Función Pública

Informe de Seguimiento administración y seguridad correo interno - Outlook

Evaluación Independiente

OFICINA CONTROL INTERNO

Versión 1

Abril de 2026

1. Objetivo

En ejercicio de las funciones legales asignadas a la Oficina de Control Interno - OCI, especialmente aquellas relacionadas con la evaluación y seguimiento al Sistema de Control Interno y a la verificación del cumplimiento de los controles definidos en los procesos y actividades del Departamento, orientadas a constatar que dichos controles sean aplicados por los responsables de su ejecución, y en concordancia con los principios de seguridad de la información establecidos en el Manual de Políticas de Seguridad de la Información, particularmente en lo relacionado con el uso adecuado del correo electrónico institucional y el manejo de correos masivos, la OCI solicitó el diligenciamiento por parte de la Oficina de Tecnologías de la información y las Comunicaciones – OTIC, de un cuestionario que tuvo como objetivo indagar la gestión de control reactiva/correctiva efectuada por los actores responsables de dicha Oficina, ante los hechos ocurridos por el incidente de seguridad del correo institucional al final de la vigencia pasada y principios de esta. Esto con el fin de analizar la actuación y determinar el grado de efectividad de los controles subyacentes.

Las observaciones registradas en el presente informe de seguimiento coadyuvan a fortalecer el ambiente de control interno actual.

2. Alcance

✓ Información del incidente de seguridad y los controles aplicados, bajo los elementos inmersos en el cuestionario aplicado a la OTIC, relacionada con:

- Explicación detallada de los hechos ocurridos.
- Gobierno y responsabilidad en la administración del correo interno (Outlook).
- Gestión de incidentes.
- Controles de autenticación y acceso.
- Configuración técnica del correo
- Administración de buzones
- Monitoreo y detección
- Respuesta y mejora continua.

3. Resultados de la verificación

Sobre la información solicitada por medio del cuestionario que cubre los elementos descritos en el alcance, se generaron los siguientes resultados:

3.1. Hechos ocurridos

El 28 de noviembre 2025 se identificaron los primeros correos sospechosos dirigidos a funcionarios específicos. Estos mensajes iniciales sirvieron como "carnada" para probar los filtros de seguridad de la entidad.

El 02 de diciembre 2025 el incidente escaló significativamente. Los atacantes lograron comprometer el buzón de un funcionario real, lo que les permitió enviar correos masivos internos. Al provenir de una fuente "confiable" dentro de la misma organización, el correo eludió sospechas iniciales. El correo solicitaba a los usuarios hacer clic en un enlace externo para ingresar datos (Suplantación de identidad o credential harvesting). Desafortunadamente, la familiaridad con el remitente provocó que varios funcionarios cayeran en el engaño, comprometiendo sus cuentas.

Lo anterior, derivo puntualmente en:

- La circulación de un correo fraudulento (phishing), el cual estaba siendo enviado a diferentes cuentas institucionales y a funcionarios de la entidad, utilizando de manera engañosa la dirección servidorespublicos@funcionpublica.gov.co
- El envío de correos masivos fraudulentos (phishing), los cuales estaban siendo enviados a diferentes cuentas personales externas, utilizando cuentas de correo interno de manera engañosa, como se puede observar en la imagen siguiente se puede observar un ejemplo de los correos enviados:

Observación: Respecto a la gestión inicial frente al incidente, no se generó el informe respectivo, ni tampoco el mismo fue escalado al Comité Institucional de Gestión y Desempeño, como lo dictan las políticas de seguridad de la información para el manejo de incidentes (Ver Manual de políticas de seguridad de la información v1, numeral 23. Reporte y tratamiento de incidentes de seguridad, publicado en el SIGP).

3.2 Gobierno y responsabilidad

Asignación de responsables: La Entidad tiene asignados actualmente dos profesionales que ejecutan la labor de administración del correo interno (Outlook/Exchange) un ingeniero de planta temporal y otro de carrera administrativa y pertenecientes a la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.

Los roles y responsabilidades se encuentran documentadas en el formato de Evaluación del Desempeño para Servidores Vinculados en Nombramiento Temporal, donde en el compromiso laboral “Brindar soporte especializado a la infraestructura tecnológica de la Entidad y emitir conceptos técnicos en caso de requerirse”, se concreta el compromiso a través de los Soportes técnicos con el proveedor, soportes especializados registrados en la herramienta mesa de servicio ProactivaNet (Administración cuentas de usuario y correo, restauración de backups, administración DNS, administración DHCP, administración políticas de grupo, administración de servidores). Ruta evidencia: \\Yaksa\10030otic\2026\DOCUMENTOS_APOYO\EVALUACIONES_DESEMPEÑO\EVALUACIONES EVENTUALES\10_2025-01_2026\GST.

