercio.
• Documentos Tributarios: Las copias de respaldo de información relacionada con obligaciones fiscales deben ser conservadas por un período mínimo de 5 años, de acuerdo con el Estatuto Tributario.
• Documentos Laborales: Las copias de respaldo de registros laborales y de seguridad social serán retenidas por un período de 5 años, alineados con la normativa laboral y de seguridad social.

• Datos Personales: Las copias de respaldo que contengan datos personales deben conservarse únicamente durante el tiempo que sea necesario para el cumplimiento de su propósito original, conforme a la Ley 1581 de 2012. Al vencimiento de este período, los datos deben ser eliminados de manera segura.

Almacenamiento de copias de respaldo

• Las copias de respaldo se almacenarán en ubicaciones seguras, tanto dentro como fuera de las instalaciones de la compañía, para garantizar la recuperación en caso de desastres.
• Los medios de almacenamiento utilizados para los respaldos deben estar protegidos con cifrado para asegurar la confidencialidad de la información.
• Se mantendrán copias de respaldo en diferentes ubicaciones geográficas para mitigar riesgos de pérdida de datos por eventos catastróficos.

Eliminación de copias de respaldo

• Las copias de respaldo que hayan cumplido con el período de retención establecido en esta política serán eliminadas de manera segura y completa para garantizar que la información no pueda ser recuperada.
• La eliminación de los datos debe cumplir con las normativas de protección de datos personales, asegurando que la eliminación sea irreversible.

POLÍTICA DE INCIDENTES DE SEGURIDAD

Todos los incidentes o eventos de seguridad ocurridos en RGC Activa SAS deberán ser reportados a la Gerencia o a quien asume el rol de Oficial de Seguridad de la Información, con el fin de determinar sus causas y responsables. Teniendo en cuenta la gravedad, se decidirá si se contacta un aliado para asistir en la investigación. Según las responsabilidades identificadas, se definirán planes de acción y se iniciarán las sanciones disciplinarias correspondientes.

Es responsabilidad de todos los empleados de RGC Activa SAS reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

RGC Activa SAS podrá por medios propios o a través de un tercero utilizar herramientas automatizadas de monitoreo y búsqueda de evidencia física y/o digital que indiquen uso no adecuado de los recursos de RGC Activa SAS por parte de los funcionarios y contratistas.

POLÍTICA DE INCUMPLIMIENTO

El cumplimiento de las Políticas de Seguridad de la información es obligatorio para todo empleado de RGC Activa SAS Todo incumplimiento a estas se considerará como un incidente de seguridad, será investigado y de acuerdo a la gravedad, se tomarán las acciones legales correspondientes.

POLÍTICA DE ACUERDOS DE CONFIDENCIALIDAD

Todos los empleados de RGC Activa SAS, como parte del proceso de contratación, deberán aceptar los acuerdos de confidencialidad definidos en sus correspondientes contratos de trabajo mediante una cláusula, la cual indica los compromisos de protección y el buen uso de la información de acuerdo a los criterios establecidos por la Gerencia.

POLÍTICA DE ELIMINACIÓN Y DESTRUCCIÓN

Para RGC Activa SAS es importante eliminar documentación clasificada como sensible, con el objeto de que la Seguridad de la Información no se vea afectada.

La información que será sometida a eliminación, y de acuerdo a su criticidad, siguiendo las recomendaciones el Decreto 805 del 24 de abril de 2013 (que modifica el artículo 56 del Código de Comercio), que indica que "*todas las compañías tienen la obligación de conservar los libros y la documentación, por los medios que le facilita la ley, por un periodo mínimo de diez (10) años, término a partir del cual cesa la obligación; por ende, nada obsta para proceder a la su destrucción, sin perjuicio que con posterioridad decidan continuar conservándolos*", será toda aquella que clasifique como obsoleta, aquella que haya pasado el período legal obligatorio de reclamaciones y aquella que carezca de valor, sometiendo su correspondiente eliminación por medio de medios y herramientas que garanticen su destrucción y borrado seguro, sea el caso.

Dichos acuerdos deberán ser divulgados con los empleados de manera oportuna.

POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

El intercambio de información clasificada como sensible entre RGC Activa SAS y terceras partes u otras compañías deberá realizarse de forma controlada y los contratos con compañías o terceros se deberán incluir acuerdos de confidencialidad de la información, acordes con el cumplimiento de la normatividad vigente nacional e internacional para el tratamiento de la información que así corresponda.

Dicha transferencia deberá establecerse de común acuerdo, definiendo los mecanismos que se van a utilizar con el fin de evitar la interceptación, copiado, modificación y/o destrucción de la información.

Los controles que se aplicarán serán los siguientes:

- Para información física, esta irá en un sobre sellado y etiquetado como Información Confidencial, utilizando medios de embalaje, de forma que esta información pueda estar protegida, si es el caso, contra golpes o daños.
- Se deberán usar servicios de mensajería fiables.
- El envío de información por medios electrónicos clasificada como sensible, y dado el caso, deberá ser enviado por medio de herramientas certificadas como correo seguro (gmail) o por medio de archivos cifrados o con contraseña.
- Si la transferencia de la información se realiza por medios extraíbles como USB y discos duros externos, ésta deberá ser cifrada mediante algoritmos fuertes y confiables.
- Los empleados de RGC Activa SAS no deberán revelar información sensible de proyectos por medios telefónicos.
- Los empleados de RGC Activa SAS deben evitar mantener conversaciones de carácter confidencial en oficinas abiertas y lugares públicos.
- La información compartida con clientes y usuarios externos se debe realizar por medio de un protocolo seguro SFTP.
- Para todos los usuarios la información debe compartirse y transferirse por carpetas de red del File Server o Unidades compartidas de Drive, a través de VPN.

La fuga de información puede ser sujeto de sanciones que podrían dar lugar a la terminación del contrato de trabajo y acciones legales, según las leyes vigentes.

