



TIC



# 5 acciones estratégicas para el proceso electoral

para entidades Públicas Colombianas

# Advertencia

## 5 acciones estratégicas para el proceso electoral

COLCERT AD-20260307- 032

TLP:CLEAR

En el marco del proceso electoral y ante el incremento de amenazas cibernéticas dirigidas a infraestructuras tecnológicas críticas el Equipo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT presenta este documento que reúne recomendaciones prácticas que pueden ser implementadas por los equipos técnicos y responsables de tecnología de las entidades públicas, con el propósito de apoyar la continuidad, integridad y confiabilidad de los servicios digitales durante el proceso electoral.

Estas acciones buscan promover medidas preventivas que contribuyan a la protección de los sistemas de información, portales institucionales, plataformas de comunicación y servicios tecnológicos que acompañan el desarrollo del proceso democrático. La adopción de controles básicos de seguridad, buenas prácticas en la gestión de accesos, actualización de sistemas y monitoreo permanente permite reducir las brechas, disminuyendo las vulnerabilidades y fortaleciendo la resiliencia digital de las instituciones.

### Principales riesgos críticos

Se identifican amenazas clave para la infraestructura tecnológica electoral, tales como:

- **Ataques de DDoS** que buscan saturar la red y dejar inaccesibles los portales web.
- **Defacement (Desfiguración web)**, modificación no autorizada de sitios oficiales mediante explotación de vulnerabilidades, credenciales comprometidas o configuraciones inseguras, con el objetivo de insertar propaganda, mensajes desestabilizadores o desinformación.
- **Campañas de spear-phishing** dirigidas a funcionarios estratégicos con el objetivo de comprometer credenciales de acceso y evadir perímetros de seguridad.
- **Ransomware** compromete y cifra sistemas críticos para interrumpir servicios institucionales, afectar la continuidad operativa y generar presión pública durante el proceso electoral.
- **Desinformación, campañas coordinadas que buscan manipular la percepción pública** mediante contenido falso o engañoso, amplificadas especialmente cuando existen interrupciones en los canales oficiales.
- **Compromiso de cuentas institucionales**, Ataques orientados a comprometer cuentas oficiales de correo, redes sociales o plataformas administrativas mediante phishing o robo de credenciales, permitiendo la difusión de información falsa o el acceso a sistemas internos.
- **Explotación de vulnerabilidades en portales electorales**, ataques dirigidos a explotar vulnerabilidades en aplicaciones web expuestas a internet con el objetivo de acceder a bases de datos, alterar información o provocar indisponibilidad de los sistemas.

### Cadena típica de escalamiento de un ataque en el entorno electoral

La siguiente ilustración muestra cómo una intrusión inicial, generalmente iniciada mediante campañas de phishing o ingeniería social, puede escalar progresivamente hasta comprometer sistemas institucionales, provocar indisponibilidad de servicios y facilitar la difusión de desinformación que impacte el proceso electoral.



Figura 1. Cadena de escalamiento de un ataque contra infraestructura digital

# Advertencia

## 5 acciones estratégicas para el proceso electoral

COLCERT AD-20260307- 032

TLP: CLEAR

Recomendaciones prioritarias



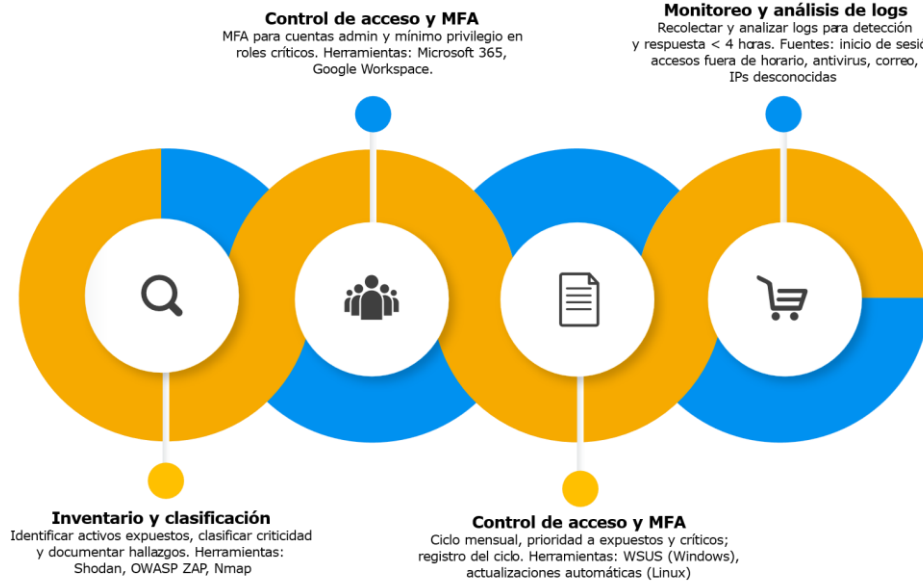
Se enfatiza la implementación de medidas estratégicas como:

Área / Medida	Objetivo	Implementación sugerida	Prioridad
Endurecimiento de correo (DMARC, DKIM, SPF)	Prevenir phishing y suplantación de dominio; proteger comunicación oficial.	<p><b>SPF</b></p> <ul style="list-style-type: none"> <li>• Crear registro DNS TXT con servidores autorizados</li> <li>• Publicar en DNS</li> <li>• Validar (MXToolbox SPF Check / mail-tester.com)</li> </ul> <p><b>DKIM</b></p> <ul style="list-style-type: none"> <li>• Generar claves (pública/privada) en proveedor (M365 / Google)</li> <li>• Publicar clave pública en DNS (TXT o CNAME) con selector</li> <li>• Activar firma DKIM en el servicio.</li> <li>• Validar (mail-tester.com)</li> </ul> <p><b>DMARC</b></p> <p>Registro DNS que define qué hacer con correos que fallan SPF y/o DKIM y habilita reportes del dominio. Implementación gradual (3 fases).</p> <p><b>Validación completa</b></p> <ul style="list-style-type: none"> <li>• Enviar correo a mail-tester.com</li> <li>• Revisar puntaje (meta: 10/10)</li> <li>• Verificar: DKIM_VALID, SPF_PASS, SPF_HELO_PASS</li> <li>• Indicador final: DMARC en p=reject antes del 01/02/2026</li> </ul>	ALTA
Protección DDoS (servicios + WAF)	Mantener disponibilidad de portales y servicios críticos ante ataques de volumen o aplicación	Implementar WAF, rate limiting, CDN/caché y plan de escalamiento con proveedor anti-DDoS.	ALTA
Continuidad (backups robustos, inmutables y offline)	Recuperar la operación frente a ransomware, fallas y pérdida/corrupción de datos.	<p><b>Estrategia 3-2-1 de backups</b></p> <p>Se recomienda mantener copias de datos en dos tipos de medios y al menos una copia offline para protegerse contra ransomware, siendo esta última esencial para protegerse del ransomware.</p> <p><b>Implementación según capacidad</b></p> <ul style="list-style-type: none"> <li>• Nivel básico: backups manuales de bases de datos y copias offline en discos externos desconectados, retención extendida para correo Microsoft 365.</li> <li>• Nivel intermedio: soluciones automáticas open source o comerciales, replicación a nube o segundo sitio, monitoreo y alertas.</li> <li>• Nivel avanzado: sitios de recuperación ante desastres con replicación continua, pruebas mensuales de restauración y backups inmutables para alta protección.</li> </ul>	ALTA
Perímetro y acceso (gestión de vulnerabilidades, MFA, firewalls)	Reducir superficie de ataque y prevenir accesos no autorizados a sistemas críticos.	Ciclo de parches; escaneos periódicos; MFA para cuentas admin; reglas de firewall mínimas necesarias.	MEDIA
Respuesta a incidentes (procedimiento CoCERT)	Recuperar la operación frente a ransomware, fallas y pérdida/corrupción de datos.	Definir roles, contactos, tiempos (RTO), checklist por fase y ejercicios de simulación.	MEDIA

La gestión continua de vulnerabilidades constituye un proceso permanente orientado a identificar, priorizar y mitigar debilidades en los sistemas expuestos a internet, reduciendo la probabilidad de explotación por parte de actores maliciosos.