Respecto al reporte y tratamiento de incidentes, se presentó una falla en el escalamiento y gobernanza, debido a que la OTIC en su momento no convocó al Comité Institucional de Gestión y Desempeño, impidiendo una respuesta estratégica más coordinada, como lo establece el manual de Seguridad de la Información del Departamento.

De otro lado, el Departamento no tiene contratado proveedores externos con niveles y accesos de administración sobre el correo.

3.3 Gestión de incidentes

Antecedentes

Aunque los ataques comenzaron de forma leve el 28 de noviembre de la vigencia 2025, el informe de revisión de seguridad generado por Check Point Harmony (Licencia adquirida

en el mes de enero a traves de la nube publica), el cual proporciona una visión general semanal de las amenazas detectadas en correos electrónicos y otras aplicaciones de colaboración protegidas, y cómo fueron gestionadas por la política, mostró un crecimiento exponencial en diciembre de Emails Phishing sobre los 19,343 eventos que afectaron toda las cuentas del dominio “funcionpublica.gov.co”. El sistema de seguridad logró filtrar la mayoría de los ataques, pero el riesgo persistió debido a la naturaleza del phishing (donde basta con que un solo usuario haga clic para comprometer la red).

Los informes de Check Point mencionados se encuentran en la ruta: \\yaksa.dafp.local\10030otic\2025\DOCUMENTOS_APOYO\SEGURIDAD\VULNERABILIDADES\CHECKPOINT.

Esquemas de soporte y apoyo

Si bien Función Pública no dispone actualmente del servicio de un Centro de Operaciones de Seguridad – SOC, la OTIC implementó la solución Check Point Harmony en modalidad de nube pública, logrando una efectividad del 100% en la detección y eliminación de ataques de phishing en el correo institucional. Además se tiene programado a corto plazo la implementación de XDR (Extended Detection and Response – Detección y respuesta ampliadas) con el fin de establecer un nivel de protección mediante la integración de datos de múltiples capas, incluyendo red, nube, correo electrónico y dispositivos finales, ofreciendo una visión unificada y una respuesta automática más rápida ante amenazas complejas (integración con el Firewall(Fortigate) y alarmas).

Gestion de contención adelantada

Ante la detección de las amenazas inmersas en la vulnerabilidad acaecida con el correo, se procedió con la ejecución del protocolo de respuesta, apoyado por las capacidades de remediación automática de la herramienta Check Point Harmony. Para ello:

- ✓ Se ejecutó una acción de remediación masiva mediante la configuración de una GPO (Group Policy Object) en el Directorio Activo, obligando a todos los usuarios a realizar el cambio de contraseña en su próximo inicio de sesión. Especificamente, las actividades y cambios que se realizaron en el directorio activo y en la política de contraseñas para el ingreso de los usuarios a los aplicativos que están integrados y para prevenir futuros inconvenientes fortaleciendo los sistemas de información internos como externos, fueron:

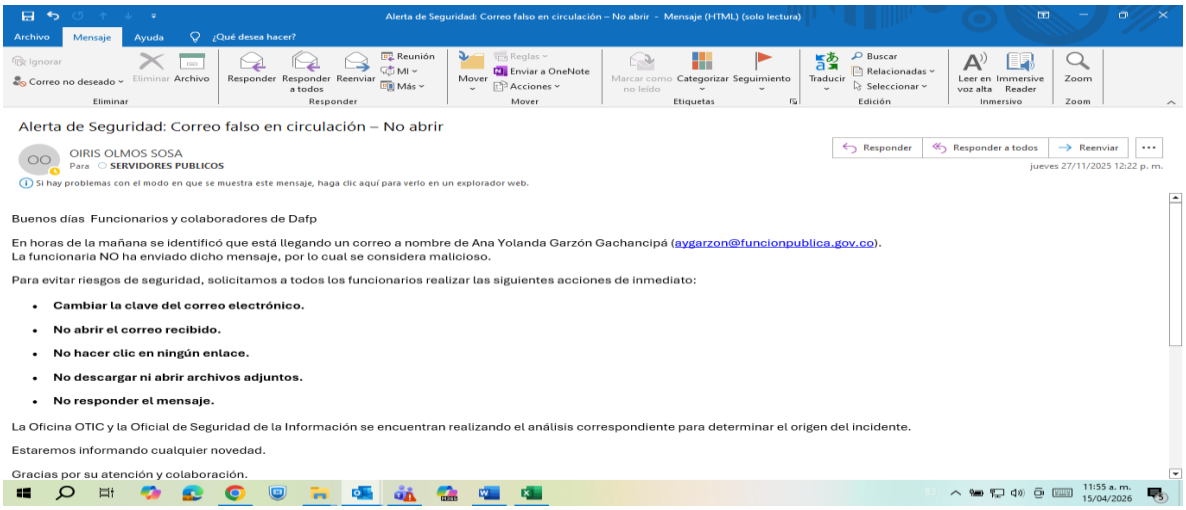
- Se modifican los días de cambio de contraseña para todos los usuarios de la entidad de 60 a 45 días.
- Se aumenta el numero de caracteres para la creación de contraseñas de 12 a 14 caracteres.
- Se valida que este activada la opción de contraseñas con minúsculas mayúsculas y símbolos.
- De inmediato desde el 1 de diciembre de 2025 se forzó la política y se envió el mensaje de cambio de contraseña para todos los usuarios de la entidad.
- Respecto a los usuarios afectados que estaban por VPN y que no pudieron cambiar la contraseña, la OTIC brindo ayuda de manera remota y se solucionó su ingreso a los aplicativos.

