CORGESDE
NIT: 900.976.334-8
Domicilio principal: Espinal, Tolima
Representante Legal: CAMILO ANDRES JIMENEZ

POLÍTICAS DE SEGURIDAD INFORMÁTICA

1. Objetivo

Establecer las directrices para proteger la información, los sistemas tecnológicos y los recursos informáticos de CORGESDE, garantizando la confidencialidad, integridad, disponibilidad y legalidad en el manejo de los datos y la operación del servicio como proveedor de Internet y televisión.

2. Alcance

Estas políticas aplican a todos los empleados, contratistas, técnicos, asesores y terceros que accedan, procesen o administren información, equipos o sistemas pertenecientes a CORGESDE, en cualquiera de sus sedes y plataformas digitales (SIIGO, WhatsApp Business, sitio web, entre otros).

3. Normatividad de referencia

- Ley 1273 de 2009 (Delitos informáticos).
- Ley 1581 de 2012 y Decreto 1377 de 2013 (Protección de datos personales).
- Ley 1341 de 2009 (TIC).

POLÍTICAS GENERALES

a. Control de acceso

- Cada usuario deberá contar con credenciales personales y únicas.
- Se prohíbe compartir contraseñas o accesos.
- Las contraseñas deben tener al menos 8 caracteres y cambiarse cada 90 días.
- Los accesos a routers, servidores y sistemas administrativos serán otorgados solo al personal autorizado.
- Todo acceso remoto deberá realizarse mediante canales seguros (VPN u otros métodos cifrados).

b. Seguridad de la red

- Las redes deberán segmentarse entre zonas administrativas, técnicas y de clientes
- Se mantendrán actualizados los firewalls, antivirus y demás herramientas de protección.
- Queda prohibido conectar equipos personales a la red corporativa sin autorización.

- El monitoreo de la red deberá realizarse de manera continua para detectar anomalías o intentos de intrusión.

c. Uso aceptable de los recursos informáticos

- Los recursos tecnológicos se destinan exclusivamente a fines laborales.
- No se permite instalar software sin licencia o sin aprobación técnica.
- Está prohibido el uso de los equipos para actividades personales, ilegales o que comprometan la reputación de la empresa.
- Ningún colaborador podrá divulgar información de clientes, precios o configuraciones técnicas sin autorización expresa.

d. Protección de datos personales

- CORGESDE garantiza el cumplimiento de la Ley 1581 de 2012 y su Decreto reglamentario.
- Solo se recolectarán los datos estrictamente necesarios para la prestación del servicio.
- Toda información personal será tratada bajo los principios de legalidad, finalidad, libertad, veracidad, transparencia, seguridad y confidencialidad.
- Los titulares podrán ejercer sus derechos de acceso, corrección, actualización y supresión mediante los canales oficiales de atención.
- No se compartirán datos personales con aliados ni terceros, salvo obligación legal.

e. Copias de seguridad y recuperación de información

- Se realizarán copias de seguridad diarias de las bases de datos y sistemas críticos.
- Los respaldos deberán almacenarse en ubicaciones seguras o en la nube bajo control corporativo.
- Cada seis (6) meses se deberán probar los procedimientos de restauración.
- Solo el personal autorizado podrá acceder o modificar las copias de seguridad.

f. Correo electrónico y mensajería

- Está prohibido el envío de información confidencial sin cifrado o a cuentas personales.
- Todos los correos corporativos deberán incluir firma institucional.
- Los sistemas de correo deben contar con filtros antispam y antivirus activos.

g. Manejo de incidentes de seguridad

- Todo evento que afecte la información o infraestructura debe reportarse de inmediato a la gerencia o al responsable técnico.
- Los incidentes serán registrados y analizados para prevenir recurrencias.
- Se aplicarán medidas correctivas y disciplinarias según la gravedad del hecho.

h. Dispositivos y equipos

- Los equipos de cómputo y dispositivos móviles de la empresa deben mantenerse con antivirus actualizado.
- Al finalizar la relación laboral o contractual, los dispositivos deberán ser devueltos y los accesos revocados.
- Queda prohibido almacenar datos de clientes en dispositivos personales.

i. Continuidad operativa

- Se deberá mantener un plan de contingencia ante fallas eléctricas, ataques o desastres.
- Los sistemas críticos deberán contar con respaldo eléctrico (UPS o planta).
- En caso de interrupción grave, se priorizará la restauración del servicio de Internet y la atención al usuario.

j. Cumplimiento y sanciones

- El incumplimiento de estas políticas será considerado falta grave y podrá generar sanciones disciplinarias, suspensión de accesos o terminación del contrato.
- CORGESDE se reserva el derecho de realizar auditorías internas para verificar el cumplimiento.

