POLÍTICA DE CONTROLES EN LA RED DE DATOS Y TRANSFERENCIA DE INFORMACIÓN DE LA PERSONERÍA DE BOGOTÁ, D.C.

1. INTRODUCCIÓN

La Dirección de Tecnologías de la Información y las Comunicaciones de la Personería de Bogotá, D.C., establecerá los controles y mecanismos necesarios para suministrar el servicio de transferencia de información de una manera segura, con el fin de contribuir a mantener la confidencialidad, integridad y disponibilidad de la información que circula a través de las redes de datos y comunicaciones de la Entidad.

Para cumplir con este objetivo, se establecen controles y lineamientos de obligatorio cumplimiento relacionados con las configuraciones de seguridad, el uso y responsabilidades de los funcionarios(as) y contratistas a cargo de la administración y uso de equipos y servicios de TI que soportan la transferencia interna y externa de la información institucional.

2. ALCANCE

Los lineamientos establecidos en este documento son de obligatorio cumplimiento para funcionarios(as) y contratistas de la Entidad, que intervengan en actividades de administración, configuración y uso de cualquier componente tecnológico conectado a la red de datos y comunicaciones de la Personería de Bogotá, D.C., así como de los servicios institucionales autorizados para la transferencia de datos y/o información institucional.

3. OBJETIVO GENERAL

Establecer los lineamientos para gestionar y controlar la información institucional en forma apropiada y de manera formal, mediante el uso de las redes de datos y comunicaciones de la Personería de Bogotá, D.C.

4. LINEAMIENTOS

- La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, gestiona y establece mecanismos y controles para prestar el servicio de redes de datos y comunicaciones en la Entidad y propende por la protección de los datos y los servicios conectados en las redes de la Personería de Bogotá D.C., contra el acceso no autorizado.

- La transferencia de la información institucional de la Personería de Bogotá D.C., se controla según los niveles de clasificación legal de la información establecidos y las políticas de seguridad de la información de la Entidad. En caso de que se requiera intercambiar información **Clasificada, reservada o sensible**, se deben implementar los controles de cifrado de información de acuerdo con lo establecido en la política de controles criptográficos.

- Los intercambios de información con terceros deben estar soportados por medio de contratos o acuerdos debidamente formalizados, determinando los medios y controles para el tratamiento de la información. Así mismo, se firmarán acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas.

4.1 Gestión de la Seguridad en las Redes

- Se debe establecer los procedimientos para la administración de los equipos remotos, incluyendo los equipos en las áreas restringidas.

- Se deben establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.

- Se deben Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.

- Todos los componentes de red deben contar con un sistema fuerte de autenticación para poder acceder a los mismos.

- La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, implementa los mecanismos necesarios y establece acuerdos de niveles de servicio, para garantizar la disponibilidad de los servicios de redes de datos y comunicaciones.

- Únicamente personal autorizado puede ingresar a los equipos de comunicación.

- El acceso administrativo a los equipos de red debe ser centralizado y auditado.

- Tocas las conexiones de administración deben ser bajo conexiones cifradas.

- La Personería de Bogotá D.C. implementa mecanismos de segmentación de redes a través de Vlan´s, dependiendo de la criticidad de los recursos y servicios involucrados, con el fin de contribuir al control de acceso, optimizar el rendimiento en la red y garantizar que los servidores y los usuarios no ocupan el mismo segmento de red.

- Todos los componentes de red deben estar actualizados a su último paquete de seguridad estable.

- Los componentes de red deben ser monitoreados todo el tiempo para asegurar su correcta configuración y seguridad basada en las líneas base definidas por el área de seguridad de la información.

- Únicamente los servicios requeridos deben estar habilitados. Aquellos servicios de red que no se necesiten deberán ser deshabilitados.

- Todos los accesos remotos a la red deben ser autorizados por el administrador de red y el líder de seguridad de la información.

- Los funcionarios(as), contratistas o terceros que desarrollen actividades en los sistemas de información de la Entidad de manera remota, deben utilizar equipos de cómputo seguros que garanticen la no afectación de la seguridad de la red.

- Todas las conexiones entrantes (incoming) y salientes (outbound) entre la red de la Personería de Bogotá, D.C y cualquier otra red debe realizarse a través de dispositivos firewall y deberán usar protocolos NAT/PAT para realizar traducción de direcciones IP y así evitar divulgación externa de los direccionamientos internos de la entidad; en caso de poder usar NAT/PAT se

deberán configurar listas de acceso donde se garantice que únicamente personal autorizado pueda visualizar estos direccionamientos.

- Todo equipo o servicio que sea expuesto en la red externa deberá ser ubicado en una zona desmilitarizada (DMZ) la cual debe ser segmentada mediante dispositivos firewall.

- Estos servicios expuestos serán protegidos mediante el Web Application Firewall que ha destinado la Personería de Bogotá, D.C para la protección contra ataques informáticos.

- La información de direccionamiento interno, segmentación de red y enrutamiento se encuentra clasificada como confidencial y solo personal autorizado puede acceder a la misma.