Soportes en la ruta: \\Yaksa\10030otic\2025\DOCUMENTOS_APOYO\SEGURIDAD\VULNERABILIDADES

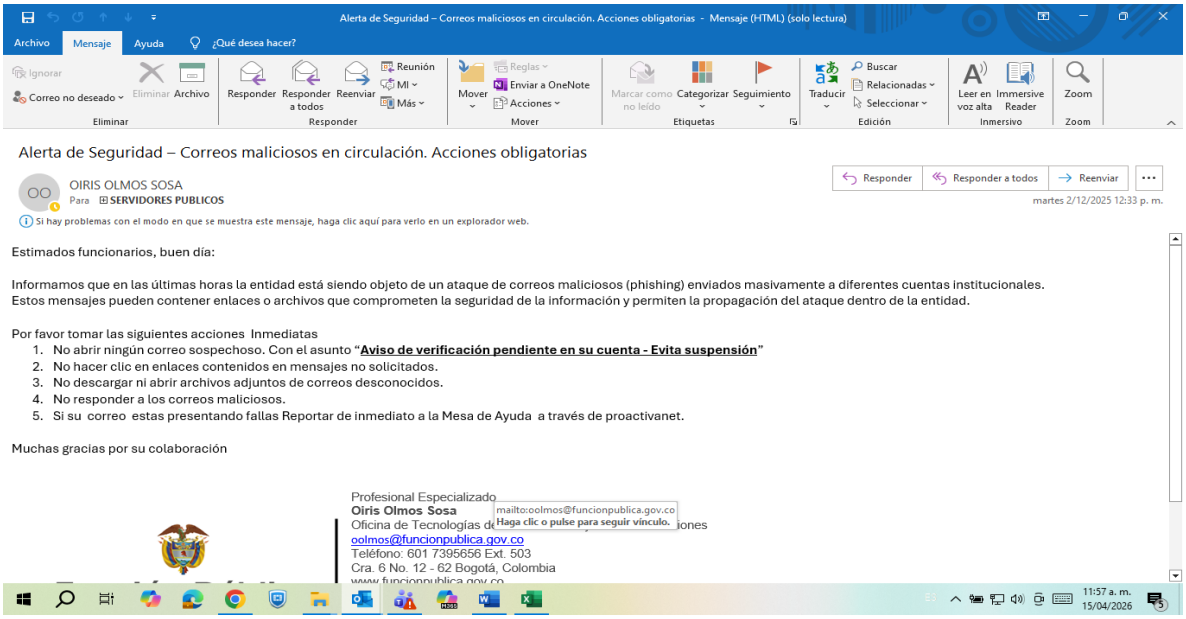
✓ Como medida de mitigación, se habilitó el Doble Factor de Autenticación (2FA) inicialmente para el personal afectado y tras una campaña institucional en la semana del 26 al 30 de enero de 2026, se estandarizó para todas las cuentas de la organización. Acorde a lo anterior, se verifico la campaña de autenticación a traves de los correos y piezas de comunicación respectivas que fueron aplicadas (Ruta: \\yaksa.dafp.local\10030otic\2026\DOCUMENTOS_APOYO\SEGURIDAD\DOBLE FACTOR).

✓ Respecto a la revisión de reglas y reenvío, se efectúo a cada uno de los usuarios afectados: cambio inmediato de la contraseña del correo electrónico, revocación de todas las sesiones activas, eliminación de dispositivos móviles asociados a la cuenta, eliminación de reglas de correo configuradas, activación del doble factor de autenticación (MFA), revisión del equipo desde el cual se accede a la cuenta. Luego se realizo masivamente este proceso para los demas usuarios

✓ Una vez analizado el incidente, La OTIC procedió a informar a través del correo institucional a todos los sevidores los hechos sucedidos e indicandoles algunas acciones a realizar. A continuación se presentan algunos de los correos remitidos:



Fuente: Correo remitido por la Oficial de seguridad el 27 de noviembre de 2025



Fuente: Correo remitio por el Oficial de seguridad de la Información informando que la entidad está siendo objeto de un ataque de correos maliciosos (phishing) enviados masivamente a diferentes cuentas institucionales y las medidas preventivas a tener en cuenta.