4. Revisión y actualización

Estas políticas serán revisadas anualmente o cuando se presenten cambios tecnológicos, normativos o estructurales en la empresa.

5. Aprobación

Estas políticas fueron aprobadas por la Gerencia General de CORGESDE el día 21 de octubre de 2025.

Firma:

CAMILO ANDRES JIMENEZ Representante Legal – CORGESDE

POLÍTICA DE BLOQUEO DE SITIOS WEB POR DNS

1. OBJETIVO

Establecer los lineamientos técnicos y administrativos para la implementación del bloqueo de sitios web por DNS dentro de la infraestructura de red de CORGESDE., con el fin de restringir el acceso a dominios no autorizados, de contenido riesgoso, o señalados por autoridad competente, garantizando así la seguridad, integridad y estabilidad de los servicios prestados por la compañía.

2. ALCANCE

Esta política aplica a:

- Todos los equipos de red y servidores DNS administrados por CORGESDE, incluidos routers MikroTik, servidores internos y plataformas de acceso de clientes.
- Los usuarios, suscriptores y colaboradores que utilicen la red o los servicios de conectividad de la empresa.

3. RESPONSABLES

- Área Técnica / Seguridad Informática: Implementar, supervisar y actualizar las configuraciones de bloqueo.
- Gerencia General: Autorizar bloqueos permanentes o por orden legal.
- Área Jurídica o Administrativa: Verificar el sustento normativo o contractual del bloqueo, cuando aplique.

4. CRITERIOS DE BLOQUEO

Los dominios podrán ser bloqueados por las siguientes causas:

1. Solicitud u orden de autoridad judicial, administrativa o regulatoria (MinTIC, SIC, Policía Nacional, entre otras).
2. Presencia de contenido malicioso, phishing, o software potencialmente dañino.
3. Sitios que afecten la seguridad, estabilidad o desempeño de la red.
4. Portales que vulneren derechos de autor, propiedad intelectual o normas vigentes.
5. Solicitudes internas aprobadas por la Gerencia, en función de políticas operativas o de cumplimiento.

2. **Verificación y mantenimiento:**
    - Monitorear las estadísticas DNS con /ip dns print stats. ○ Limpiar la caché tras aplicar cambios (/ip dns cache flush). ○ Documentar cada acción en el registro de bloqueos, incluyendo: fecha, dominio, motivo y responsable.

5. CONTROLES Y REGISTROS

- Registro de dominios bloqueados: listado actualizado con la fecha, motivo, área solicitante y autorización.
- Auditoría interna: revisión trimestral para verificar la vigencia y pertinencia de los bloqueos.
- Informe técnico: reporte de actividad DNS y efectividad del mecanismo.

6. VIGENCIA Y REVISIÓN

Esta política entra en vigencia a partir de su aprobación y deberá ser revisada anualmente o cuando se produzcan cambios en la infraestructura de red, las disposiciones legales o los requerimientos regulatorios aplicables al sector de telecomunicaciones.

POLÍTICA Y PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD

1. Objetivo

Establecer el procedimiento para la identificación, análisis, respuesta y documentación de los incidentes de seguridad de la información que puedan afectar la confidencialidad, integridad o disponibilidad de los sistemas, servicios o datos de CORGESDE.

2. Alcance

Aplica a todos los sistemas tecnológicos, infraestructuras de red, servicios de internet y televisión, y a cualquier activo de información de la empresa, incluyendo datos de clientes, proveedores y personal

3. Definiciones

Se considera **incidente de seguridad** cualquier evento que comprometa o intente comprometer los sistemas informáticos, tales como:

a. Accesos no autorizados o intentos de intrusión.
b. Ataques de denegación de servicio (DDoS).
c. Infecciones por malware, ransomware o virus.
d. Fugas, pérdida o alteración de información.
e. Fallas graves en servicios críticos o infraestructura.
f. Uso indebido de credenciales o dispositivos.