POLÍTICA DE SEGURIDAD PARA VISITANTES

RGC Activa SAS adoptará medidas de seguridad para salvaguardar los principios de la Seguridad de la Información en cuanto al manejo de activos de información y garantizará una adecuada gestión de aquellos activos clasificados como Confidenciales por medio de los siguientes controles alineados a la norma ISO 27001:2013.

- Aquellos visitantes que requieran el ingreso a las instalaciones de RGC Activa SAS deberán registrarse en la recepción y esperar allí la correspondiente autorización de ingreso.
- El ingreso de dispositivos electrónicos es responsabilidad de cada proveedor de servicios, al igual que toda licencia de software que requiera.
- Como parte de la política de visitantes del edificio, todo visitante deberá portar la tarjeta de acceso en un lugar visible.
- Todo proveedor deberá dar cumplimiento a los acuerdos de confidencialidad, SGSI y demás políticas establecidas para el intercambio comercial con terceros.

- Todo proveedor deberá ser recibido y contar con acompañamiento por un empleado asignado desde su ingreso hasta salir de las instalaciones de RGC Activa SAS
- Para el intercambio de información se deberá tener en cuenta cumplir con los protocolos indicados en la "Política de transferencia de Información", garantizando de esa forma la integridad, disponibilidad y confidencialidad de la información.

Todos los proveedores de RGC Activa SAS deben aceptar los acuerdos de confidencialidad definidos, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos. Sea el caso, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de RGC Activa SAS a personas o entidades externas.
Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

El no cumplimiento de las cláusulas de confidencialidad puede ser sujeto de sanciones que podrían dar lugar a la terminación del contrato de trabajo y acciones legales, según las leyes vigentes.

POLÍTICA DE TELETRABAJO

RGC Activa SAS maneja una opción de home office para sus empleados, la cual debe cumplir con las siguientes directrices:

a) Tener una antigüedad mayor a 2 meses en la compañía.
b) Aprobación de Jefe Inmediato.
c) Aprobación por parte del departamento de Talento Humano.
d) Condiciones seguras de puesto de trabajo (Salud ocupacional - verificación por registro fotográfico)

Esta modalidad de trabajo será aprobada por su jefe inmediato, pero puede ser suspendida por, requerimiento en la operación por incumplimiento en el desarrollo de su labor y de igual manera se le dará fin al no cumplir con los requisitos ya mencionados no habiendo ningún tipo de compensación de estos horarios de Home Office.

a) Se realizará trabajo en casa máximo 2 veces a al mes
b) Por área de trabajo solo saldaran 2 personas según designación de coordinador
c) Su jornada de trabajo será la establecida como horario laboral
d) Supervisión permanente y reporte del resultado

Relación de usuarios que disponen de la opción de trabajar en remoto. Será necesario llevar un control de las personas que, por su perfil dentro de la empresa o las características de su trabajo,

tienen la opción de teletrabajar.

Aplicaciones y recursos a los que tiene acceso cada usuario. Cada empleado tendrá acceso solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo, dependiendo de su perfil dentro de la empresa. Se detallarán las aplicaciones permitidas, así como sus condiciones de uso evitando utilizar programas no controlados por la empresa. En el caso de que el empleado necesitase la instalación y uso de un nuevo *software*, este tendrá que ser previamente aprobado por el área de infraestructura de la empresa.

Acceso seguro. Para las credenciales de acceso se utilizarán contraseñas robustas y el doble factor de autenticación siempre que sea posible, forzando su cambio periódicamente.

Configuración de los dispositivos de teletrabajo. Los dispositivos utilizados por el empleado para teletrabajar serán previamente configurados por el área de infraestructura de la empresa (sistema operativo, antivirus, control de actualizaciones etc.).

Cifrado de los soportes de información. Todos los dispositivos deben almacenar la información cifrada, tanto para proteger los datos de la empresa de posibles accesos malintencionados, como para garantizar su confidencialidad e integridad.

Definición de la política de almacenamiento en los equipos de trabajo en la red corporativa. Se dispondrá de políticas que detallen a los empleados dónde deben guardar la información con la que trabajan en remoto.

Uso de conexiones seguras a través de una red privada virtual o VPN. **La implementación de esta tecnología permite que la información que se** intercambia entre los equipos de la empresa viaje cifrada a través de Internet, protegiéndola de posibles accesos malintencionados.

Aplicaciones de escritorio remoto siempre a través de una VPN. Habilitar el acceso al escritorio desde Internet no es recomendable, puesto que estas aplicaciones pueden contar con vulnerabilidades o configuraciones inadecuadas. Para ofrecer un extra de seguridad y privacidad a las comunicaciones, se debe utilizar siempre el escritorio remoto bajo una VPN. Así cuando se acceda a una cuenta por medio del escritorio remoto, primero se deberá acceder a la VPN, la cual proporcionará el acceso al escritorio remoto, haciendo el sistema más robusto.
A excepción cuando por temas de impedimento debido a una falla en la conexión VPN o en la maquina no se pueda brindar soporte al usuario se empleará la herramienta Asistencia Rápida de Windows.

Priorizar el Uso de dispositivos corporativos. Estos dispositivos cuentan con las políticas de seguridad que la empresa considera necesarias y tienen instalado el software preciso para realizar el trabajo de forma segura.

Conexión a Internet. Cuando no sea posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utiliza la red de datos móvil 4G o 5G siempre evitando la conexión a redes wifi-públicas.

Aplicaciones de teleconferencia y colaborativas. El uso de estas aplicaciones ha de estar supervisado por el equipo de infraestructura. Se usarán solo las aplicaciones permitidas y con las configuraciones establecidas que permitan un uso seguro.

En caso de presentarse calamidad personal, temas de orden público u otra eventualidad no contemplada se facilitará la posibilidad de realizar Home Office

Dichos acuerdos deberán ser aceptados como parte del proceso de contratación.