### Protección de activos (componentes clave)



## Protección contra DDoS y Defacement

### Vectores de ataque

#### ① Vectores de ataque (resumen)

- ✓ DDoS volumétrico
- ✓ DDoS de aplicación (HTTP)
- ✓ SQL Injection
- ✓ Defacement (credenciales/vulnerabilidades)
- ✓ Amplificación DNS

#### ② Mitigación Anti-DDoS (por nivel)

- ✓ **Básico:** Cloudflare gratuito + rate limiting + ajuste TTL DNS + deshabilitar servicios no esenciales.
- ✓ **Intermedio:** Cloudflare Pro/Business con WAF + CDN/caché agresivo + balanceo/segmentación.
- ✓ **Avanzado:** Anti-DDoS dedicado + SOC 24/7 + plan de respuesta con tiempos definidos

#### ③ Prevención de Defacement (CMS)

- ✓ MFA en panel administrativo.
- ✓ Cambiar URL de acceso al panel y limitar fuerza bruta.
- ✓ Actualizar CMS/plugins y eliminar componentes no usados.
- ✓ Permisos estrictos de archivos (mínimo privilegio).
- ✓ Plugin de seguridad (hardening / firewall / anti-malware).
- ✓ Backups diarios para restauración rápida.
- ✓ Modo solo lectura durante el periodo crítico (día de elecciones)

¿Por qué el correo es el vector #1 de ataque?



En el contexto electoral, este vector se potencia: un correo que aparente venir de la Registraduría Nacional, el Consejo Nacional Electoral o una secretaría de gobierno puede engañar a funcionarios clave y comprometer sistemas completos.



### Protección adicional: Endurecimiento de encabezados de correo

Se recomienda evaluar la configuración mediante herramientas como mail-tester.com para lograr una puntuación óptima. Asimismo, es conveniente implementar controles adicionales, tales como la eliminación de encabezados que revelan versiones, mecanismos de protección anti-spoofing, filtrado de archivos adjuntos maliciosos, advertencias en correos externos y la gestión de listas de remitentes bloqueados. .

Medida	Qué hace (y cómo activar)	Prioridad
Encabezado X-Mailer personalizado	Evita fingerprinting ocultando versión del servidor. Activar en Exchange/M365 ajustando configuración de transporte (p. ej., Set-TransportConfig).	MEDIA
Anti-spoofing en Exchange	Bloquea suplantación (spoofing) con controles nativos. Activar en Seguridad <input checked="" type="checkbox"/> Directivas anti-phishing <input checked="" type="checkbox"/> Inteligencia de suplantación.	ALTA
Filtrado de adjuntos maliciosos	Bloquea extensiones peligrosas (.exe, .bat, .vbs, .js, .ps1, .iso, .img). Activar con reglas de transporte o Defender (Adjuntos seguros).	ALTA
Advertencia de correo externo	Reduce clics en phishing marcando correos externos. Activar con regla de transporte (banner / disclaimer o Prepend Subject).	ALTA
Lista de remitentes bloqueados	Bloquea dominios/emisores conocidos por phishing. Gestionar en Exchange Admin Center <input checked="" type="checkbox"/> Protección <input checked="" type="checkbox"/> filtro de conexión / listas de bloqueo.	MEDIA



### Protocolo de respuesta a incidentes

Se detalla un procedimiento basado en ColCERT para la gestión de incidentes digitales con cinco fases:

Diagrama de flujo –  
Protocolo de respuesta a  
incidentes (5 fases)



#### 1. Detección y activación

Identificar, evaluar impacto, notificar y activar equipo. Preservar evidencia.



#### 3. Contención y erradicación

Aislar, cambiar credenciales, cerrar vector, analizar logs y parchear.



#### 5. Cierre y lecciones

Documentar, cerrar reporte en ColCERT y ajustar controles y evidencias.



#### 2. Clasificación y reporte

Clasificar gravedad. Reportar a ColCERT y a SIC si hay datos personales



#### 4. Recuperación (RTO)

Restaurar desde backups verificados y activar contingencia. Monitorear.



La protección de la infraestructura tecnológica asociada a los procesos electorales es una responsabilidad compartida que exige la adopción oportuna de medidas de seguridad, la implementación de acciones inmediatas de prevención, la coordinación interinstitucional y la vigilancia permanente frente a riesgos y amenazas cibernéticas.

La aplicación de estas recomendaciones contribuye a fortalecer las capacidades preventivas de las entidades públicas, reducir posibles vulnerabilidades y promover una gestión responsable de los sistemas de información institucionales.

Desde el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) se mantiene la disposición de acompañar a las entidades del país mediante sus capacidades técnicas de orientación, monitoreo y coordinación en seguridad digital, contribuyendo al fortalecimiento de un entorno digital confiable para el desarrollo del proceso electoral.