El propósito de la siguiente política es fijar las directrices encaminadas a proteger la información, datos privados y confidenciales de Security & Co Ltda., sus empleados y asociados de negocio, así como asegurar que se utilicen correctamente los recursos técnicos y tecnológicos que la empresa pone a disposición de sus trabajadores y contratistas para el desarrollo de sus funciones.

La información incluye datos mantenidos en los sistemas de Security & Co Ltda., en soporte físico (papel), correos electrónicos, registros de llamadas, memorias USB, discos duros y compactos, dispositivos móviles u otros medios de almacenamiento. El tratamiento apropiado de los datos personales es fundamental para generar la confianza tanto de nuestros clientes como de nuestros colaboradores y demás grupos de interés.

Esta política es de obligatorio cumplimiento. El funcionario que la incumpla, responderá por sus acciones, omisiones o por los daños causados a la infraestructura de información de la empresa, de conformidad con la normatividad penal vigente y la disciplinaria de la empresa.

1. DEFINICIONES

Las siguientes definiciones se aplican a esta Política y a todos los procedimientos asociados con la misma:

Ciberseguridad: Todas las actividades tendentes a garantizar, tanto la seguridad de la información, como la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas que puedan verse afectadas por las ciberamenazas.

Datos Personales: Toda información sobre una persona física identificada o identificable. Esto incluye cualquier dato que, directa o indirectamente, pueda ser utilizado para identificar a una persona como nombres, fotografías, direcciones de correo electrónico, datos bancarios, información sobre redes sociales, ubicación, o dirección IP de un ordenador, entre otros. Los Datos Personales están protegidos por diversas legislaciones y se deben seguir prácticas adecuadas para su recogida, tratamiento y almacenamiento de cara a respetar los derechos de privacidad de las personas involucradas.

Gerente de Tecnología e Innovación: Responsable en materia de seguridad de las redes y de los Sistemas de Información.

Control y Gestión de Riesgos: Actividades coordinadas para dirigir y controlar en la organización los riesgos identificados.

Gestión de Incidentes: Conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y limitar un Incidente, resolviéndose e incorporando medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Incidente de Ciberseguridad o Ciberincidente: Suceso inesperado o no deseado que pueda comprometer la disponibilidad, autenticidad, trazabilidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por Sistemas de Redes y de Información o accesibles a través de ellos.

Información: Activo principal de cualquier empresa que puede estar en formato físico o digital y pueden estar determinados en ficheros de todo tipo (texto, imagen, multimedia, bases de datos…), pasando por los programas y aplicaciones que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios.

Principio de autenticidad: Persigue garantizar que el origen y las identidades asociadas a la información son realmente los que aparecen en los atributos de esta. Este principio va unido al de no repudio, que consiste en asegurar que un Usuario no pueda negar la autoría de un acto en el sistema o la vinculación a un dato o conjunto de datos.

Principio de confidencialidad: Procura que la información solo sea accesible para los Usuarios autorizados a acceder a ella y que no podrá ser divulgada a terceros sin la correspondiente autorización.

Principio de disponibilidad: Consiste en que la información esté accesible y se pueda utilizar de forma constante, asegurando la continuidad de los procesos y de la actividad. Este principio va unido al de resiliencia, que consiste en asegurar la capacidad de recuperación de los sistemas y la información tras un Incidente que impida el acceso temporal a los mismos.

Principio de integridad: Pretende asegurar que los datos se mantendrán libres de modificaciones no autorizadas y que la información existente no ha sido alterada por personas o procesos no autorizados.

Principio de trazabilidad: Busca la posibilidad de determinar en cada momento la identidad de las personas que acceden a la información y la actividad que desarrollan en relación con la misma, así como los distintos estados y rutas que ha seguido la información.

Riesgo: La posible pérdida o perturbación causada por un Incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal Incidente.

Sistema de Gestión de Seguridad de la Información (“SGSI”): Conjunto de políticas y procedimientos de seguridad de la información que tratan de componer un sistema de organización y gestión, diseñado para implantar, mantener y mejorar dichas políticas. El SGSI trata de asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los Riesgos de seguridad de la Información teniendo en cuenta los Riesgos analizados dentro de los procesos de negocio de Security & Co Ltda., y cuya base es la presente Política.

Sistema de Información: Conjunto discreto de recursos de información que soportan

aplicaciones o servicios de negocio, los cuales se organizan para obtener, procesar, mantener, utilizar, compartir, distribuir o disponer de la información.

