

## POLÍTICAS DE SEGURIDAD PARA LOS SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA TECNOLÓGICA

Virtual Prime S.A.S.

### Introducción.

Las políticas de seguridad para los sistemas de información e infraestructura tecnológica para la empresa Virtual Prime S.A.S. descritas en este documento, define y detalla el uso adecuado de los sistemas de información, así como de las herramientas de comunicaciones, infraestructura tecnológica de la empresa, cuentas de usuario y correo electrónico, con el fin de proteger al usuario y a la empresa de situaciones que puedan poner en riesgo o explotar vulnerabilidades que permitan la fuga o secuestro de información, como también el de suplantación de identidad u otros factores que puedan alterar de cualquier forma la correcta prestación de los servicios de cara al usuario.

Las políticas aquí descritas, son de obligatorio cumplimiento por parte de todos y cada uno de los funcionarios, colaboradores, contratistas, en todas las ramas o áreas de la empresa, como también para las personas naturales, independientes o empresas de carácter público o privado que pudieran tener vinculación temporal o fija con nuestra empresa y que hagan uso en una o todas sus partes de nuestros sistemas de información o infraestructura tecnológica asociada.

Pretendemos facilitar y agilizar los procesos mejorando la calidad en la prestación del servicio para todos los clientes, públicos y privados, logrando así la mejora de los procesos en los sistemas de información, con el planteamiento y regulación del uso apropiado de todos sus componentes y equipos, así como implantar aquellas medidas necesarias para garantizar la seguridad y confidencialidad de la información de carácter reservado para la empresa y nuestros usuarios.

Para cumplir con los objetivos propuestos, resulta necesario establecer políticas que garanticen el uso efectivo y seguro de los sistemas de información e infraestructura tecnológica y las herramientas o aplicaciones asociadas a estos, y, por tanto, este documento tiene como objetivo fijar las normas fundamentales que deben regir el comportamiento de todos los actores involucrados en cualquier nivel o proceso con vinculación directa o indirecta hacia nuestra empresa.

Estas normas serán revisadas, actualizadas y publicadas periódicamente en nuestra página oficial <https://www.virtualprime.co>, y enviadas a todos los correos electrónicos institucionales de nuestros empleados y colaboradores en cualquier nivel de operación.

Es responsabilidad de todos los empleados, trabajadores, colaboradores y contratistas estar al tanto del contenido de las políticas y todas sus modificaciones o actualizaciones.

## Contenido

- 1- Disposiciones generales para el correcto uso de los sistemas de información. ....3
- 2- Disposiciones para el correcto uso de las redes de datos y servicios de internet. ....4
- 3- Disposiciones para el uso de cuentas de correo electrónico corporativo. ....5
- 4- Disposiciones para la atención de incidentes de seguridad informáticos. ....6
- 5- Disposiciones para el uso de los sistemas de comunicación corporativa. ....8

