	CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS	Código:	SI-F-037
		Versión:	3
		Fecha:	13/02/2026
		Clasificación:	PUBLICO
		Etiquetado:	PUB-M-2

AUTORIDADES

ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	CASOS EN LOS CUALES SE DEBE CONTACTAR	ACTIVIDADES PARA MANTENER CONTACTO	PERSONA AUTORIZADA PARA EL CONTACTO DESDE SISA
Centro Cibernético Policial (CCP)	Es la dependencia de la Subdirección de Investigación Criminal, encargada de investigar los delitos informáticos y apoyar la investigación criminal de los fenómenos en el ciberespacio, a través del análisis de información, atención de incidentes cibernéticos y el desarrollo de estrategias, programas, acciones y proyectos de ciberseguridad. El CAI Virtual, es el primer servicio en Iberoamérica dedicado a la prevención, sensibilización y atención de incidentes cibernéticos, brindando atención policial contra el delito cibernético, el cual ha permitido focalizar la atención al ciudadano, destacando de manera diferencial el servicio online 24/7, orientado a dar respuestas a los diferentes requerimientos reportados por los ciberciudadanos	https://caivirtual.policia.gov.co/	Acceso abusivo a sistemas informáticos Violación de Datos personales Uso de Software malicioso Suplantación de Sitios Web Transferencia no consentida de activos Hurto por medios informáticos Phishing Ingeniería Social	**Estrategia de comunicación:** Comunicación reactiva mediante reportes formales de incidentes (correo, plataforma CAI Virtual) y coordinación a través de equipo NOC-SOC. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	El equipo encargado del procedimiento para el SI-P-001 Registro y gestión de incidentes de SI y ciberseguridad. En este caso el Gerente NOC-SOC o el Especialista de Ciberseguridad autorizado por el Gerente NOC-SOC. Así mismo en caso que el comité de seguridad de la información lo autorice puede ser ejecutado por el Equipo de Seguridad de la Información.
COLCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia	Grupo de Respuesta a Emergencias Cibernéticas de Colombia - COLCERT Identificar infraestructuras criticas, gestionar sus riesgos de ciberseguridad, ofrecer a las empresas del sector público y privado, información preventiva sobre amenazas y vulnerabilidades, apoyo y asesoría en la gestión de los incidentes de ciberseguridad, que garanticen la continuidad de las operaciones y servicios a la ciudadanía colombiana.	http://www.colcert.gov.co/	Reportar un Phishing Denunciar Ciberdelitos Reportar incidente de SI Boletines de información relacionada	**Estrategia de comunicación:** Comunicación bidireccional: recepción de alertas + reporte de incidentes vía canales oficiales. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	El equipo encargado del procedimiento para el SI-P-001 Registro y gestión de incidentes de SI y ciberseguridad. En este caso el Gerente NOC-SOC o el Especialista de Ciberseguridad autorizado por el Gerente NOC-SOC. Así mismo en caso que el comité de seguridad de la información lo autorice puede ser ejecutado por el Equipo de Seguridad de la Información.
CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia	El CSIRT del sector Gobierno hace parte del COLSERT, surge como necesidad de realizar una adecuada gestión y reaccionar ante los incidentes cibernéticos de modo centralizado, para lo cual realiza seguimiento de manera unificada a las principales tipologías de ciberincidentes que atentan contra la defensa del Gobierno, para realizar de manera eficiente la gestión de sus riesgos.	https://cc-csirt.policia.gov.co/ https://cc-csirt.policia.gov.co/alertas-tips https://cc-csirt.policia.gov.co/suscribete	Registrar un incidente Revisar un archivo o URL malicioso (Sandbox) Analizar aplicaciones móviles (APK) Revisar boletines emiten alertas sobre vulnerabilidades insurgentes y de día 0.		
Registro Nacional de Bases de Datos ante la SIC	El Registro Nacional de Bases de Datos – RNBD - es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos. El Gobierno Nacional, mediante el capítulo 26 del Decreto Único 1074 de 2015, reglamentó la información mínima que debe contener el RNBD y los términos y condiciones bajo los cuales se deben inscribir en éste las bases de datos sujetas a la aplicación de la Ley 1581 de 2012.	https://www.sic.gov.co/registro-nacional-de-bases-de-datos	Registrar las bases de datos personales de clientes, colaboradores, excolaboradores, visitantes y proveedores Así mismo se debe registrar si se realiza Transferencia o trasmisión Internacional de Datos sensibles.	**Estrategia de comunicación:** Reporte periódico y actualización de bases de datos a través del portal oficial. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	El equipo de seguridad de la información realizará el reporte de las bases de datos de SISA según la frecuencia establecida, apoyando el cumplimiento del control 5.29.