Respecto a la documentación del incidente, inicialmente el Jefe de la OTIC y el CISO avisaron verbalmente a la Dirección General, con el fin de enterar el suceso y obtener el aval para la generación de una pieza informativa correspondiente al incidente de seguridad que se estaba presentando, para ser comunicada a Función Publica en su pagina principal

y al Grupo de Respuesta a Emergencias Cibernéticas de Colombia – Colcert. El aviso rezó así:

"Aviso de Seguridad

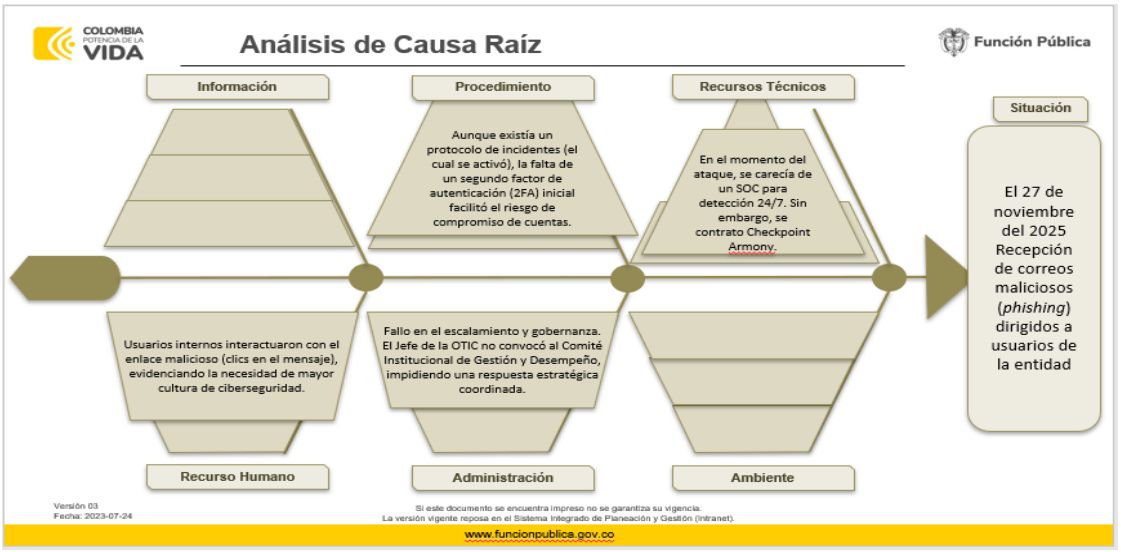
Se ha identificado un intento de phishing que suplanta al Departamento Administrativo de la Función Pública con el fin de engañar a usuarios y entidades mediante el envío de correos fraudulentos.

Por favor tomar las siguientes recomendaciones:

- *No abrir enlaces ni copiar url que se encuentren dentro del cuerpo del mensaje*
- *No suministrar información personal o institucional en enlaces desconocidos*
- *Reporte al equipo de seguridad de su entidad*

El Dafp continua adelantando las acciones técnicas correspondientes para mitigar el incidente"

También, se adelantó por demás un análisis de causa raíz, en el cual se evidencia un archivo en Power Point que tiene esquematizado el analisis de causa así:



Fuente: presentación análisis de causa raíz del incidente presentado (05-01-2026)

La presentación que soporta el análisis de causa raíz generada por la OTIC presento los siguientes elementos de causa:

- Procedimentales : Aunque existía un protocolo de incidentes (el cual se activó), la falta de un segundo factor de autenticación (2FA) inicial facilitó el riesgo de compromiso de las cuentas de correo.
- Recursos técnicos: En el momento del ataque, la Entidad carecía de un SOC para detección 24/7.
- Recurso humano: Algunos usuarios internos interactuaron con el enlace malicioso haciendo click en el mensaje inmerso, desencadenando el incidente, esto demuestra debilidades en la cultura de ciberseguridad.
- Gobernanza: Fallo en el escalamiento y gobernanza. El Jefe de la OTIC asignado en su momento, no convocó al Comité Institucional de Gestión y Desempeño, impidiendo una respuesta estratégica coordinada.

No obstante, no se evidencia un reporte o informe oficial del incidente que de acuerdo a las mejores prácticas y a lo expuesto por MinTIC en la Guía N° 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información, incluya lo siguiente:

1. Información General y del Reportante:
    - Nombre y cargo de quien reporta el incidente.
    - Área o departamento afectado.
    - Información de contacto (correo, teléfono).
2. Detalles del Incidente:
    - Fecha y hora exacta en que ocurrió el evento y cuándo fue detectado.
    - Descripción detallada: ¿Qué pasó?, ¿cómo pasó?, ¿quién estuvo involucrado?
    - Tipo de incidente: Por ejemplo, phishing, malware, denegación de servicio (DoS), acceso no autorizado, pérdida de equipo.
    - Ubicación: Física o lógica (redes, servidores, aplicaciones).
3. Impacto y Alcance:
    - Análisis de causa raíz
    - Sistemas o activos de información afectados (servidores, bases de datos, dispositivos).
    - Clasificación de severidad: Alto, medio o bajo impacto.
    - Información comprometida: Tipo de datos (personales, confidenciales, financieros) y cantidad aproximada de registros.
4. Acciones y Evidencias:
    - Acciones de contención inmediatas: Medidas tomadas para frenar el incidente (apagar servidores, bloquear usuarios, aislar red).

