SECRETARÍA
TIC Y CTEI

POLÍTICA DE USO CORREO ELECTRÓNICO INSTITUCIONAL 2024 - 2027

ALCALDÍA DE CAJICÁ

“CAJICÁ IDEAL 2024 - 2027”

ING. FABIOLA JÁCOME RINCÓN
ALCALDESA MUNICIPAL

Ing. Nicolás Mauricio Castiblanco Navarrete
Secretario de TIC- CTeI

Ing. Javier Enrique Lamprea
Profesional Gobierno Digital TIC - CTeI

Ing. Edwin Andrade Ayala
Profesional Especializado TIC – CTeI - Contratista

CAJICÁ, JULIO 2024

POLÍTICA DE USO
CORREO ELECTRÓNICO INSTITUCIONAL 2024 - 2027

OBJETIVO

Por medio de esta política se establecen lineamientos, directrices y recomendaciones mínimas sobre el uso adecuado y permitido del correo electrónico institucional asignado a funcionarios, contratistas y colaboradores de la Alcaldía Municipal de Cajicá, a través de la aplicación de esta política garantizaremos mejores niveles en la confidencialidad, privacidad y seguridad de la información al interior de nuestra entidad.

ALCANCE

Con el fin de establecer las responsabilidades, normas y buenas prácticas para el manejo seguro y adecuado del correo electrónico, respaldando la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI de la entidad y con el fin de evitar la pérdida y/o daño de los recursos e información, se establece esta política, la cual aplica de manera obligatoria para todos los funcionarios, contratistas, colaboradores y todo aquel que tenga asignada una cuenta de correo electrónico sobre el dominio **@cajica.gov.co.**

DOCUMENTOS DE REFERENCIA

- Política de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Política de Seguridad Informática.
- Política de Tratamiento de Datos Personales.
- Plan Estratégico de Tecnologías de la Información y Comunicaciones – PETI.
- Plan de Seguridad y Privacidad de la información.
- Plan de Riesgos de Seguridad y Privacidad de la Información.

CONCEPTOS Y DEFINICIONES

Usuario: Toda persona que ha recibido acceso a cualquier recurso tecnológico (correo electrónico, cuenta de dominio, bases de datos, aplicaciones corporativas entre otras) previa autorización con el propósito del cumplimiento de sus funciones.

Correo electrónico: también conocido como e-mail, es un servicio de red que permite mandar y recibir mensajes con múltiples destinatarios o receptores, situados en cualquier parte del mundo.

Contraseña: es una combinación de palabras, frases y signos que sirven de autentificación ante un sistema de información y por lo tano debe mantenerse en secreto para evitar la suplantación de identidad, pérdidas y fugas de información.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato personal semiprivado: Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información (ejemplo: dato financiero y/o crediticio).

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Confidencialidad: Pilar de seguridad de la información orientado al propósito de contar con procesos de lectura de información sólo al alcance de quienes deben tener autorización de acceso a los mismos.

Disponibilidad: Requerimiento a los sistemas de información para que siempre estén prestos a ser usados; sin embargo, por la naturaleza de los componentes electrónicos que los conforman, nunca habrá disponibilidad total.

Información: Conjunto de datos que organizados en determinado contexto tienen significado o importancia.

Información pública: Es aquella en poder de los entes obligados contenida en documentos, archivos, datos, bases de datos, comunicaciones y todo tipo de registros que documenten el ejercicio de sus facultades o actividades, que consten en cualquier medio, ya sea impreso, óptico o electrónico, independientemente de su fuente, fecha de elaboración, y que no sea confidencial o reservada. Dentro de la información pública se encuentra un subconjunto de información denominado “información oficiosa”, la cual debe de ser publicada de forma inmediata sin que ninguna persona lo solicite. Esta información puede estar impresa o colgada en los sitios web de las instituciones y deben entregártela en el mismo momento en que lo solicites.

Información reservada: Es la información pública cuyo acceso se restringe de manera expresa, en razón de un interés general durante un periodo determinado y por causas justificadas. Por ejemplo, los planes militares secretos, las negociaciones internacionales o cualquier tipo de negociación o discusión que se tenga, mientras no se adopte una decisión definitiva. O toda aquella información que esté relacionada con la investigación o persecución de actos ilícitos o que genere una ventaja indebida en perjuicio de un tercero.

Información confidencial: Es la información privada en poder del Estado cuyo acceso público se prohíbe por mandato constitucional o legal en razón de un interés personal jurídicamente protegido. Es decir, la información referente a la intimidad personal y familiar, al honor y propia imagen, así como archivos médicos cuya divulgación constituiría una invasión a la privacidad de la persona. A esta información solo tendrán acceso las personas que son dueñas de ella. Dentro de la información confidencial están los datos personales la cual es la información privada de una persona, como por ejemplo su nacionalidad, domicilio, patrimonio, dirección electrónica, número de teléfono o cualquier otra parecida.