## 1- Disposiciones generales para el correcto uso de los sistemas de información.

- 1.1- Los sistemas de información de la empresa Virtual Prime S.A.S., incluyendo la infraestructura tecnológica, programas, aplicaciones y archivos electrónicos, pertenecen a Virtual Prime S.A.S. y solo pueden utilizarse para fines relacionados con el desempeño de las actividades encomendadas al interior de la empresa, esta misma consideración se aplica a la información almacenada en el computador corporativo asignado o la emitida o comunicada a través de los sistemas de información, aplicativos o correo corporativo de la empresa.
- 1.2- Los sistemas de información, infraestructura tecnológica, programas, aplicaciones y correo electrónico corporativo asociadas a la empresa, solo podrán ser utilizadas por personal debidamente autorizado por la Junta de Accionistas o por la Gerencia General, será responsabilidad de cada área el definir las tareas que conllevan acceso a las herramientas descritas, el uso de estos recursos deberá circunscribirse al ámbito profesional, técnico y administrativo, con el fin de agilizar las actividades desarrolladas por Virtual Prime S.A.S. en pro de la eficiencia y eficacia de estas y no se autoriza el uso con fines personales sin justificación previa de usabilidad, requerimiento, oportunidad o de compatibilidad horaria para los empleados de planta o del desarrollo habitual de las actividades de los colaboradores y contratistas.
- 1.3- La divulgación de información de carácter reservado o con datos sensibles sin la debida justificación de carácter penal o investigativa por una entidad de seguridad pública nacional o sin su respectiva autorización se encuentra prohibida. La alteración, destrucción, distribución fraudulenta o malintencionada de cualquier documento en formato electrónico de propiedad o con logos de Virtual Prime S.A.S. puede perjudicar gravemente la empresa y constituir una infracción grave; en tal caso, se aplicarán las medidas disciplinarias y de ley previstas en las leyes aplicables en el territorio colombiano, reservándose la empresa Virtual Prime S.A.S. el derecho de interponer cuantas acciones legales sea necesarias.
- 1.4- Los sistemas operativos, programas, aplicativos, herramientas de ofimática, antivirus, sistemas de comunicación, correos corporativos y bases de datos utilizados en los computadores corporativos de la empresa Virtual Prime S.A.S. deben tener su correspondiente licencia de uso o autorización de uso explícita para su utilización, dichos elementos o software solo podrán ser instalados por personal autorizado a tales efectos, además no deberán instalarse programas adicionales a los que ya se configuran inicialmente sin la previa autorización de la Gerencia General de la empresa, incluso cuando se trate de programas gratis o de libre distribución.
- 1.5- Los aplicativos, herramientas, bases de datos, formatos, imágenes o cualquier otro elemento digital o electrónico creado por la empresa o por sus empleados, colaboradores y contratistas en función de sus cargos o el desarrollo de sus actividades contractuales, no podrán reproducirse o utilizarse para fines ajenos a sus

funciones o tareas encomendadas sin autorización explícita de la dirección de la empresa.

- 1.6- Sera responsabilidad de la Gerencia General, establecer las normas mediante las cuales se asignan cuentas de acceso, claves secretas, contraseñas, controles de acceso a los servidores y sistemas, auditar su uso, integridad y seguridad de los datos corporativos.
- 1.7- Virtual Prime S.A.S., ni la Gerencia General se hacen responsables por la pérdida de información de carácter personal que resulte afectada por la mala utilización de los recursos tecnológicos, ataques o virus informáticos, y es responsabilidad de los usuarios realizar el respaldo a la información personal contenida en los equipos designados por la empresa o en sus propios equipos.
- 1.8- Cada usuario es responsable por el uso adecuado de los equipos tecnológicos, aplicativos, formatos, documentos digitales, software y de las claves de acceso con sus usuarios ante la entidad y la Ley.
- 1.9- El acceso a la información o a una cuenta ajena sin autorización por la Junta de Accionistas o por la Gerencia General obtenido mediante la modificación de privilegios de acceso o la interceptación de información de cualquier otra manera estará sujeta a las medidas disciplinarias y/o penales pertinentes.
- 1.10- Las disposiciones aquí establecidas, deberán interpretarse como complementarias a las normas legales comúnmente aplicables en todo el territorio colombiano.
- 1.11- La violación a cualquiera de las presentes políticas puede conllevar a la revocación de cualquier privilegio de uso de los sistemas de información y será notificada a la Junta de Accionistas y la Gerencia General, quienes informaran al responsable inmediato de los empleados, colaboradores, contratistas o empresas donde este adscrito para que estas emprendan las acciones de control o jurídicas pertinentes.

## **2- Disposiciones para el correcto uso de las redes de datos y servicios de internet.**

- 2.1- Los usuarios y operadores de los sistemas informáticos de la empresa Virtual Prime S.A.S., deben evitar, en casos o actividades corporativas descargar y/o emplear archivos de imagen, sonido o similares que puedan estar protegidos por derechos de autor o de terceros sin la previa autorización de estos por escrito.
- 2.2- Abstenerse de visitar sitios de baja reputación como páginas de acceso a juegos online, sitios de pornografía u otros sitios que pueden perjudicar la seguridad informática de la empresa.