- La totalidad de reglas configuradas en los dispositivos firewall deben estar documentadas, justificadas y aprobadas; dicha documentación deberá ser verificada con una periodicidad mínima de 6 meses.

- Todos los dispositivos sin excepción alguna que sean ingresados a las redes de datos Corporativas (incluyendo equipos de cómputo, impresoras, escáner, dispositivos de comunicaciones, entre otros) deben ser previamente registrados y configurados por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC.

- Cuando un componente tecnológico es registrado para uso en las redes corporativas un nombre de red y dirección IP le será asignado de acuerdo al mecanismo establecido por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC. La información básica del propietario del componente, descripción y función debe ser registrada por el Administrador de dicho Componente o a quien designe.

- La definición y diseño del direccionamiento de las redes, así como la aprobación de asignación de direcciones IP fijas en la red es responsabilidad del Administrador de Redes y Telecomunicaciones.

- Todo componente tecnológico que sea ingresado a las redes corporativas debe cumplir con los requerimientos de seguridad y estándares mínimos establecidos por cada Administrador de Componente.

- Es responsabilidad de la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC realizar revisiones periódicas de las configuraciones y estándares aplicados en los diferentes componentes tecnológicos con el fin de evaluar y velar por el cumplimiento de los requerimientos de aseguramiento de plataforma.

4.2 Transferencia de Información

- La Personería de Bogotá D.C., establecerá mecanismos seguros para la transferencia de información institucional internamente y con terceros, en cumplimiento de sus funciones y obligaciones legales.

- La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC., proporcionará las herramientas para garantizar la seguridad de la información, durante la transferencia a nivel interno y externo.

- La Entidad proporcionará tecnologías de acceso remoto a sus funcionarios(as) a través de medios como VPN (Red virtual privada), y autorizará su uso de forma particular cuando así se requiera. La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, garantizará un adecuado esquema de seguridad para los mismos.

- Todos los computadores de la entidad que sean accedidos a través de herramientas de acceso remoto deben ser protegidos por mecanismos de control de acceso aprobados por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC.

- La conexión directa entre los sistemas de información de la Entidad y otra organización o tercero vía redes públicas de datos como Internet, requieren de la aprobación de la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, quien definirá los mecanismos de seguridad apropiados.

- La Personería de Bogotá D.C., se reserva el derecho de cancelar y/o terminar la conexión a sistemas de terceros, que no cumplan con los requerimientos internos de seguridad y confidencialidad establecidos o acordados.

- Antes de autorizar y establecer las conexiones con sistemas de información de terceros para la trasferencia o consulta de información institucional, se deben establecer Acuerdos de Confidencialidad entre las partes, para lo cual se contará con la participación de la Oficina Asesora de Jurídica de la Personería de Bogotá D.C.

- Está prohibido el uso de herramientas de acceso remoto o de transferencia de información que no hayan sido autorizadas por la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC.

- Está prohibido el envío o intercambio de información **clasificada, reservada o sensible**, sin la autorización del responsable o Jefe inmediato.

- Para la transmisión o envío de información **clasificada, reservada o sensible** a través de medios electrónicos, incluido el correo institucional, se debe asegurar de aplicar las medidas de seguridad necesarias y como mínimo, cumplir con los lineamientos establecidos en la política de controles criptográficos.

- Está prohibido utilizar el correo electrónico personal, para el envío y recepción de información institucional **clasificada, reservada o sensible.**

- No está permitido el envío o almacenamiento de información institucional **clasificada, reservada o sensible** a través de plataformas gratuitas como (wetransfer, google drive, Dropbox, WhatsApp, Messenger, etc.) o cualquier servicio diferente a Office 365 institucional.

- El servicio de correo electrónico institucional debe ser utilizado exclusivamente para las tareas propias de la función desarrollada por la Personería de Bogotá D.C. El uso del servicio de correo electrónico de la Personería de Bogotá D.C., para fines personales no está autorizado.

- Todo funcionario(a) o contratista inscrito en la Personería de Bogotá D.C., dispondrá de una cuenta de correo electrónico activa, y para su creación se debe seguir con el procedimiento “Gestión de usuarios” Código: 03-PT-01” establecido de la Personería de Bogotá, D.C.

- El servicio de correo electrónico oficial de la Personería de Bogotá, D.C., es el aprobado por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC ; los funcionarios(as), contratistas y terceros reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su entera responsabilidad.

- La clave de acceso al servicio de correo electrónico es personal e intransferible, no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información - SGSI de la Personería de Bogotá, D.C.

- Las contraseñas de las cuentas de correo institucional genéricas o que no estén asociadas a un usuario particular, (Por ejemplo prensa@personeriabogota.gov.co), deberán ser cambiadas cuando la persona encargada de administrarla sea retirada de la Entidad o trasladada de dependencia, o cese su responsabilidad sobre la cuenta de correo.

- De ser estrictamente necesario y cuando exista justificación para ello, la Personería de Bogotá D.C., podrá supervisar el uso del servicio de correo electrónico corporativo respetando los derechos del titular de la cuenta de correo electrónico, para lo cual el usuario propietario de la misma debe ser previamente informado del procedimiento a realizar.