    - Evidencias recopiladas: Capturas de pantalla, archivos maliciosos, logs de sistema.
- 5. Seguimiento y Cierre:
    - Acciones de erradicación y recuperación: Pasos para eliminar la causa y restaurar el servicio.
    - Recomendaciones para prevenir futuros incidentes similares.
    - Personas notificadas

El informe o reporte detallado, coadyuva a “Crear bases de conocimiento para los incidentes de seguridad presentados con las respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros. Lo anterior con el apoyo con la Oficina de Tecnologías de la Información y las Comunicaciones, la Dirección de Gestión de Conocimiento y la Secretaría General”, como se establece en el manual de políticas de seguridad de la información de la Entidad.

Protocolo para manejo de incidentes

Función Pública tiene documentado el Procedimiento de Gestión de incidentes de seguridad de la información, versión 2 de diciembre de 2024; dicho procedimiento se encuentra publicado en el Sistema Integrado de Planeación y Gestión – SIPG, y tiene por objetivo:

- “Gestionar de Manera Oportuna, ordenada y efectiva los incidentes y eventos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información en el Departamento Administrativo de la Función Pública, realizando acciones correctivas y preventivas que reduzcan sus impactos.
- Construir una base de conocimientos que facilite la gestión de incidentes y eventos de seguridad.
- Identificar oportunidades de mejora que reduzcan la probabilidad o impacto de eventos, incidentes y riesgos de seguridad de la información.”

Sin embargo:

- No se logró obtener evidencia de su socialización a los interesados respectivos al interior de la Entidad.
- El procedimiento no especifica claramente la necesidad de generar un informe o reporte detallado del incidente, tal y como específico en el titulo anterior.

Tratamiento de riesgos

De acuerdo con el impacto del incidente, según lo aseverado por la OTIC, en el cuestionario aplicado, se identificó la materialización de un riesgo relacionado con la pérdida de Integridad de credenciales de usuario de correo, debido a las siguientes amenazas:

- Interacción de algunos usuarios de correo con enlaces maliciosos (Phishing), permitiendo así el compromiso de cuentas institucionales.
- Ausencia de monitoreo en tiempo real por falta de un servicio de SOC para la detección temprana.

Este riesgo, así como el tipo de amenazas no han sido identificadas en la matriz de riesgos de seguridad de la información oficializado en el SGI.

Por otra parte, la OTIC efectuó el tratamiento del riesgo materializado mediante el reporte y tratamiento del incidente de seguridad el día 5 de enero 2025, activando el protocolo institucional de respuesta a incidentes. Incluyéndose la identificación de la causa raíz (phishing dirigido), la contención técnica inmediata mediante el bloqueo de URLs maliciosas y el restablecimiento de la seguridad de las cuentas afectadas mediante políticas de grupo (GPO) y 2FA. Los soportes de estas actividades se encuentran en la ruta: \\Yaksa\10030otic\2026\DOCUMENTOS_APOYO\SEGURIDAD\VULNERABILIDADES.

Así mismo, la efectividad de las herramientas de seguridad implementadas y la ejecución inmediata de los protocolos internos permitieron la mitigación del riesgo en su fase inicial, evitando una afectación de gran escala.

Sin embargo, pese a la gestión mencionada, no se evidencia en la sabana de materialización del Sistema de Gestión Institucional - SGI, este riesgo materializado y su información correspondiente:

- ✓ Código
- ✓ Proceso
- ✓ Riesgo
- ✓ Clasificación
- ✓ Causa generadora
- ✓ Descripción del evento
- ✓ Fecha descubrimiento

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

- ✓ Fecha evento
- ✓ Producto servicio afectado
- ✓ Tipo perdida
- ✓ Perdida
- ✓ Usuario descubrimiento

Por otro lado, en el informe de gestión de riesgos también contenido en el SGI tampoco se registró dicha materialización, donde se haya registrado la siguiente información:

- ✓ Impacto
- ✓ Causa inmediata
- ✓ Causa raíz
- ✓ Activos
- ✓ Probabilidad inherente
- ✓ Impacto inherente
- ✓ Zona inherente
- ✓ Probabilidad residual
- ✓ Impacto residual
- ✓ Zona residual
- ✓ Tratamiento
- ✓ Periodicidad
- ✓ N°. Controles
- ✓ Controles
- ✓ Responsables de los controles
- ✓ N°. Acciones
- ✓ Acciones
- ✓ Responsables de las acciones
- ✓ Fecha materialización
- ✓ Acontecimiento materialización

Según la Política de Administración de Riesgos en Función Pública, cuando se materializan riesgos identificados en la matriz de riesgos institucionales sean de gestión o de seguridad digital, el líder del proceso debe aplicar las acciones descritas a continuación:

- Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

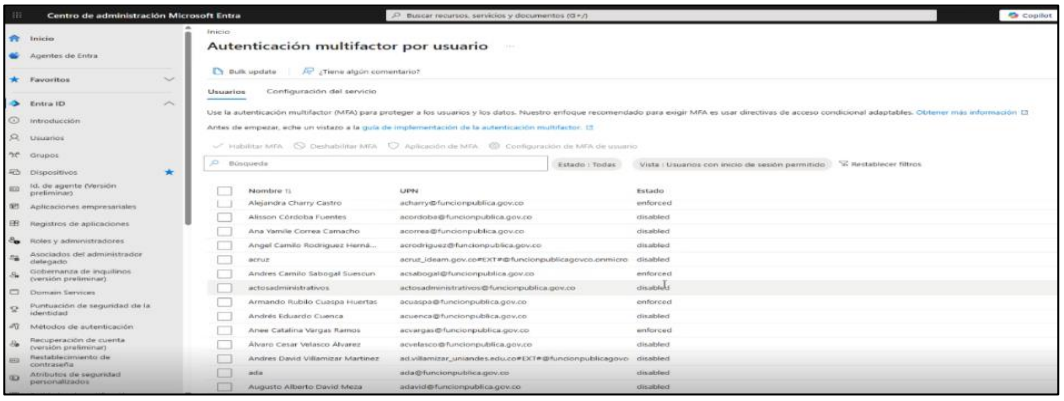
F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

- Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento.
- Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos.
- Dar cumplimiento al procedimiento del plan de mejoramiento.

Autenticación y accesos

Se evidenciaron adecuados controles relacionados con:

- Autenticación multifactor -MFA para todos los funcionarios y sin excepciones injustificadas. Actualmente, la autenticación MFA está habilitada para la totalidad de los funcionarios, con excepción de una cuenta identificada en la alta Dirección que se encuentra en proceso de gestión a la fecha. Respecto a los buzones institucionales compartidos, la OTIC está trabajando en una solución técnica diferenciada, debido a que estas cuentas son gestionadas por múltiples funcionarios. La implementación de MFA estándar presenta una mayor complejidad operativa que está siendo evaluada para no afectar la continuidad del servicio. Se evidencia al respecto el listado de todos los usuarios de Función Pública debidamente asegurados, como se puede apreciar en la siguiente imagen extraída de la suite de administración:



- Políticas de acceso condicional vigentes a través de Bloqueo geográfico (Geo-blocking) para permitir accesos únicamente desde Colombia. Requisito de equipos enrolados o

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

que cumplan con los estándares de seguridad de la OTIC. Al respecto, se evidencia correos cruzados con el soporte CCE MEDIA COMMERCE, solicitando el aseguramiento del segmento de red de la IP respectiva en el año 2023 (Evidencia: \\Yaksa\10030otic\2026\DOCUMENTOS_APOYO\SEGURIDAD\VULNERABILIDADES)

- Respecto al bloqueo de protocolos heredados (IMAP/POP/SMTP Auth) para usuarios estándar, es decir conjuntos de reglas antiguas utilizados para enviar y recibir correos electrónicos que dependen de la "autenticación básica" (nombre de usuario y contraseña), la Entidad no puede mantenerlos bloqueados por que corresponden a la operatividad propia de la gestión de correo inmersa en el tipo de licenciamiento contratado. Esta medida prevendría de ataques de fuerza bruta y aseguraría que la autenticación se realice únicamente a través de protocolos modernos que soportan MFA y políticas de Acceso Condicional. Se aclara por parte de la OTIC que se podrían bloquear siempre y cuando se tenga un nivel más avanzado de licenciamiento, aprovechando las bondades de protocolos modernos, pero el tener versiones más avanzadas requiere de tener un presupuesto alto para su adquisición. Lo importante, es que con la autenticación 2FA se cubre actualmente en alto grado la seguridad del correo.

Configuración técnica del correo

Se evidenciaron adecuados controles relacionados con:

- Los protocolos de autenticación de correo electrónico (SPF, DKIM y DMARC) están configurados y operando en modo de protección. Estos protocolos esenciales de autenticación de correo electrónico trabajan juntos para verificar la identidad del remitente, asegurando que los correos provengan de fuentes legítimas y no de suplantadores (phishing o spoofing). A continuación, y como soporte a esta configuración se presenta la parametrización actual:

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Fuente: Estado DKIM en Exchange (21-04-2026)

Fuente: Registro DNS TXT SPF del dominio (21-04-2026)

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Fuente: Registro DNS TXT DMARC del dominio (21-04-2026)

- Revisiones periódicas de las reglas de flujo de correo y reenvíos externos por parte del administrador del correo para detectar configuraciones anómalas que puedan indicar un compromiso de la cuenta, mediante Logs extraídos de la consola Exchange (Office 365) que muestran la ausencia de reenvíos no autorizados.