- 2.3- Todos los empleados, colaboradores, contratistas y empresas relacionadas con la empresa son conscientes que los sistemas de información de la empresa solamente deben ser utilizados para propósitos lícitos y en cumplimiento de las actividades encomendadas por la corporación hacia los usuarios finales y que toda actividad de navegación puede ser registrada por la empresa, quien podrá revelar cualquier acceso cuando una autoridad judicial colombiana así lo requiera.
- 2.4- En ninguna circunstancia se puede introducir intencionalmente programas maliciosos o virus dentro de la red de datos o sistemas tecnológicos de la empresa Virtual Prime S.A.S., ni acceder o forzar accesos a información sobre la cual no se tengan permisos y autorizaciones adecuadas, ni obtener accesos adicionales o ampliación de privilegios por medios ilícitos.
- 2.5- El escaneo de puertos, análisis de tráfico y vulnerabilidades de la red solo es permitido cuando se lleve a cabo por la Gerencia General o con autorización previa de la misma o por la Junta de Accionistas mediante documento escrito donde conste la autorización, las fechas de realización y la programación de esta.
- 2.6- Se encuentra prohibido realizar ataques para aprovechar vulnerabilidades identificadas en los servicios informáticos o sobre la infraestructura tecnológica de la empresa Virtual Prime S.A.S. con el fin de interrumpir, interferir, deshabilitar o cualquier aspecto que afecte la prestación de los servicios de la empresa a sus clientes finales o que vallan en contra de las personas, instituciones o que deriven en incumplimiento de las leyes nacionales e internacionales.
- 2.7- En ninguna circunstancia puede realizarse cualquier tipo de monitoreo de red con la finalidad de interceptar datos o mensajes que viajan por las redes de datos de la empresa Virtual Prime S.A.S., salvo las que sean derivadas de las investigaciones judiciales o por entes de seguridad nacional colombiana.
- 2.8- No pueden ser añadidos equipos de cómputo o dispositivos móviles o electrónicos IoT a la red de datos de la empresa Virtual Prime S.A.S. o a las redes de las entidades en convenio o cooperación que no hayan sido autorizados por la Gerencia General y se brinde el adecuado acceso.

### **3- Disposiciones para el uso de cuentas de correo electrónico corporativo.**

- 3.1- Las cuentas de correo corporativo son propiedad de la empresa Virtual Prime S.A.S. y está en cabeza de la Gerencia General la asignación de cuentas de correo con dominio @virtualprime.co o @tecnologiabacana.com, las medidas de control de acceso aplicables, las claves de acceso y/o contraseñas, los controles de acceso al servidor y la generación o eliminación de cuentas de correo electrónico.

- 3.2- Todos los usuarios, empleados, colaboradores o contratistas a quienes se les haya asignado una cuenta de correo electrónico corporativo, son los únicos responsables de esta, en consecuencia, cada usuario es responsable por toda la actividad que se genere a partir de la cuenta de correo asignada. La responsabilidad es entendida ya sea por acción, omisión o extralimitación.
- 3.3- Cuando actué en nombre de la empresa Virtual Prime S.A.S. ante esta o ante el usuario final del servicio, utilice el correo electrónico corporativo, salvo en caso de desastre informático para lo cual se debe implementar la contingencia prevista en los manuales de riesgos de la empresa.
- 3.4- Para evitar ser parte del problema de uso inadecuado de recursos tecnológicos y posibles transmisiones dañinas que se hacen vía electrónica, se insta a la eliminación inmediata y sin reenvío de cadenas de correos electrónicos.
- 3.5- Revise y valide la información que va a enviar en el correo electrónico con el fin de no cometer imprudencias o errores.
- 3.6- Para el correcto uso del correo electrónico corporativo, evite utilizar lenguaje sexista, obsceno, de acoso de cualquier índole y palabras que puedan ofender a otro, ni para hostigar o acosar a cualquier persona o compañía.
- 3.7- Siempre adopte una actitud reservada con personas que intenten obtener información personal suya o de sus compañeros por los medios electrónicos.
- 3.8- Verifique cuidadosamente los destinatarios del correo para evitar el desvío de información corporativa y errores en la entrega de esta.
- 3.9- Revise contra virus y software malicioso antes de ejecutar cualquier archivo adjunto que haya recibido por correo electrónico corporativo sin importar su procedencia.
- 3.10- En ninguna circunstancia debe ser usado el correo electrónico corporativo con fines personales y comerciales, ni para registrar servicios de pago por suscripción o para solicitar empleo en otras empresas, para esto deben ser usadas las cuentas de correo electrónico de carácter personal, en cuyo caso, la empresa Virtual Prime S.A.S. no tiene relación o vínculo alguno.