POLITICA DE INSTALACIÓN DE SOFTWARE

Propósito: Minimizar el riesgo de exposición, perdida o daño de la información de la compañía, por software malicioso, evitando a su vez posibles sanciones por el uso de software sin licenciar, indicar a los empleados, sobre los riesgos que implica la instalación de software no autorizado por RGC Activa SAS., los cuales exponen a perdida de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales.

Política

Todo software que sea instalado debe tener licenciamiento comercial, ser de licenciamiento libre (open source o free), o en su defecto la licencia debe provenir del área de infraestructura de la compañía.
Cualquier instalación de software que sea requerido por el trabajador y que no se encuentre en la lista de software proporcionado por el área de Infraestructura, deberá ser solicitada previamente por el Líder de equipo a cargo, al área de Infraestructura por medio de ticket de la mesa de servicio, para su posterior evaluación y el proceso de instalación debe ser realizado por personal calificado de la compañía.
En la adquisición de equipo de cómputo se deberá incluir el software vigente precargado con su licencia correspondiente
Todos los empleados por defecto, no podrán realizar instalación de ningún tipo de software en los equipos computacionales asignados por la compañía, a excepción de las áreas de Desarrollo y Base de Datos de RGC Activa SAS, que cuenta con privilegios para la instalación de **Librerías de desarrollo, SQL.**
Para la adquisición de Software y utilitarios, este deberá ser solicitado al área de Infraestructura quien dará su aprobación previa análisis y validación.

- El área de infraestructura dará a conocer periódicamente las tendencias con tecnología de punta vigente al proveedor de hardware y software de la compañía.

- El Área de Infraestructura será el encargado de obtener el licenciamiento de las aplicaciones solicitadas y evaluación en busca de conflictos de compatibilidad y estabilidad del sistema.
- Las actualizaciones de software proporcionados por RGC Activa SAS., se realiza de forma centralizada y en común acuerdo con los diferentes equipos, desarrollo, soporte, bases de datos, con el fin de no causar traumatismos en la operación.

- El área de Infraestructura no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

- El Área de Infraestructura controlará la instalación de software no debidamente licenciado por RGC Activa SAS., evitando el mal uso de la infraestructura disponible.

- El Área de Infraestructura será el encargado de obtener el licenciamiento de las aplicaciones solicitadas y evaluación en busca de conflictos de compatibilidad y estabilidad del sistema, para luego realizar la instalación y distribución, según corresponda.

- Se le comparte al proveedor mediante un anexo del contrato la lista de aplicaciones a preinstalar en cada equipo según el perfil y al usuario de destino.

Los usuarios, deberá considerar lo siguiente:

- Los usuarios no podrán instalar software en los equipos computacionales de la red de RGC Activa SAS.

- Los usuarios no podrán usar software que no esté debidamente licenciado y autorizado por el área de Infraestructura de RGC Activa SAS.

- Para la creación y desarrollo de documentos electrónicos de RGC Activa SAS., deberá utilizar software debidamente licenciado.

- El software que no ha sido facilitado por RGC Activa SAS., deberá ser solicitado y aprobado por el Coordinador de Proyecto a cargo. Posteriormente analizado e implementado por el área de Infraestructura.

USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

Propósito: Minimizar el riesgo de exposición, perdida o daño de la información de la compañía, por software malicioso o personas no autorizadas.

Política

Ningún trabajador de RGC Activa SAS, podrá instalar o conectar al computador de escritorio, computador portátil y demás recursos informáticos asignados, elementos adicionales a los entregados con estos. Dichos elementos, incluyen, pero no se limitan a: cámaras web, cámaras digitales, grabadoras de sonido, impresoras, escáner, reproductores multimedia, puntos de acceso inalámbricos, dispositivos móviles, etc. En caso de requerir el uso de cualquier elemento adicional, deberá solicitar autorización por medio de un ticket a la mesa de servicio del área de infraestructura.
Los empleados no deberán usar medios de almacenamiento no autorizados o personales para el manejo de la información, donde se incluyen, pero no se limitan a: disquete, memorias USB, memorias flash directamente o a través de dispositivos móviles, CD's, DVD's, BDs, discos externos, que no sean de propiedad de RGC Activa SAS, y que no hayan sido entregados con fines y autorización específicos.

Los funcionarios de RGC Activa SAS. y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de RGC Activa SAS. En caso de requerirse alguno de estos dispositivos, se deben solicitar a modo de préstamo al área de infraestructura.

Una vez se termine de realizar la labor requerida con el dispositivo se debe eliminar toda la información contenida en el mismo, realizar una limpieza con un software de antivirus y retornarse al área e infraestructura.

Los empleados de RGC Activa SAS., y sus contratistas, proveedores y terceros son responsables por la custodia de los medios de almacenamiento institucionales asignados.

Los empleados de RGC Activa SAS, y sus contratistas, proveedores y terceros deben acoger las políticas de uso de los periféricos y medios de almacenamiento, de igual forma no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por el área de Infraestructura.

POLITICAS DE USO DE INTERNET

Esta política dictamina que los privilegios de acceso a Internet serán asignados conforme a la necesidad y funciones de los empleados de RGC Activa SAS con lo cual se definen las siguientes condiciones de uso. Cualquier propósito ajeno a las funciones estrictamente laborales serán restringidas. Los equipos que cuentan con internet pueden ser sometidos a auditorías sin previo aviso con el fin de garantizar el buen uso de este.

PERFILES DE NAVEGACION

La política de navegación se aplica mediante una directiva general de la cual existen unos perfiles de navegación aplicados a los grupos de usuarios según el caso.

Navegación: (Infraestructura) Este perfil se le aplica restricciones de conteo o advertencia, mínimas (narcotráfico, armas, pornografía, etc.,) y es usada por Infraestructura, algunos servidores y dispositivos especiales.