Administración de buzones

El Administrador del Directorio Activo, es el único funcionario que delega acceso a buzones por seguridad y para evitar la fuga de información, los funcionarios estándar no tienen habilitada la opción de delegar sus propios buzones de manera autónoma; cualquier requerimiento de este tipo debe realizarse mediante la plataforma de Proactivanet de soporte técnico y contar con la aprobación pertinente.

De otra parte, el acceso a buzones compartidos (Permisos Send As - Enviar como / On Behalf - Enviar en nombre de) se gestiona bajo un modelo de responsabilidad compartida: el jefe de Área identifica la necesidad y autoriza quién debe acceder al correo de su dependencia. Este procedimiento asegura que cada área maneje su información con autonomía, pero bajo los controles de seguridad y trazabilidad institucional.

Respecto a la detección de reglas de reenvío maliciosas, desde la implementación obligatoria del Doble Factor de Autenticación (MFA) y el despliegue de Check Point Harmony, no se han detectado nuevas reglas de reenvío maliciosas en los buzones institucionales.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Los controles mencionados son registrados a través de la mesa de ayuda (Proactivanet), manteniendo así la debida trazabilidad.

Monitoreo y detección

Respecto a la revisión de logs de inicio de sesión y generación de alertas por actividades anómalas, la OTIC gestiona los correos de alerta que llegan a la cuenta del administrador.

De otro lado, en la Entidad no se evidencia la integración de la seguridad con un SIEM (Security Information and Event Management), ni con un servicio de SOC (Security Operations Center). No obstante, se garantiza la seguridad y el monitoreo mediante: Retención de Logs y Monitoreo con Check Point Harmony.

Finalmente, en la actualidad la Entidad no cuenta con la implementación de Playbooks automáticos para la respuesta a incidentes, los cuales permiten ejecutar acciones predefinidas sin intervención humana, activándose por condiciones específicas como incidentes de seguridad o cambios en la infraestructura. La OTIC hace la claridad que actualmente se tiene un licenciamiento básico y este tipo de herramientas son de costo considerable y estan por fuera del presupuesto de la Entidad.

Respuesta y mejora continua

Frente al hecho acaecido la OTIC ejecutó un plan de choque integral. Estas acciones no solo detuvieron el ataque, sino que cerraron las brechas de seguridad para evitar su repetición. Para ello:

- Se realizó el bloqueo preventivo de las URLs y dominios maliciosos identificados en la campaña de correo para detener la propagación.
- Se efectuó el restablecimiento de Credenciales: Se forzó un cambio masivo de contraseñas para todos los usuarios de la entidad mediante GPO (Directorio Activo), invalidando cualquier dato que hubiera sido capturado por los atacantes.
- Se Implementó CheckPoint Harmony: Se contrató y desplegó esta solución de seguridad en nube, logrando la detección y eliminación del 100% de las amenazas de correo fraudulentas desde su activación.
- Se reforzó la Identidad y Acceso mediante el despliegue de MFA/2FA: Se activó la autenticación multifactor inicialmente para las cuentas comprometidas y posteriormente

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

se extendió a la totalidad de los funcionarios (Con las excepciones técnicas debidamente justificadas).

Se evidencian los respectivos soportes en las rutas:
\\Yaksa\10030otic\2025\DOCUMENTOS_APOYO\SEGURIDAD\VULNERABILIDADES
\\Yaksa\10030otic\2026\DOCUMENTOS_APOYO\SEGURIDAD\DOBLE FACTOR

Por otro lado, posterior al incidente, la OTIC efectuó una simulación de correo Phishing en el mes de febrero y una campaña de sensibilización en marzo del presente año, con los siguientes resultados:

- Sensibilización: se llevó a cabo una jornada masiva de capacitación y enrolamiento al 2FA para fortalecer la cultura de ciberseguridad entre los funcionarios y colaboradores. Se evidencian los debidos soportes de asistencia y grabación de la reunión en la ruta: \\yaksa.dafp.local\10030otic\2026\DOCUMENTOS_APOYO\SEGURIDAD\CAPACITACIONES,. No obstante el esfuerzo efectuado por la OTIC, solo asistieron a la sensibilización 29 usuarios de toda la entidad, de los cuales 12 eran de la OTIC, los demás de algunas dependencias.
- Simulacro: Se efectúo una simulación de correo Phishing aplicado a 359 funcionarios, de los cuales el 10,3% (37) ingreso al link fraudulento. Los resultados generales se muestran a continuación:

ITEM	FEBRERO 2026
Atacados	359
Víctimas del ataque	37
Vulnerabilidad mes = Víctimas mes / Atacados mes	10,31
Concientización práctica mes = 100% - Vulnerabilidad mes	89,69

Fuente: Resultados simulacro correo malware a funcionarios DAFP (18 de marzo 2016)

También, se evidencia el plan anual de capacitaciones orientando entre otros los siguientes temas: Identificación de correos, SMS y llamadas fraudulentas para evitar el robo de credenciales, implementación del uso de gestores de contraseñas y la importancia del MFA (Autenticación de Dos Pasos), protección de redes domésticas, uso de VPN y seguridad

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

física de dispositivos fuera de la oficina y reconocimiento de tácticas modernas como Deepfakes y estafas basadas en Inteligencia Artificial.