#### **4- Disposiciones para la atención de incidentes de seguridad informáticos.**

- 4.1- Todos los empleados, directivos, colaboradores, contratistas y personal de apoyo en convenio de cooperación que usen en una o todas sus partes los sistemas informáticos o la infraestructura tecnológica de la empresa Virtual Prime S.A.S., son los directos responsables de cumplir con las políticas aquí consignadas para la

atención de incidentes de seguridad informática de manera ágil y oportuna, evitando afectar en mayor impacto la seguridad informática de la empresa.

- 4.2- Cuando sea evidenciado la materialización de un incidente que afecte directamente la seguridad o integridad de los equipos de computo corporativos, ya sea robo, acceso indebido, conexión de dispositivos externos como memorias USB u otros elementos sin la previa autorización del usuario designado para el equipo, deberá ser informado a la Gerencia General o a la persona designada por ella, tomar evidencia de lo sucedido en la medida de lo posible y desconectar el equipo de la red de datos donde se encuentre ubicado, apagar el equipo y esperar indicaciones.
- 4.3- Al recibir mensajes de correo en el buzón de correo corporativo con las características de un ataque informático, expresado como correos de suplantación de identidad, phishing, cobros injustificados o de empresas o páginas con quienes no tiene relación alguna, abstenerse de abrir el correo electrónico, eliminarlo de su buzón y comunicarlo a la Gerencia General para que esta realice un seguimiento de la actividad maliciosa hasta superar el incidente.
- 4.4- Si se detecta que la cuenta de correo corporativo pueda estar siendo usada en casos de suplantación de identidad o para envío de correos maliciosos, deberá ser informado de manera inmediata a la Gerencia General para que esta actúe en la inmediatez y se logre superar el incidente.
- 4.5- Todos los daños o perjuicios ocasionados por la omisión de estas políticas, como tambien por el mal uso de los medios tecnológicos suministrados por la empresa Virtual Prime S.A.S., y que sean evidenciados por esta, serán pagados por el empleado, colaborador, contratista o personal de apoyo en convenio, bajo acuerdo con la Gerencia General y será este usuario el responsable directo ante las entidades, personas naturales o cualquier usuario que considere haya sido afectado con ocasión al incidente de seguridad informática.
- 4.6- En ningún caso la empresa Virtual Prime S.A.S. será sujeta a responsabilidad civil, actual o extracontractual con personas naturales, empresas o entidades gubernamentales a causa de los incidentes provocados, ocasionados o perpetrados por los usuarios del servicio o equipo, ya que la responsabilidad es entendida ya sea por acción, omisión o extralimitación.
- 4.7- La eliminación malintencionada de archivos de evidencia, programas, archivos y documentos de la empresa, la perdida de documentación o archivos digitales de manera accidental, el envío de información errada a cuentas de correo internas o externas, como tambien el desvío de información o sustracción de esta con fines ajenos a la empresa, deberá ser tomada como un incidente de seguridad informática y deberá ser reportada bajo los mismos parámetros especificados en las presentes políticas.