Integridad: Pilar de seguridad de la información, desde donde se orienta el propósito de tener procesos de escritura de información solo al alcance de quienes deben tener autorización a éstos.

Ingeniería social: Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Asimismo, técnica utilizada para obtener datos, acceso o privilegios a sistemas de información o dispositivos, de tal modo que permite la ejecución de acciones maliciosas para comprometer información e infraestructura tecnológica de una organización.

Dispositivo móvil: aparato de tamaño pequeño con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada y pueden ser transportados a cualquier lugar.

Spam: El spam son correos electrónicos no solicitados enviados en ráfagas masivas. Si bien los filtros de spam modernos capturan y bloquean la mayoría de los correos electrónicos no deseados, es posible que uno se escape y entregue contenido malicioso a la bandeja de entrada de un usuario.

Phishing: Los correos electrónicos de phishing utilizan ingeniería social, suplantación de identidad y otras técnicas para engañar al usuario para que haga algo por el atacante. Los ataques de phishing se pueden utilizar para lograr diversos objetivos, incluido el robo de credenciales, datos o dinero de los usuarios.

Business Email Compromise (BEC): Los ataques BEC son una forma específica de correo electrónico de phishing diseñado para robar dinero de una organización. El suplantador se hará pasar por alguien alto en la jerarquía de una organización y utilizará el estatus y la autoridad de esa persona para instruir a un empleado para que envíe dinero a una cuenta controlada por el atacante.

Entrega de malware: Los correos electrónicos pueden contener malware directamente en sus archivos adjuntos o dirigir a los destinatarios a sitios maliciosos que entregan malware. Los correos electrónicos de phishing son uno de los principales mecanismos de entrega para ransomware, troyanos y otros tipos de malware.

Toma de control del sistema: Un ataque de phishing exitoso puede comprometer las credenciales del usuario o enviar malware a la computadora del destinatario, permitiendo al atacante apoderarse de esa computadora. Luego, la computadora se puede agregar a una botnet para usarla en la denegación de servicio distribuido (DDoS) y otros ataques.

Disclaimer: Es un aviso legal o descargo de responsabilidad es una referencia a las notificaciones que se encuentran comúnmente en e-mensajes de correo electrónico y páginas web, que establece los derechos del lector de un documento en particular y la responsabilidad del usuario y del autor.

POLÍTICA DE USO DE CORREO ELECTRÓNICO INSTITUCIONAL

La Alcaldía Municipal de Cajicá establece pautas para el uso correcto del correo electrónico institucional, para el envío de comunicaciones internas y externas a la entidad con el fin de minimizar el impacto de amenazas y vulnerabilidades que puedan ocasionar la pérdida o robo de la información de la entidad o suplantación del dominio; razón por la cual funcionarios, contratistas, colaboradores y partes interesadas deberán acatar con responsabilidad, integridad y seguridad los lineamientos, recomendaciones y buenas prácticas establecidos en esta política.

Para nuestra entidad el uso del correo electrónico institucional es una herramienta de trabajo, la cual se ha convertido en el medio formal y oficial de comunicaciones de la entidad, esta herramienta facilita las labores propias de sus funcionarios, contratistas y colaboradores.

La Alcaldía Municipal de Cajicá se reserva el derecho de acceder a todos los datos y archivos de cualquier sistema informático utilizado. Igualmente se reserva el derecho de monitorear el contenido que se envía o recibe por correo electrónico, en cualquier momento podrá establecer e implementar medidas de seguridad para el uso de las herramientas electrónicas en pro de ofrecer un mejor servicio y proteger la seguridad de los recursos informáticos.

La Alcaldía Municipal de Cajicá, se reserva el derecho de deshabilitar, modificar o eliminar las cuentas de correo institucional en las cuales se evidencie un uso inadecuado o que incurran en el incumplimiento de las políticas plasmadas en el presente documento y en la Política de Seguridad de la Información, las cuentas de correo electrónico deben ser gestionadas acorde con el procedimiento Gestión de los recursos tecnológicos de la entidad.

Responsabilidades de los Usuarios

- El uso del correo electrónico está orientado único y exclusivamente para el desarrollo de sus actividades en ejercicio de sus funciones a nivel institucional.

- El correo institucional es de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la contraseña, cambiarla periódicamente bajo los parámetros de contraseñas seguras y no compartirla ni divulgarla en ninguna circunstancia.

- El usuario es responsable de todas las actividades y transacciones que se realicen desde la cuenta de correo electrónico asignada.

- El usuario responsable de la cuenta de correo electrónico se compromete a reportar oportunamente a la mesa de servicios de TI, cualquier incidente de seguridad presentado con su cuenta institucional o acceso no autorizado.