Dirección Nacional de Bomberos Colombia	Es la entidad encargada de emitir lineamientos e implementar políticas, gestionar recursos y generar estrategias, coadyuvando al fortalecimiento de la actividad bomberil, para la prestación efectiva del servicio público esencial de bomberos, bajo el marco de la gestión integral del riesgo a favor de la protección de la vida, bienes y medio ambiente.	https://dnbc.gov.co/tramites-y-servicios/ 300 7121125 123	Emergencia por incendio	**Estrategia de comunicación:** Comunicación bidireccional: recepción de alertas + reporte de incidentes vía canales oficiales. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	El equipo de Seguridad de la información en caso de una interrupción por incendios en la bodega de SISA, se activará el plan de continuidad de negocio. Así mismo cada colaborador en caso de requerir los servicios en casa.
Policía Nacional	La Policía Nacional es la entidad que debe contribuir al mantenimiento de la convivencia como condición necesaria, para el ejercicio de los derechos y libertades públicas y aportar a la construcción de paz	https://www.policia.gov.co/ Línea Anticorrupción: 166 Bogotá: +57 6015159111 / 9112 Resto del país: 018000 910112	Constancia por perdida de documentos Antecedentes Judiciales Celulares Recuperados Registro importador y/o exportador de equipos de telefonía móvil Red Integral de Seguridad en el Transporte (RISTRA) Reporte de delitos informativos Reportar hechos que perjudiquen el medio ambiente y los animales Servicio de recorridos turísticos Tramite certificación caninas SICEC-K9 Frente de Seguridad Empresarial (FSE)		El equipo de Seguridad de la información en caso de una interrupción por una novedad que afecte la convivencia e integridad de SISA también cuando se requiera activar por el plan de continuidad de negocio. Así mismo cada colaborador en caso de requerir los servicios en casa.
Gaula	Los Grupos de Acción Unificada por la Libertad Personal (GAULA), velan por la protección de la vida, la integridad, la libertad y los derechos de los colombianos. Son una unidad élite, insignia de las Fuerzas Militares de Colombia, que trabaja en la defensa de los territorios, sus comunidades y sus economías.	https://www.ejercito.mil.co/grupos-gaula/ 165	Antisecuestro y Antiextorsión		El equipo de Seguridad de la información en caso de una interrupción por una novedad que afecte la integridad y libertad de cualquier colaborador de SISA también cuando se requiera activar por el plan de continuidad de negocio. Así mismo cada colaborador en caso de requerir los servicios en casa.
Defensa Civil	La Defensa Civil Colombiana, en el marco de su competencia, desarrolla procesos en gestión del riesgo de desastres, acción social, gestión ambiental y programas de educación dirigidos al voluntariado y a la comunidad, para contribuir a la seguridad humana en el territorio nacional y responder a compromisos de orden internacional.	https://www.defensacivil.gov.co/ 144	Siniestros ambientales		El equipo de Seguridad de la información / Talento Humano (SST) en caso de una interrupción por una novedad que afecte las instalaciones o integridad de cualquier colaborador de SISA en caso de desastres ambientales, también cuando se requiera activar por el plan de continuidad de negocio. Así mismo cada colaborador en caso de requerir los servicios en casa.
Cruz Roja	La CRCSCB usando la innovación tecnológica, será el primer prestador de servicios humanitarios en Bogotá y Cundinamarca comprometida con el desarrollo humano y el fomento de la recuperación y protección del medio ambiente, diversificando las fuentes de ingreso y fortaleciendo el trabajo voluntario.	142 / 119	Incidentes laborales / Ambulancias		El equipo de Seguridad de la información / Talento Humano (SST) en caso de un accidentes que ponga en peligro la vida de cualquier colaborador de SISA. Así mismo cada colaborador en caso de requerir los servicios en casa.