Navegación: (Libre) (Directivos y gerentes) Este perfil cuenta con tolerancia para la navegación con la excepción de algunas redes sociales, YouTube y otras páginas requeridas para consulta.

Navegación: (permisiva) (Lideres y casos especiales) En este perfil existe primero una lista de excepciones, luego un bloqueo por categorías (narcotráfico, armas, pornografía, y Redes Sociales etc.,), finalmente un bloqueo de páginas de navegación prohibida las cuales afectan el uso óptimo de red afecta la seguridad de la información y son consideradas innecesarias o no aptas para los usuarios.

Navegación: (permisiva)+ (Administrativos) En este perfil se asigna al personal del área administrativa ya que cuenta con acceso a algunos sitios permitidos de consulta y cargue de archivos exclusivos de esa área, que incluyen sitios oficiales como Dian, Cámara de comercio y temas legales, luego un bloqueo por categorías (narcotráfico, armas, pornografía, y Redes Sociales etc.,), finalmente un bloqueo de páginas de navegación prohibida las cuales afectan el uso óptimo de red afecta la seguridad de la información y son consideradas innecesarias o no aptas para los usuarios.

Navegación: (permisiva)(Wp) En este perfil se permite el uso de la aplicación WhatsApp previa evaluación y justificación de la solicitud, luego un bloqueo por categorías (narcotráfico, armas, pornografía, y Redes Sociales etc.,), finalmente un bloqueo de páginas de navegación prohibida las cuales afectan el uso óptimo de red afecta la seguridad de la información y son consideradas innecesarias o no aptas para los usuarios.

Navegación: (Permisiva Tecnología) En este perfil existe una lista de páginas permitidas y necesarias además tiene tolerancia a la navegación y descarga de recursos y/o aplicaciones relacionadas con el área de desarrollo web y bases de datos recursos esenciales para el desarrollo de sus actividades el resto de la navegación es bloqueada.

Restrictivo: (Operación) En este perfil existe una lista de páginas necesarias y esenciales para el desarrollo de sus actividades permitidas y el resto de la navegación es bloqueada.

Restrictivo: (Tecnología) En este perfil existe una lista de páginas necesarias y acceso a recursos esenciales para el desarrollo de sus actividades permitidas, incluyendo la salida y entrada de tráfico que implica conexión a bases de datos y conexión a ambientes de desarrollo el resto de la navegación es bloqueada.

Servidor: En este perfil se permite la conexión cifrada a alguno de los servidores de la compañía previa evaluación de parte del área de Infraestructura, el usuario será incluido en un perfil con los permisos adecuados para las tareas requeridas.

RGC Activa SAS podrá controlar, verificar y hacer monitoreo sobre el uso adecuado de este recurso. A continuación, se listan las restricciones definidas:

- El acceso a páginas relacionadas con apuestas, pornografía y drogas está estrictamente prohibido.
- Los empleados no deben abrir, ni revisar correos electrónicos considerados inseguros, por el riesgo latente de contener mensajes de dudosa procedencia o archivos contaminados con virus que pueden perjudicar la red de la compañía, fugas de información, ransomware, entre otros.
- No se permitirá la descarga, uso, intercambio e instalación de productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.
- No se permite cualquier tipo de transmisión vía internet que no esté debidamente autorizada.
- El servicio de Internet podrá ser utilizado para uso personal de manera ética, y responsable, sin afectar la productividad ni la protección de la información de RGC Activa SAS

- Los servicios de la nube, son una herramienta de trabajo de RGC Activa SAS Es responsabilidad de sus empleados la utilización de ésta de forma responsable de acuerdo a los lineamientos de la Gerencia General. Queda totalmente prohibido ceder su uso a personas no vinculadas a la compañía.
- Se contempla la posibilidad de habilitar el servicio de Skype, para el contacto corporativo (conciliaciones), para algunos funcionarios, previa aprobación de la coordinación correspondiente.
- La descarga de archivos y ejecución de programas desde Internet debe estar restringida a las actividades necesarias para la operación del negocio.
- El intercambio y descarga de archivo haciendo uso de protocolos P2P (Peer to Peer), Torrents, etc., está prohibido.

Los empleados de RGC Activa SAS., a quienes se les otorgue el privilegio de navegación por Internet deben utilizarlo como una herramienta de consulta, para propósitos de las funciones del negocio, acatando y respetando las Políticas vigentes alrededor de su uso.

El área de infraestructura está en potestad de monitorear todas las comunicaciones entrantes y salientes dentro de la red de la organización. Esto incluye conocer la IP de origen, la fecha, la hora, el protocolo, el servidor o dirección de destino y los datos comunicados.

El área de Infraestructura puede bloquear los sitios de Internet que se consideren inapropiados para la compañía. Se considera una falta disciplinaria que da lugar a la imposición de las sanciones disciplinarias previstas en el reglamento de trabajo, o incluso a la terminación del contrato de trabajo con justa causa, el acceso a páginas y sitios web de contenido sexual explícito, sitios de juegos o apuestas, sitios relacionados con sustancias ilícitas, sitios de citas y redes sociales, sitios de fraude, contenidos SPAM o en relación a delitos tipificados por la ley colombiana, contenido racista o de alguna forma ofensivo y discriminatorio, contenido violento, y todo contenido que no esté relacionado con el desarrollo de las finalidades de la compañía sin que medie previa autorización.

Los empleados de RGC Activa SAS., a quienes se les otorgue el privilegio de navegación por Internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Skype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de RGC Activa SAS.

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución que no esté autorizado, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el líder de equipo y el área de Infraestructura, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

No está permitido el intercambio no autorizado de información de propiedad de RGC Activa SAS., de sus clientes y/o de sus empleados, con terceros.

Así mismo está totalmente prohibido el uso de la infraestructura compañía para realizar ataques informáticos o similares a menos que sean pruebas previamente autorizadas y controladas por el área de infraestructura.