Tratamiento de datos: Cualquier operación o conjunto de operaciones realizadas sobre Datos Personales, o conjuntos de éstos, ya sea por procesos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Usuario: Cualquier persona vinculada a Security & Co., por una relación civil o mercantil, así como clientes, proveedores, subcontratistas, consultores o cualesquiera otras personas o entidades a los que se autorice a utilizar, custodiar o acceder a las tecnologías de la información

Vulnerabilidad: Cualquier debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado. Salvo que se disponga expresamente lo contrario en cualquier apartado de la presente Política, las definiciones en singular incluyen el plural y viceversa.

2. CUENTAS DE USUARIO

a) Cada persona que acceda a su equipo de cómputo y al sistema debe tener una sola cuenta de usuario. Esto permite realizar seguimiento y control y evita que interfieran las configuraciones de distintos usuarios.

b) El Gerente de Tecnología e Innovación, es el único usuario administrador de cada equipo de cómputo y del sistema. En caso de ausencia, la Gerencia General podrá tener acceso a la contraseña de usuario administrador y designar a quien considere competente para atender algún requerimiento de mantenimiento.

c) La solicitud de una nueva cuenta o el cambio de privilegios, deberá hacerse por escrito y ser debidamente autorizada por el Gerente de Tecnología e Innovación.

d) Cuando un usuario recibe una cuenta, debe firmar este documento donde declara conocer las políticas y procedimientos de seguridad de la información y acepta sus responsabilidades con relación al uso de su cuenta.

e) No debe concederse una cuenta a personas que no sean empleados de la empresa, a menos que estén debidamente autorizados por la Gerencia General.

f) Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye al usuario administrador del sistema.

g) Las cuenta de usuario para el ingreso al equipo y al correo deben ser digitadas en cada ingreso, por ningún motivo se debe activar la opción de recordatorio de clave

para acceso directo.

h) El Director de Gestión Humana debe reportar al Gerente de Tecnología e Innovación sobre los empleados que cesan sus actividades y solicitar de forma inmediata la desactivación de su(s) cuenta(s) de acuerdo con los aplicativos autorizados.

i) No se otorgará cuentas a técnicos de mantenimiento externos, ni permitir su acceso remoto, a menos que el responsable de los sistemas de información determine que es necesario. En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).

j) No se crearán cuentas anónimas o de invitado.

3. INTERNET

Internet es una herramienta cuyo uso autoriza la empresa en forma extraordinaria, puesto que contiene ciertos peligros. Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas para poder acceder a la información de la empresa.

a) El acceso a internet es únicamente de uso laboral no personal, con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.

b) Está prohibido acceder a páginas de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana: aquellas que realizan apología del terrorismo, páginas con contenido xenófobo, racista etc., y en general todas aquellas que estén fuera del ámbito y contexto laboral.

c) En ningún caso se puede recibir o compartir información con archivos adjuntos de dudosa procedencia, esto para evitar el ingreso de virus al equipo.

d) Se prohíbe descargar programas, demos, tutoriales, ficheros o documentos que no sean de apoyo para el desarrollo de las tareas diarias de cada empleado y que contravengan las normas de Security & Co Ltda., sobre instalación de software y propiedad intelectual.

e) Ningún usuario está autorizado para instalar software en su ordenador. El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá comunicarlo al Gerente de Tecnología e Innovación quien determinará su conveniencia y cotizará según el proceso de compras, previa autorización de la Gerencia General.

f) Está prohibido instalar programas para ver vídeos, canales de televisión o de música vía Internet.

g) No debe usarse el Internet para realizar llamadas internacionales salvo en casos

previamente autorizados por la Gerencia General y por necesidad estrictamente comercial u operativa.

h) Los empleados tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.

i) Las redes WIFI solo podrán ser usadas por empleados de Security & Co Ltda, previa autorización del Gerente de Tecnología e Innovación, no se tendrán redes para invitados.

4. CORREO ELECTRÓNICO

El correo electrónico es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para agilizar las comunicaciones que apoyen la gestión de la empresa en el desarrollo de su objeto social.

Es de anotar que el correo electrónico es un instrumento de comunicación de la empresa y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con la ley.

Los usuarios que tienen asignada una cuenta de correo electrónico corporativo, deben establecer una contraseña para poder utilizar su cuenta de correo, y esta contraseña la deben mantener en secreto para que su cuenta de correo no pueda ser utilizada por otra persona.