- El usuario responsable es consciente de que los mensajes de correo electrónico son válidos en un proceso jurídico (Ley 524 de 1999) y revisten la misma fuerza probatoria que tienen los documentos físicos.

- El usuario debe garantizar que los mensajes emitidos desde su cuenta de correo electrónico no contengan palabras irrespetuosas, mensajes obscenos, difamatorios, ni material alguno que pueda dañar la reputación de la entidad y la propia.

- El usuario no debe enviar ni contestar cadenas de correo o cualquier otro mensaje considerados sospecho de contener spam, phishing, Business Email Compromise (BEC), Entrega de Malware, Toma de Control del Sistema entre otras modalidades.

- El usuario debe velar porque la gestión de la información contenida en su correo electrónico sea idónea y de carácter institucional; para ello debe revisar frecuentemente la bandeja de entrada y salida, de igual manera utilizar la herramienta para actividades relacionadas con el cargo.

- Se recomienda al usuario, eliminar los mensajes que no deban conservarse y archivar el resto en carpeta o subcarpetas etiquetadas acorde con su contenido. El usuario debe reportar a la mesa de servicios de TI, todo correo de procedencia desconocida, o sospechoso, SPAM, correo basura o correo no deseado que sea recibido en los buzones de correo electrónico, este tipo de correo debe ser eliminado de manera inmediata y no debe abrirse para evitar posibles riesgos de virus o ataques informáticos.

Restricciones de uso de correo institucional

- El usuario no debe configurar la cuenta de correo electrónico en los dispositivos de uso personal a través de clientes de correo electrónico no oficiales, o que no estén relacionados con la plataforma utilizada.

- El usuario no debe crear ningún tipo de regla o configuración, para la replicación automática de mensajes desde su cuenta de correo electrónico institucional hacia cuentas internas o externas.

- El usuario no debe utilizar la cuenta de correo institucional para configurar cuentas en redes sociales y/o servicios de mensajería instantánea.

- El usuario no debe utilizar el correo electrónico institucional para el envío de propaganda, ofertas, negocios personales, avisos publicitarios, propaganda política o cualquier información ajena a las laborales propias del cargo.

- El usuario no debe leer ni divulgar los correos ajenos o acceder a archivos de correo electrónico que estén en el buzón de otra persona. Excepto si se requiere con fines de auditoría.

- El usuario no debe generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantando su identidad, también queda prohibido él envió de correos masivos orientados a fines diferentes al institucional.

- El usuario no debe utilizar el correo electrónico con el fin de realizar algún tipo de acoso, difamación, calumnia o con intención de intimidar, insultar, injuriar o cualquier otra forma de actividad hostil o maliciosa.

- El usuario no debe compartir los contactos o listas de distribución de la entidad con personas externas para el uso de propagandas, negocios, ofertas, avisos publicitarios entre otros.

Cambio de contraseñas cuentas de correo electrónico

Para garantizar la seguridad de nuestras cuentas de correo electrónico, todas las contraseñas deben tener al menos 10 caracteres, incluyendo letras mayúsculas, minúsculas, números y caracteres especiales. Las contraseñas deben cambiarse cada 60 días, no deben reutilizarse las últimas 5 contraseñas, y los usuarios deben mantenerlas confidenciales.

Es obligatorio cambiar la contraseña tras un incidente de seguridad, asignación de una nueva cuenta o recuperación de una cuenta.

Caducidad de las cuentas de correo electrónico

La administración de las cuentas de correo electrónico se realizará desde la Secretaria de TIC y CTEI, esta administración está acorde con el procedimiento de administración de cuentas de usuario, las cuentas serán desactivadas cuando el usuario esté haciendo un mal uso de dicho servicio o en el monitoreo de las mismas se encuentre algún riesgo de seguridad de la información.

Las cuentas de correo electrónico se mantendrán activas mientras esté vigente la relación contractual de la persona con la Alcaldía Municipal de Cajicá, la cual se reserva el derecho de crear, modificar y/o eliminar cuentas de correo electrónico.

Firma del correo y disclaimer

Los usuarios de correo electrónico institucional deben unificar la firma del correo electrónico y el disclaimer de acuerdo con la actividad a desarrollar, teniendo en cuenta la Política de Tratamiento de Datos Personales de la entidad y normatividad relacionada.

Canales de soporte y reporte de eventos de seguridad

Los canales autorizados para el reporte de eventos o debilidades de seguridad de la información son los siguientes:

1) Vía correo electrónico: soportetic@cajica.gov.co.

2) Números de contacto:

   Telefónico: PBX 8767077 ext. 2013,
   Celular: 3132790497.

3) WhatsApp 3132790497.

Nota: El uso no adecuado o incumplimiento de las medidas definidas en la presente Política de Uso de Correo Electrónico Institucional, da lugar a la aplicación de las medidas administrativas, disciplinarias o legales a las que haya lugar.