Cualquier intento por evadir los controles técnicos impuestos, será considerado en sí mismo una falta disciplinaria que da lugar a la imposición de las sanciones disciplinarias previstas en el reglamento de trabajo, o incluso a la terminación del contrato de trabajo con justa causa.

Por razones de seguridad, se restringe a todo nivel los servicios de FTP (Protocolo para la transferencia de archivos), Telnet (Programa de emulación de terminales remotas) y Chat (Comunicación electrónica interactiva) distintas a las dispuesta por el área de Infraestructura para uso corporativo para adicionar un protocolo o conexión se debe hacer por medio de ticket a la mesa de ayuda de Infraestructura, quien evaluara y dará tramite a dicha solicitud.

De acuerdo con las necesidades específicas y relacionadas con las funciones del cargo, se les brindará a los empleados el acceso a los servicios y sitios restringidos, previa solicitud y justificación de la respectiva al líder de equipo.

La descarga de archivos y ejecución de programas desde Internet debe estar restringida a las actividades necesarias para la operación del negocio.

A los gerentes, directores, coordinadores, jefes, lideres y personal de área administrativa que por su labor lo requieran se les habilitara Youtube, Whastapp.y Linkedin

RGC ACTIVA

REGISTRO DE ACTIVIDADES Y SUPERVISION

Propósito: Registrar eventos y generar evidencia.

Política

RGC Activa SAS., realizará monitoreo permanente del uso que dan los empleados y terceros a los recursos de la plataforma tecnológica y los sistemas de información de la compañía. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros (un año).

Se producirán revisiones regulares y cuidadosas a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Los registros de información se protegerán contra la manipulación y el acceso no autorizado. Las actividades del administrador del sistema y de la red serán registradas.

Estos registros serán protegidos y regularmente revisados.

Los relojes de todos los sistemas de informática relevantes serán sincronizados a una fuente de tiempo de referencia única (**Servidor SNTP**).

El Área de Infraestructura, debe definir de manera anual cuáles monitoreos se realizarán de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la compañía. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado. (Actualmente están habilitados logs relacionados abajo)

- Aplicación
- Seguridad
- Instalación
- Sistema
- Eventos reenviados

El Área de Infraestructura debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar relacionados arriba.

El Área de Infraestructura debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de RGC Activa SAS., Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

El Área de Infraestructura debe determinar los periodos de retención de los registros (logs) de auditoría de los recursos tecnológicos y los sistemas de información de la compañía. (Actualmente está estipulado a 1 año de retención)

El Área de Infraestructura debe revisar periódicamente los registros de auditoría de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo los logs se revisan cada dos meses o cuando se requiera por alguna eventualidad.

CONFIDENCIALIDAD CON TERCERO

Propósito: Establecer los requerimientos de confidencialidad en las relaciones con proveedores, contratistas, en particular con empleados y los terceros en general.

Política

Para el desarrollo de las relaciones contractuales civiles y comerciales, se debe exigir a los terceros la aceptación de los acuerdos de confidencialidad definidos por la organización. En dichos acuerdos se debe establecer el compromiso de salvaguardar la información, velar por su correcto uso, impedir el uso no autorizado de dicha información y guardar reserva. Se debe estipular a su vez la información que es objeto de protección dentro del acuerdo y su temporalidad.

Los acuerdos deben incluirse dentro de los contratos celebrados entre la organización y terceros, como parte integral del contrato o firmarse como un acuerdo independiente.

La aceptación de las condiciones de confidencialidad es indispensable para conceder al tercero el acceso a la información protegida.

POLÍTICA DE CIBERSEGURIDAD

RGC Activa SAS considera que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar el correcto funcionamiento de la compañía.

La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de la compañía, así como los activos que participan en sus procesos.

Esta Política tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre la los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

Esta política de ciberseguridad es de aplicación a todos los empleados, directivos y administradores que integran RGC Activa SAS incluyendo aquellas compañías participadas sobre las que tenga un control efectivo, dentro de los límites previstos en la normativa aplicable. En aquellas compañías participadas en las que RGC Activa SAS no tenga control efectivo, la compañía promoverá principios y directrices coherentes con los establecidos en esta política.

Principios básicos

Para ello se establecen los siguientes principios básicos:

- Garantiza que los Sistemas de Información y Telecomunicaciones de que dispone RGC Activa SAS poseen el adecuado nivel de ciberseguridad y resiliencia.

- Sensibiliza a todos los empleados, contratistas y colaboradores acerca de los riesgos de ciberseguridad y garantiza que disponen de los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para sustentar los objetivos de ciberseguridad de RGC Activa SAS

- Potencia las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las nuevas amenazas.

Impulsa la existencia de mecanismos de ciberseguridad y resiliencia adecuados para los sistemas y operaciones gestionados por terceros que presten servicios a la compañía.

- Se dota de procedimientos y herramientas que permiten adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas.

- Colabora con los organismos y agencias gubernamentales relevantes para la mejora de la ciberseguridad de la compañía, el cumplimiento de la legislación vigente y contribuye a la mejora de la ciberseguridad en el ámbito internacional.

Modelo de Gestión

RGC Activa SAS dispone de un modelo de gestión aplicable a la ciberseguridad basado en la normativa internacional y nacional, de modo que facilita, por todos los medios a su alcance y de forma proporcional a las amenazas detectadas, los recursos necesarios para que la organización disponga de un entorno alineado con los objetivos de negocio y los objetivos de ciberseguridad establecidos.

El modelo definido por RGC Activa SAS se basa en:

- Un marco para la gestión de las medidas de ciberseguridad aplicables mediante el establecimiento de una metodología de riesgos aprobada por la dirección en la que se fijen los objetivos y las metas de ciberseguridad, así como los principios de la ciberseguridad alineados con la estrategia y los objetivos de negocio y coherente con el contexto dónde se desarrollan las actividades de la compañía.