Es obligación del empleado:

a) Utilizar el correo electrónico como una herramienta de trabajo, y no como casilla personal de mensajes, para eso deberá usar su cuenta de correo particular la cual de cualquier forma no podrá ser usada en los equipos de Security & Co Ltda., así mismo las cuentas corporativas no podrán ser usadas en equipos que no sean autorizados por el Gerente de Tecnología e Innovación.

b) Evitar enviar archivos de gran tamaño a compañeros de oficina. Si se hace necesario compartir un archivo con estas características podrá gestionar previa autorización de la Gerencia de Tecnología e Innovación el uso de carpetas compartidas en la red o en el servidor.

c) Evitar participar en la propagación de mensajes encadenados o en esquemas piramidales o similares.

d) Evitar distribuir mensajes con contenidos impropios y/o lesivos a la moral.

e) Si se recibe un correo de origen desconocido, debe consultar inmediatamente con el Gerente de Tecnología e Innovación sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos

maliciosos (virus, troyanos, keyloogers, gusanos, etc.).

f) Evitar "responder a todos" cuando se contesta un correo a no ser que este absolutamente seguro que el mensaje puede y debe ser recibido por todos los intervinientes. De igual forma si va a reenviar un correo.

g) Evitar el acceso a las cuentas personales durante la jornada laboral.

h) Cerrar el correo electrónico cuando deje de usar su estación de trabajo para evitar que otra persona use su cuenta.

i) Se prohíbe tajantemente facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.

j) Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantenerse en línea y activada la opción de aviso cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes respetando siempre y de cualquier manera las políticas de desconexión laboral salvo que por la vía del contrato se haya pactado algo diferente en virtud de sus responsabilidades y funciones.

k) Se recomienda mantener los mensajes que en virtud de su importancia o trazabilidad se desean conservar, agrupándolos por temas en carpetas según el tema tratado.

l) Utilizar siempre el campo “asunto” a fin de resumir el tema del mensaje. Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.

m) Enviar mensajes bien formateados y evitar como norma de cortesía, el uso generalizado de letras mayúsculas.

n) Evitar usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces esto provoca demasiado tráfico en la red.

o) Evitar enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a toda la institución.

p) El Gerente de Tecnología e Innovación determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional, ésta capacidad quedara configurada en el servidor de correos.

q) Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en carpetas personales en el disco duro del computador personal.

5. COMPUTADORES, IMPRESORAS, PERIFÉRICOS Y LÍNEAS TELEFÓNICAS FIJAS Y MÓVILES

a) La infraestructura tecnológica: servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general; no puede ser utilizado en funciones diferentes a las corporativas.

b) Está prohibido el uso de líneas telefónicas fijas y móviles para comunicación distinta a la relacionada con el trabajo.

c) Los usuarios no pueden instalar, suprimir o modificar el software originalmente entregado en su computador. Es competencia del Gerente de Tecnología e Innovación, o a quien el designe la instalación de software.

d) No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia del Gerente de Tecnología e Innovación o a quien el delegue, el retiro o cambio de partes.

e) Cualquier medio externo de almacenamiento de información traído a la empresa, debe superar una verificación de virus mediante el antivirus instalado, en su defecto, debe ser entregado al Gerente de Tecnología e Innovación para control de circulación de virus.

f) No es permitido destapar o retirar la tapa de los equipos, por personal diferente al Gerente de Tecnología e Innovación o bien a quien designe sin la autorización de este.

g) Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, sin previa autorización del Gerente de Tecnología e Innovación.

h) Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.

i) Es estrictamente obligatorio, informar oportunamente al Gerente de Tecnología e Innovación la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, recurso humano, o cualquiera otra, que altere la correcta funcionalidad de los procesos. El reporte de las novedades debe realizarse tan pronto se presente el problema.

j) Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.

k) Los protectores de pantalla y tapiz de escritorio, serán establecidos por Gerente de Tecnología e Innovación y deben ser homogéneos para todos los usuarios.

l) Ningún empleado, podrá formatear los discos duros de los computadores.

m) Ningún empleado podrá retirar o implementar partes sin la autorización de la Gerencia de Tecnología e Innovación.

6. LINEAMIENTOS PARA LA GESTIÓN DE VULNERABILIDADES TÉCNICAS

El objetivo de estas directrices es prevenir la ocurrencia de eventos e incidentes de seguridad de la información generada por el aprovechamiento de vulnerabilidades técnicas por parte de atacantes, las cuales se definen a continuación:

a) El Gerente de Tecnología e Innovación como responsable de la seguridad informática y ciberseguridad realiza un análisis de vulnerabilidades periódica de los servicios y análisis de riesgos de los activos de información. Como resultado del análisis, se establece un plan de tratamiento de riesgo acorde con los recursos técnicos y financieros con los que se cuente, a fin de cerrar las brechas de seguridad encontradas.

b) El Gerente de Tecnología e Innovación es el encargado de dar lineamientos y recomendaciones para la mitigación de las vulnerabilidades.

c) El Gerente de Tecnología e Innovación, establece la prioridad en la ejecución de los controles dentro de la declaración de aplicabilidad y los responsables de su ejecución.

d) El Gerente de Tecnología e Innovación establece el procedimiento y los protocolos para la gestión de incidentes de seguridad informática, el cual debe seguirse cuando se considere que un incidente es causado por una falla de seguridad.