- 4.8- La responsabilidad del usuario frente a las afectaciones ocasionadas o derivadas de los incidentes de seguridad informática, surtirán efecto y estarán asignadas a los usuarios y procesos en los tiempos y medidas que se declaren en la ley y la jurisdicción colombiana.

**5- Disposiciones para el uso de los sistemas de comunicación corporativa.**

- 5.1- Se entiende como sistemas de comunicación corporativa todos y cada uno de los equipos o dispositivos de propiedad y entregados por la empresa Virtual Prime S.A.S., o de los canales de comunicación corporativos como son el Correo Electrónico Institucional, la plataforma para asignación de Tickets de soporte, los chat de WhatsApp y Telegram corporativos, los grupos de trabajo, las herramientas de Google Suite o Google Work Space, a los cuales serán aplicables las siguientes políticas.
- 5.2- Siempre al utilizar los equipos y canales de comunicación establecidos por la empresa, se deberá propender por el uso adecuado de los signos de puntuación, el manejo de la ortografía de forma correcta y el uso de la Netiqueta o buenas normas y que son el conjunto de reglas que regulan el comportamiento que deben tener los usuarios en la red, con el fin de garantizar la fluidez en la interacción con respeto entre los usuarios.
- 5.3- Evitar utilizar lenguaje obsceno u ofensivo al referirse a los usuarios, actividades o personas ajena a la empresa por los medios corporativos, ni utilizar apelativos o sobrenombres al referirse a sus compañeros u otras personas que influyen en las actividades propias de la empresa.
- 5.4- No utilizar lenguaje sexista u ofensivo que pueda alterar el orden entre los participantes del grupo.
- 5.5- Evitar hacer parte de cadenas de correo masivo o de información sin contenido relevante para el desarrollo de las actividades y evitar compartir información sin verificación de medios oficiales o información de dudosa procedencia.
- 5.6- Evitar hacer uso de Stickers, memes, imágenes, gif, videos, audios, o cualquier otro elemento digital que denigre la calidad del ser humano o que pueda afectar de cualquier manera a los demás integrantes del equipo de trabajo o que pueda generar confusión referente a un tema u otro.

- 5.7- No realizar publicaciones pornográficas o de contenido explicito por ningún medio corporativo, en ninguna circunstancia.
- 5.8- La comunicación de carácter corporativo podrá ser auditada en cualquier momento o lugar con el fin de tomar las medidas correctivas pertinentes para cada caso en específico.
- 5.9- Evitar hacer uso de los canales de comunicación corporativos en horarios no establecidos para el desarrollo de las actividades cotidianas, solo en casos puntuales especificados con anterioridad por la Gerencia General, se dispondrá de estos espacios previa comunicación verbal, como es el caso de las actividades en horario especial por inactividad de las empresas. En los casos en los que por fuerza mayor se requiera la comunicación con uno de los integrantes del equipo, deberá utilizarse solo el contacto de la persona o personas implicadas en la necesidad, evitando así entorpecer o afectar el tiempo de disfrute de los empleados, colaboradores o contratistas de la empresa Virtual Prime S.A.S.
- 5.10- Los únicos medios de comunicación establecidos para su uso las 24 horas, los 7 días de la semana son el Correo Electrónico Corporativo y la plataforma para la asignación de tickets de soporte, esto con el fin de que los empleados, colaboradores y contratistas puedan verificar y dar respuesta la primera hora del primer día hábil en que se reciban los correos de solicitud y verificación y que la cuadrilla implementadora de redes de telecomunicaciones y la Gerencia General tengan siempre la información actualizada en el tiempo debido o se realice la atención a los tickets de soporte o casos con asignación de horario especial.

El incumplimiento de las políticas de seguridad para los sistemas de información e infraestructura tecnológica anteriormente descritos acarreara las sanciones a que haya lugar, ya sean de carácter administrativo, jurídico o monetario de acuerdo con la gravedad de la afectación y el nivel de responsabilidad evidenciado.

Firmado en Itagüí a los 30 días del mes de julio del año 2023.



CARLOS MARIO ARIAS VÁSQUEZ  
Gerente General.