- Mecanismos para alinear los objetivos y metas de la ciberseguridad con la conformidad de los requisitos legislativos, reguladores y contractuales.

- Mecanismos para reaccionar frente a los incidentes que se produzcan tanto en la gestión del sistema como en los procedimientos operativos que dependen del mismo.

- La existencia de un conjunto de funciones y responsabilidades en materia de ciberseguridad claramente definidas y asignadas en el organigrama corporativo.

- Mecanismos para el tratamiento global de las amenazas de ciberseguridad incluyendo todas las actividades oportunas para el tratamiento de la seguridad.

- Un proceso de revisión y actualización continua del modelo de gestión de la ciberseguridad para adecuarlo en todo momento a las ciber amenazas que van surgiendo y puedan afectar a RGC Activa SAS

POLITICA AREAS SEGURAS

Establecer los lineamientos generales para controlar el acceso físico a las áreas seguras de La organización.

SISTEMA DE CONTROL DE ACCESO:

- El acceso al centro de datos deberá realizarse mediante un sistema autónomo de control de acceso o sistemas biométricos.
- El sistema de control de acceso debe ser administrado y debe mantener información histórica de accesos al centro de datos.
- El acceso se debe registrar en la bitácora que se encuentra en la recepción de cada sede.

MEDIDAS DE SEGURIDAD INTERNA:

- Se prohíbe el ingreso al centro de datos con material combustible, líquidos, productos volátiles, y todo producto o sustancia que pudiera ocasionar una reacción química perjudicial para la infraestructura del centro de datos.
- Los pasillos de circulación interna deben mantenerse despejados de todo objeto.

POLITICA DE ENMASCARAMIENTO DE DATOS

Por razones de seguridad de la información, los accesos a nuestro software corporativo, aplicaciones de misión crítica, equipos de trabajo, consolas de administración y gestión de herramientas están protegidos mediante enmascaramiento con asteriscos (*). Esta medida asegura la confidencialidad de los datos sensibles y la integridad de nuestros sistemas.

Procedimiento de Ofuscación en desarrollo de Software:

Identificación de Datos Sensibles:

Se identificarán las tablas y campos que contienen datos sensibles en las bases de datos de prueba. En este caso, se han identificado las tablas Adjuntos y Personas.

Ejecución de Scripts de Ofuscación:

Se diseñarán y ejecutarán seis scripts de SQL en un orden establecido para asegurar la correcta ofuscación de los datos. A continuación, se detalla el orden y la función de cada script:

i) **Script 1:** Anonimización de Apellidos, Fechas de Nacimiento, Direcciones y Correo Electrónico, y enmascaramiento de Números de Identificación en la tabla Personas_Mirror.
ii) **Script 2:** Anonimización de Apellidos, Fechas de Nacimiento, Direcciones y Correo Electrónico, y enmascaramiento de Números de Identificación en la tabla Personas.
iii) **Script 3:** Enmascaramiento de PATH en la tabla Adjuntos_Mirror para actas, historias de usuario, autorizaciones, etc. Así como enmascaramiento de Tipos y Nombres de archivos.
iv) **Script 4:** Enmascaramiento de PATH en la tabla Adjuntos para actas, historias de usuario, autorizaciones, etc. Así como enmascaramiento de Tipos y Nombres de archivos.
v) **Script 5:** Limpieza de todas las tablas de históricos.
vi) **Script 6:** Verificación de la integridad y consistencia de los datos ofuscados.

Verificación y Validación:

Después de la ejecución de los scripts, se realizará una verificación para asegurar que todos los datos sensibles han sido adecuadamente ofuscados y que no se ha comprometido la integridad de los datos.

POLITICA CONTROL CRIPTOGRAFICO

Establecer los controles criptográficos para proteger la información de RGC Activa SAS permitiendo asegurar que la información clasificada como restringida y/o confidencial reciba un tratamiento especial en el proceso de transportación, trasmisión y almacenamiento, aplicando mecanismos criptográficos que permitan minimizar los riesgos y lograr que el almacenamiento, transportación y trasmisión de la información sea segura.

Todo usuario que utiliza y administra documentos en formato digital con información de RGC Activa SAS, debe encriptar la misma de acuerdo a los requerimientos definidos, autorizados y de acuerdo a los niveles de clasificación definidos por la Gerencia de IT.
De ser necesario, la alta Gerencia de IT aprobara un software criptográfico para los archivos en los sistemas de información y recursos tecnológicos que los usuarios requieran proteger de acuerdo al rol y responsabilidad que tienen sobre la información que utilizan y administran dentro de RGC Activa SAS.
Para dar cumplimiento al control criptográfico, todos los involucrados en el alcance deberán acatar lo siguiente:

- Se debe utilizar herramientas de criptografía para la protección de la confidencialidad.

- Se debe definir los logaritmos criptográficos que podrán utilizarse al interior de RGC Activa SAS, como aplicación directa o como parte de la configuración de otros productos de seguridad comerciales,

- Solo se debe utilizar logaritmos criptográficos, definidos por los estándares internacionales.

Servicio de no repudiación

- Los servicios de no repudio deben utilizarse cuando sea necesario resolver disputas acerca de la ocurrencia o no de un evento o acción. Estos servicios están basados en el uso de técnicas criptográficas y firma digital.
- RGC Activa SAS establece que estos servicios estarán definidos por el uso de firma digital basada en certificados Digitales.

Administración de claves criptográficas

- La administración de claves criptográficas utilizadas es responsabilidad de la Gerencia de TI.
- Se debe implementar un sistema de administración para respaldar el uso por parte de RGC Activa SAS, de los dos tipos de técnicas criptográficas más usadas: clave secreta y clave pública.
- Las técnicas de clave publica se utilizarán para el cifrado y para generar firmas digitales.
- Todas las claves deben ser protegidas contra divulgación, modificación y destrucción. Las claves secretas y privadas necesitan protección contra divulgación no autorizada.