Respecto al fortalecimiento de las políticas tras el incidente, la OTIC no solo fortaleció las configuraciones técnicas, sino que estableció un ciclo de validación para asegurar que los controles fueran operativos y reales. Se pasó de un modelo de "uso opcional" a uno de enrolamiento mandatorio para todos los funcionarios. Se eliminaron las excepciones injustificadas y se bloquearon los protocolos heredados (POP/IMAP) que permitían evadir el segundo factor.

3. Conclusiones

1. A nivel general se exalta la gestión oportuna y metódica de OTIC en el análisis de causas y el tratamiento del incidente evitando impactos mayores en la integridad del correo institucional.

2. Con el fin de fortalecer la memoria de gestión y crear bases de conocimiento para los incidentes de seguridad que se presenten en el tiempo, como lo estipula el manual de políticas de seguridad de la información, es importante generar en su momento un reporte o informe detallado, tal y como se recomienda en el título de **Gestión de contención adelantada,** de este informe.

3. En pro de mantener una respuesta estratégica unificada y con un alto grado de coordinación en la gestión de los incidentes de seguridad, es importante como lo establece la Política de Seguridad de la información, que el líder del proceso escale al Comité Institucional de Gestión y Desempeño, aquellos que consideren pertinentes de acuerdo a su nivel de impacto y materialización de riesgo.

4. Con relación al procedimiento para el manejo de incidentes de seguridad de la información, publicado en el SIGP, es fundamental:

    - Efectuar una socialización periódica a los responsables e interesados respectivos, al interior de la entidad, con el fin de mantener actualizado el conocimiento y la cultura de seguridad.
    - Especificar claramente dentro de las actividades a gestionar la relacionada con la generación del informe o reporte detallado del incidente, teniendo en cuenta el contenido que sugiere MinTIC en la Guía para la gestión y clasificación de incidentes de seguridad.

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

5. Con respecto Tratamiento de riesgos para este incidente, si bien la OTIC activó el protocolo institucional de respuesta a incidentes logrando contener técnicamente la amenaza, e identificó en el análisis de causa el riesgo y sus amenazas, no se registró la gestión en el modelo de riesgos materializados del SGI como lo establece la política de gestión de riesgos. Por ende, se recomienda para futuros escenarios de materialización con el apoyo de la OAP, cumplir con las acciones determinadas por la política y mantener así la trazabilidad y gestión de la mejora continua, identificando en primera instancia el nuevo riesgo en la matriz de riesgos institucional e implementando los controles respectivos que permitan garantizar que este evento no se vuelva a presentar.

6. Si bien, aunque no se tiene actualmente contratado un servicio de SOC, se utilizó la solución Check Point Harmony - CH en modalidad de nube pública, la cual logro un 100% en la detección y eliminación del ataque de Phishing, no obstante, es importante analizar que solución puede ser más efectiva en cuanto a la vigilancia continua de la infraestructura tecnológica, redes y servidores y la identificación temprana de amenazas y contención inmediata para minimizar el impacto de un posible ciberataque. Las mejores prácticas indican en lo posible mantener un entorno maduro que puede combinar elementos de protección de primera línea como lo puede ser un **CH** y un **SOC** para la supervisión y gestión de alertas.

7. Es de suma importancia que desde la Administración se inste a toda la Entidad a participar en las diferentes campañas de sensibilización y capacitación sobre ciberseguridad que efectúa la OTIC, debido al índice tan alto de deserción que se ha venido presentando. Este elemento mitiga en alto grado la exposición a incidentes como el sucedido, debido a errores humanos que son la principal causa en las brechas de seguridad.

Jorge Iván De Castro Barón

Firmado digitalmente por Jorge Iván De Castro Barón
Fecha: 2026.04.24 15:46:09 -05'00'

Jorge Iván De Castro Barón
Jefe Oficina Control Interno

Elaboró: Juan Mauricio Cornejo Rodríguez
Revisó y Aprobó: Jorge Iván de Castro Barón

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)

Función Pública

Informe de Seguimiento administración y seguridad correo interno - Outlook

Versión 1
Proceso Evaluación Independiente
Abril de 2026

Carrera 6 No. 12-62
Bogotá, D.C. Colombia
Teléfono: 601 7395656
Fax: 601 7395657
Código Postal: 111711

Página web:
www.funcionpublica.gov.co

Email:
eva@funcionpublica.gov.co

F Versión 5 Fecha: 2024-06-28
Si este formato se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en el Sistema Integrado de Gestión (Intranet)