7. ARCHIVO FÍSICO Y DOCUMENTOS

a) Cada Líder de Proceso es responsable por el archivo de sus registros tanto físicos como electrónicos haciéndolo de tal manera que permita una oportuna ubicación y trazabilidad. Así mismo se hace responsable de salvaguardar los intereses de la compañía, dando la debida protección a información que se considere sensible.

b) Se considera justa causa para la terminación unilateral del contrato de trabajo, sin perjuicio de las acciones penales que puedan derivar de la acción, quien brinde información de la compañía a terceros sin la debida autorización y cuyo uso pueda ser perjudicial para la labor comercial de la compañía y su competitividad en el mercado.

c) La información laboral contenida en las hojas de vida de los empleados tiene carácter de confidencial por lo tanto no podrá exhibirse a personas diferentes al representante legal o la autoridad requirente.

8. CORRESPONDENCIA

a) Los documentos producidos en la empresa tienen un funcionario quien los emite, quien es el responsable de controlar su envío a la persona o entidad destinataria, el recibo por parte del destinatario, así como de controlar la llegada, trámite y archivo de la copia con el respectivo sello de recibido.

b) Los documentos llegados a la empresa, tienen un destinatario específico, quien es el responsable de recibirlo, darle el trámite correspondiente, controlar que produzca los efectos requeridos y su posterior archivo.

c) Todo funcionario que elabore un documento, debe responsabilizarse del control y seguimiento del mismo hasta que finalice el proceso correspondiente, así como de su archivo y conservación para consultas.

9. OTRAS DIRECTRICES

a) Las memorias USB, discos duros y compactos, dispositivos móviles u otros medios de almacenamiento que pertenezcan a Security & Co Ltda., no deben contener música, videos, imágenes, ni información que no sea necesaria para el desarrollo de las tareas propias de cada cargo, en caso de ser necesario debe haber una autorización previa del Gerente de Tecnología e Innovación.

b) Todo empleado responsable de equipos informáticos debe dejarlo bloqueado ante su ausencia en el puesto de trabajo.

c) No se autoriza el retiro de las instalaciones de documentos, equipos de cómputo o información sensible para la organización salvo con la autorización expresa de la Gerencia General.

10. LINEAMIENTOS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de gestionar adecuadamente los eventos e incidentes que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información, Security & Co Ltda., adopta, implementa, mantiene y mejora un procedimiento de gestión de incidentes de seguridad de la información, el cual se complementa con los siguientes lineamientos:

a) Todos los colaboradores, contratistas y demás personal deben reportar sin demoras injustificadas a los lideres de proceso o a la Gerencia de Tecnología e Innovación cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de cualquier activo de información.

b) El reporte de los eventos o incidentes de seguridad de la información se realiza de acuerdo con el procedimiento de gestión de incidentes de seguridad de la información

en la mesa de ayuda de la Gerencia de Tecnología e Innovación.

c) La evaluación de los diferentes eventos e incidentes de seguridad de la información es realizada por la mesa de ayuda de la Gerencia de Tecnología e Innovación. Los eventos de seguridad de la información que sean calificados como incidentes de seguridad de la información se administran mediante el procedimiento de gestión de incidentes de seguridad de la información.

d) La Entidad evaluará como incidentes de seguridad de la información eventos asociados a: incumplimiento de las políticas de seguridad de la información los que correspondan a delitos informáticos calificados como tales por la normatividad vigente y los eventos que materialicen riesgos de ciberseguridad.

e) El procedimiento de gestión de incidentes de seguridad de la información define las acciones específicas para el reporte de eventos, incidentes o debilidades en seguridad de la información, evaluación y respuesta ante incidentes de seguridad de la información, recolección de evidencias asociadas a los incidentes de seguridad de la información y lecciones aprendidas.

ROCIO JOHANNA QUIROGA
Representante Legal

CONTROL DE CAMBIOS		
VERSION	**FECHA**	**DESCRIPCION DEL CAMBIO**
1	14/02/2025	Emisión de la Política de Seguridad de la Información en su versión inicial.