POLITICA CONTROL DE ACCESO

Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de RGC Activa SAS estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

Para RGC Activa SAS es prioritario definir el personal que tenga acceso a información sensible, por lo cual limita el acceso de usuarios de aplicaciones computarizadas únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de la misma.

La plataforma tecnológica es responsabilidad del área de infraestructura, así como los sistemas de información de la Entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso pertinentes a dichos recursos.

Directrices de seguridad para todo el personal

Para dar cumplimiento al control de acceso a la información, todos los involucrados en el alcance deberán acatar lo siguiente:

- Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información de RGC Activa SAS.

- Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato debe realizar la solicitud al área respectiva.

- Una vez que el contrato del contratista o proveedor haya finalizado, el supervisor del contrato tiene la responsabilidad de solicitar la cancelación de los derechos de acceso a el(los) usuario(s) vinculado(s) con ese contrato.

- Se deberá deshabilitar o borrar los usuarios y nombres de usuario correspondientes al personal que ya no tenga relación con RGC Activa SAS.

- Se deberán realizar revisiones periódicas en los diferentes sistemas de la RGC Activa SAS para garantizar que se remuevan los usuarios deshabilitados o redundantes, mínimo cada tres meses, para infraestructura On-premise o en la nube.

- Cada miembro del personal de RGC Activa SAS deberá hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.

- El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

Normas de seguridad para el control de acceso lógico

- El jefe de área o líder de proceso deberá ser el único autorizado para solicitar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario, a través de las diferentes categorías de la mesa de ayuda.

- La administración de los perfiles de usuario es responsabilidad de los administradores de cada aplicación (sistema) y de las áreas responsables de dicho activo.

- El jefe de área o Líder de proceso deberá establecer los permisos que corresponde a cada perfil que puede acceder a los recursos de la plataforma tecnológica, servicios de red y los sistemas de información.

- Los administradores de cada aplicación (sistema) deberán crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información cuando esto sea solicitado por el jefe de área o líder de proceso.

- Se deberá establecer un procedimiento de entrega de usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red de RGC Activa SAS, a los recursos de la plataforma tecnológica o a los sistemas de información.

- Se deberán inhabilitar o eliminar los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica.

- Se deberá verificar periódicamente las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y sistemas de información de RGC Activa SAS.

- Se deberá establecer controles de acceso a los ambientes de producción de los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios adecuados para garantizar el acceso a la información.

- Se deberán establecer mecanismos de auditoria al personal encargado de la administración del acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información.

Directrices de seguridad para el Control de acceso físico

- Se deberá identificar al personal que requiere acceso a las instalaciones de RGC Activa SAS, autorizar su ingreso y conceder los privilegios necesarios para el acceso físico.

- Se deberá contar con mecanismos de control de acceso para las áreas seguras (el centro de cómputo, la unidad de diagramación administración de infraestructura y oficinas que almacenen información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que RGC Activa SAS considere pertinentes.

- Las puertas de acceso al centro de cómputo, unidad de diagramación, administración de infraestructura, y centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.

- Se deberá aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo, administración de infraestructura, unidad de diagramación o a los centros de cableado, además se

deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.

- Se deberá registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado en una bitácora ubicada en la recepción de cada sede.

- Se deberá monitorear los ingresos al centro de cómputo permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

- Se deberá bloquear de manera inmediata los privilegios de acceso físico a las instalaciones de RGC Activa SAS tan pronto el personal termine su vinculación.

- Se deberá realizar la devolución del carné institucional tan pronto el personal termine su vinculación con RGC Activa SAS.

POLÍTICA DE USO DISPOSITIVOS MÓVILES

Establecer las condiciones para el manejo de los dispositivos móviles institucionales o personales que acceden a información de **RGC Activa SAS** y velar por el uso responsable de estos por parte del personal.

Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, El Área de Infraestructura debe implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

RGC Activa SAS pone a disposición de algunos miembros del personal dispositivos móviles institucionales para facilitar el desempeño de sus labores y propende porque dichos funcionarios hagan un uso responsable de ellos.

Con el fin de dar cumplimiento al tratamiento definido para los activos de información, todos los involucrados en el alcance deben cumplir las siguientes directrices:

Directrices de seguridad para el uso de dispositivos móviles

Se permite el uso de dispositivos móviles de conexión inalámbrica al interior de las instalaciones de RGC Activa SAS, únicamente para desarrollar y cumplir con los objetivos laborares y/o contractuales del personal, procurando que no se almacene en estos dispositivos información organizacional.

Los dispositivos móviles asignados a administrativos, contratistas y/o operativos, son responsabilidad de RGC Activa SAS, y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección.

Si el equipo móvil es asignado por la empresa, no se puede tener cuentas personales solo se debe tener información de la compañía.

Los medios de almacenamiento de estos dispositivos pueden ser protegidos tecnológicamente con medios de cifrado de datos o mediante cualquier otro mecanismo definido por el área de infraestructura, con el fin de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

Los trabajadores asumirán los riesgos y costos asociados a la perdida, fuga o uso indebido de la información que se encontraba en los dispositivos extraviados, además del cumplimiento de POLÍTICA SEGURIDAD DE LA INFORMACIÓN DE RGC Activa SAS.

La solicitud de conexión de dichos dispositivos a la red inalámbrica de la organización se realizará por intermedio de la mesa de ayuda de tecnología.

La autorización de retiro de las instalaciones de los dispositivos móviles se deberá regir por los protocolos ya estipulados por la compañía.

Se prohíbe conectar a los perfiles de red organizacional dispositivos móviles de uso personal, salvo que exista autorización explícita emitida por Infraestructura.