4. PROCEDIMIENTO GENERAL DE GESTIÓN DE INCIDENTES

a. Detección y reporte

- Todo empleado, contratista o proveedor que detecte un incidente debe reportarlo de inmediato al responsable técnico o a la gerencia mediante los canales oficiales (correo institucional, WhatsApp de soporte o línea de emergencia interna).
- Se debe registrar el evento con fecha, hora, sistema afectado, descripción y evidencias (capturas, logs, mensajes).

b. Análisis y clasificación

- Se evalúa el nivel de impacto y urgencia (alto, medio o bajo).
- Se identifica si afecta la disponibilidad del servicio, los datos personales o la infraestructura.
- Se determina la causa raíz (falla técnica, error humano, ataque externo, etc.).

c. **Contención inmediata**

- Aislar los equipos o segmentos comprometidos de la red.
- Cambiar contraseñas o deshabilitar cuentas afectadas.
- Suspender temporalmente servicios si el riesgo de propagación es alto.

d. **Erradicación y recuperación**

- Eliminar software malicioso o restaurar configuraciones seguras.
- Aplicar parches o actualizaciones de seguridad.
- Recuperar información desde respaldos verificados.
- Monitorear el sistema hasta confirmar la estabilidad.

e. **Comunicación y escalamiento**

- Notificar al Representante Legal y a la autoridad competente en caso de vulneración de datos personales (SIC).
- Informar al MinTIC o CRC si el incidente afecta la prestación del servicio público.
- Comunicar a los usuarios solo si el evento compromete sus datos o experiencia.

f. **Registro y documentación**

- Cada incidente deberá quedar documentado en el **Registro de Incidentes de Seguridad**, indicando: descripción, fecha, responsable, impacto, acciones correctivas y medidas preventivas futuras.

g. **Mejora continua**

- Los incidentes servirán como insumo para fortalecer controles, ajustar políticas y capacitar al personal.

GUÍA TÉCNICA: CÓMO DETECTAR Y GESTIONAR ATAQUES CIBERNÉTICOS

DETECCIÓN TEMPRANA DE ATAQUES

Puedes identificar ataques mediante:

- **Monitoreo de red (logs, firewall, IDS/IPS, SIEM):** detectar conexiones sospechosas, tráfico inusual o intentos de fuerza bruta.
- **Alertas del antivirus o sistemas de endpoints (EDR):** comportamiento anómalo de procesos o software no autorizado.
- **Análisis de consumo:** picos de ancho de banda, CPU o memoria sin explicación.
- **Reportes de usuarios:** lentitud, bloqueos o mensajes extraños. **Tipos comunes de ataques**

Tipo de ataque	Descripción	Medidas de detección
Phishing / Ingeniería social	Correos falsos para robar credenciales	Filtros antispam, educación al usuario

Malware / Ransomware	Software malicioso que cifra o roba datos	Antivirus actualizado, EDR
DDoS	Saturación de red para tumbar servicios	Monitoreo de tráfico, firewalls perimetrales
Intrusión o hacking	Acceso no autorizado a sistemas	IDS/IPS, auditoría de accesos
Fuga de datos	Exfiltración de información confidencial	DLP, registros de transferencia

Pasos recomendados del procedimiento

1. **Preparación:** asignar roles, canales de comunicación y herramientas.
2. **Detección:** establecer alertas automáticas y reportes manuales.
3. **Contención:** minimizar daños (aislar, bloquear, cortar tráfico).
4. **Erradicación:** eliminar causa raíz (virus, vulnerabilidad).
5. **Recuperación:** restaurar servicios desde copias seguras.
6. **Lecciones aprendidas:** documentar, corregir, mejora

Elaborado por: Oscar David Pulido Zuluaga	**Revisado por:** Brayan Rojas Rocha	***Aprobado por:*** *CAMILO ANDRES JIMENEZ*
Cargo: ***de Coordinador administrativo***	***Cargo:*** ***Profesional Ingeniero telecomunicaciones.*** ***Middle de***	***Cargo: Representante legal y Gerente general***