- La vigencia de la cuenta para funcionarios(as) y contratistas comprende el periodo desde la fecha de ingreso o firma del contrato y finaliza el último día de la fecha de retiro o terminación/suspensión del contrato.

- El uso de la cuenta de correo es con fines del cumplimiento de las funciones y/o obligaciones contractuales, y su uso es de carácter obligatorio, en ella llegará información oficial de conocimiento necesario para los funcionarios(as) y contratistas de la Entidad.

- Se prohíbe el uso de cuentas de correo gratuito con propósitos institucionales o cuentas de suscripción gratuita a otros proveedores.

- La Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, será la encargada de establecer las cuotas y límites de almacenamiento para las cuentas de correo electrónico institucionales de acuerdo a las necesidades propias de la entidad.

- Es responsabilidad del funcionario(a) o contratista depurar su cuenta periódicamente siendo él el único responsable de realizar las copias de seguridad de sus correos.

- El usuario(a) debe leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.

- Solo podrán enviar correos masivos aquellas dependencias que por su naturaleza de socialización y sensibilización lo requieran a través de la cuenta de correo del jefe de la dependencia; tales como (Secretaría General, Dirección de Talento Humano, Oficina Asesora de Divulgación y Prensa y la Subdirección de Gestión Documental, Recursos Humanos, etc.).

- El incumplimiento por parte del funcionario(a) y/o contratista de los lineamientos o el mal manejo de su cuenta de correo institucional, puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, la suspensión del mismo y en un último caso la notificación a la Dirección

de Talento Humano y/o Dirección Administrativa y Financiera para que proceda disciplinariamente.

- No están autorizados los siguientes usos del servicio de correo electrónico y pueden constituir un incidente de seguridad de la información con las consecuencias legales correspondientes:

  Exceder los servicios para los cuales se autorizó la cuenta.

  Enviar mensajes para la difusión de noticias, mensajes políticos, religiosos, correos sin identificar plenamente a su autor o autores o enviar anónimos.

  Difundir "cadenas" de mensajes que saturen el servicio entre otros problemas.

  Perturbar el trabajo de los demás enviando mensajes que puedan interferir con sus actividades laborales.

  Agredir o lesionar directa o indirectamente a otras personas a través del envío de mensajes con contenido que atente contra la integridad y el buen nombre de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la Entidad o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta la Entidad.

  Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.

  Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.

  Suscribir las cuentas de correo institucional en servicios externos (comerciales) con fines no gubernamentales ni afines a la misión institucional.

  Enviar correos de información masivos sin estar autorizado para ello.

  Envío de mensajes no deseados o que puedan ser considerados como SPAM.

5. RESPONSABLES

Dirección de Tecnologías de la Información y las Comunicaciones – DTIC

Establecer las condiciones necesarias para garantizar la transmisión segura de la información institucional, a través de las redes de datos y comunicaciones de la Entidad.

Designar el personal idóneo para que establezca, configure y administre los parámetros de uso y seguridad de los equipos y servicios de redes y transferencia de información institucional para garantizar la seguridad de la información institucional.

Líder de Seguridad de la Información

Realizar el seguimiento al cumplimiento de los lineamientos establecidos en la presente política y proponer las modificaciones que considere pertinentes.

Funcionarios(as) y contratistas

Dar cumplimiento a los lineamientos establecidos en la presente política e informar oportunamente a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, sobre cualquier violación o situación que represente un riesgo para la seguridad de la información institucional.

6. POLÍTICAS RELACIONADAS

Política de control de acceso
Política de internet
Política de seguridad en la nube
Política de seguridad de redes inalámbricas

Revisó:

FIRMA DEL(LA) PRESIDENTE
Comité Institucional de Gestión y Desempeño

Política Controles en la Red de Datos y transferencia de Informacion

Informe de auditoría final 2020-06-25

Fecha de creación:	2020-06-24
Por:	Henrry Diaz (hdiaz@personeriabogota.gov.co)
Estado:	Firmado
ID de transacción:	CBJCHBCAABAAyGZtuyhy5qz3_4xrqYCdYupEXhsFzj-w

Historial de “Política Controles en la Red de Datos y transferencia de Informacion”

Henrry Diaz (hdiaz@personeriabogota.gov.co) ha creado el documento.
2020-06-24 - 16:34:16 GMT- Dirección IP: 190.158.137.240.

El documento se ha enviado por correo electrónico a Luz Estella García Forero (legarcia@personeriabogota.gov.co) para su firma.
2020-06-24 - 16:34:53 GMT

Luz Estella García Forero (legarcia@personeriabogota.gov.co) ha visualizado el correo electrónico.
2020-06-25 - 16:38:34 GMT- Dirección IP: 181.61.183.223.

Luz Estella García Forero (legarcia@personeriabogota.gov.co) ha firmado electrónicamente el documento.
Fecha de firma: 2020-06-25 - 16:39:11 GMT. Origen de hora: servidor.- Dirección IP: 181.61.183.223.

El documento firmado se ha enviado por correo electrónico a Henrry Diaz (hdiaz@personeriabogota.gov.co) y Luz Estella García Forero (legarcia@personeriabogota.gov.co).
2020-06-25 - 16:39:11 GMT