Se prohíbe el ingreso de teléfono celulares y otros dispositivos móviles a los centros de datos y centros de cableado de la organización, salvo que exista una autorización explícita emitida por infraestructura.

La alta dirección de la organización podrá exigir para determinadas reuniones la ausencia de dispositivos móviles, dispositivos de grabación y cualquier otro equipo electrónico que se especifique por razones confidencialidad o de evitar la interceptación y/o uso indebido de la información que en ellos se almacene.

Para los visitantes y personal de apoyo que ingrese a la organización y que requiera para sus funciones o servicios a prestar, el uso de alguno de estos dispositivos móviles, deben aplicarse las mismas restricciones de uso; adicionalmente, deberá estar siempre acompañado del responsable por parte de RGC Activa SAS para esta visita, con el fin de evitar usos indebidos de las tecnologías.

Pérdida del dispositivo.

En caso de pérdida o hurto de dispositivos móviles se debe reportar por escrito la perdida a El Área de Infraestructura y la Coordinación Administrativa lo más pronto posible.

SEGURIDAD DE LA INFORMACIÓN EN TORNO AL RECURSO HUMANO

En tratamiento de los datos personales, antes, durante y después de la relación laboral, se regirá por las siguientes reglas:

- RGC Activa, informará a las personas interesadas en participar en un proceso de selección, las reglas aplicables al tratamiento de los datos personales que suministre el interesado durante el respectivo proceso de selección, así como de aquellos daros que se obtengan durante la realización del mismo.

- El tratamiento de los datos suministrados por los interesados en las vacantes de RGC Activa, y los obtenidos del proceso de selección, será únicamente la informada en la autorización al aspirante.

- La empresa realizará estudios de seguridad previos a la contratación de nuevo personal para la empresa.

- La empresa contará con un proceso de eliminación de las hojas de vida de los candidatos (titulares) sobre los que ya no se tenga interés en conservar contacto, teniendo en cuenta las herramientas de archivística tales como tablas de valoración documental, tablas de retención documental y cuadros de comparación documental.

- Una vez seleccionada un aspirante para ocupar un cargo en RGC Activa, se celebrará el respectivo contrato de trabajo, acuerdo de confidencialidad y se le asignará cuando el cargo lo requiera, un usuario con un perfil definido relacionado directamente con el cargo a desempeñar, el cual le permitirá el acceso a la información personal tratada por la empresa, cuando el cargo así lo requiera.

- Seleccionado el candidato para el cargo, la empresa almacenará los datos personales del trabajador en una carpeta identificada con el nombre de cada persona. A esta carpeta solo tendrá acceso el Área de Gestión Humana y Administrativa y con la finalidad de gestionar la relación laboral entre la empresa y el empleado.

- Para cuando RGC Activa, requiera contratar servicios externos para el tratamiento de datos durante la relación contractual con los trabajadores, podrá requerirse la transferencia de datos personales a un tercero que se denominará Encargado, Para este caso, la empresa seguirá los lineamientos para la selección de Encargados en la transmisión de datos personales contenidos en esta política.

- Una vez se termine el contrato de trabajo, la empresa suscribirá un acuerdo de confidencialidad con el ex trabajador para salvaguardar la confidencialidad de la información personal manipulada por el ex trabajador; así como solicitará la entrega formas de perfiles y contraseñas que le hayan sido asignadas durante la ejecución del contrato de trabajo.

- Terminada la relación laboral, RGC Activa igualmente procederá a almacenar los datos personales de sus en un archivo general, sometiendo tal información a medidas y niveles de seguridad altas, atendiendo la calidad de los datos que dicho archivo puede contener.

SELECCIÓN DE ENCARGADOS PARA TRANSMISIÓN DE DATOS PERSONALES

Propósito: Garantizar que en los eventos en los que se realicen transmisiones de datos personales, se elija el encargado teniendo en cuenta las prerrogativas que trata la normativa sobre protección de datos personales.

Política
Cuando RGC Activa SAS. como responsable del tratamiento de datos personales, cuando realice Transmisión de datos personales, es de imperativo cumplimiento por parte de la empresa, seguir los siguientes lineamientos:

- Determinar cuál será el alcance del tratamiento que se permitirá realizar al Encargado.

- Evaluar la competencia y capacidad del Encargado para realizar el tratamiento que se le encomendará

- Revisar el manual de políticas de tratamiento de datos personales propias del Encargado.

- Examinar las medidas de seguridad implementadas por el Encargado para el tratamiento de los datos personales, y su compatibilidad con los estándares determinados por RGC Activa SAS.

- Suscribir un contrato de transmisión de datos personales.

- Realizar auditorías para medir el nivel de protección de los datos personales en la ejecución del contrato de transmisión.

REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Propósito: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos de la organización.

Política
Los sistemas de información son revisados regularmente a través de Auditorias para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la entidad.

SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los empleados, personal externo y proveedores de RGC Activa SAS, Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

MODIFICACIÓN DE LAS POLÍTICAS

RGC Activa SAS se reserva el derecho de modificar la presente Política de Seguridad de la información en cualquier momento, comunicando de forma oportuna a todas aquellas personas que estén relacionadas o que participen en la manipulación de la información de la compañía para su correcta implementación.

VIGENCIA

La presente Política rige a partir del 04 de Abril de 2022 y será revisada una vez al año.

CAROLINA SCANO GONZALEZ
Representante Legal (S)

CONTROL DE VERSIONES Y CAMBIOS

Versión	Fecha aprobación	Nota de cambio	Elaboró
3	12/07/2021	Ajuste de Políticas	Coordinador de Procesos
4	14/04/2022	Ajuste de Políticas	Gerente de TI Director de Infraestructura Coordinador de Procesos
5	31/08/2024	Inclusión de política de enmascaramiento de datos, inclusión de información de ciclo de almacenamiento de información, ajuste de perfiles de navegación	Gerente de TI Director de Infraestructura Coordinador de Procesos