GRUPOS DE INTERES

ORGANIZACIÓN	DESCRIPCIÓN	CONTACTO	CASOS EN LOS CUALES SE DEBE CONTACTAR		PERSONA AUTORIZADA PARA EL CONTACTO DESDE SISA
MinTIC	Ministerio de tecnologías de la información y las comunicaciones	https://www.mintic.gov.co/portal/inicio/	Lienamientos y cambios en normatividad, boletínes, recursos de aprendizaje	**Estrategia de comunicación:** Monitoreo continuo de normatividad y boletínes (web oficial). Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Cualquier colaborador
ISO	Estándares globales para bienes y servicios confiables	https://www.iso.org/	Normas ISO, definiciones, noticias y recursos de aprendizaje	**Estrategia de comunicación:** Consulta de estándares, capacitaciones y actualización documental. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC / Equipo de Gobierno de Seguridad de la Información
IEC	Internacional Electrotécnica Comisión	https://www.electropedia.org/	El vocabulario electrotécnico en línea del mundo	**Estrategia de comunicación**: Consulta de estándares, capacitaciones y actualización documental. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC / Equipo de Gobierno de Seguridad de la Información
CCOC	Comando Conjunto Cibernéticlo - Infraestructura tecnológica	https://www.cgfm.mil.co/es/comando-conjunto-cibernetico#:~:text=Comando%20Conjunto%20Cibern%C3%A9tico%20Conocenos%20Qui%C3%A9nes%20somos,%20Historia,%20Organigrama,%20Cultura%20militar.	Boletínes, noticias y recursos de aprendizaje	**Estrategia de comunicación:** Comunicación bidireccional: recepción de alertas + reporte de incidentes vía canales oficiales. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC / Equipo de Gobierno de Seguridad de la Información

	CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS	Código:	SI-F-037
		Versión:	3
		Fecha:	13/02/2026
		Clasificación:	PUBLICO
		Etiquetado:	PUB-M-2

CSIRT - CCIT	Centro de Coordinación Seguridad Informática Colombia	https://cc-csirt.policia.gov.co/	Boletínes, noticias y recursos de aprendizaje	**Estrategia de comunicación:** Comunicación bidireccional: recepción de alertas + reporte de incidentes vía canales oficiales. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC / Equipo de Gobierno de Seguridad de la Información
ColCERT	Grupo de Respuesta a Emergencias Cibernéticas en Colombia	https://colcert.gov.co/800/w3-article-198656.html	Resumen de Vulnerabilidades de la última semana	**Estrategia de comunicación:** Comunicación bidireccional: recepción de alertas + reporte de incidentes vía canales oficiales. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC / Equipo de Gobierno de Seguridad de la Información
Bureu Veritas	Auditorías al Sistema Integrado de gestión	https://www.bureauveritas.com.co/es	Auditorías certificadas, consultorias, capacitaciones, boletines, novedades	**Estrategia de comunicación:** Comunicación programada (auditorías, capacitaciones). Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo de Gobierno de Seguridad de la Información / Sistema Integrado de Gestión
Fourtelco	Consultorías para los sistemas integrados de gestión	http://fourtelco.com/	Auditorías internas, consultorias, capacitaciones, boletines, novedades	**Estrategia de comunicación**: Comunicación programada (auditorías, capacitaciones). Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo de Gobierno de Seguridad de la Información / Sistema Integrado de Gestión
Ministerio Ambiente	Información sobre aspectos e impactos ambientales relacionados con la operación de SISA	https://www.minambiente.gov.co/	Información sobre normatividad, aspectos e impactos ambientales	**Estrategia de comunicación:** Consulta de normativa y cumplimiento regulatorio. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo de SST / Sistema Integrado de Gestión
Microsoft 365 Microsoft MSRC	Learn / Configuración de Microsoft 365 para la operación Alerta de seguridad de sistemas MS	https://www.microsoft.com/en-us/msrc	Revisión de reportes sobre alertas de seguridad de sistemas MS	**Estrategia de comunicación:** Suscripción RSS / Email Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo de Operaciones (Sistemas Operativos - Redes y seguridad) / Equipo de ciberseguridad
MITRE	Estudio de casa de Amenazas y Correlacion de Eventos	https://attack.mitre.org/	Información sobre amenazas	**Estrategia de comunicación**: Monitoreo automatizado + análisis técnico por NOC-SOC. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC
NIST	Base de datos de Vulnerabilidades Conocidas	https://nvd.nist.gov/vuln	Información sobre vulnerabilidades	**Estrategia de comunicación:** Monitoreo automatizado + análisis técnico por NOC-SOC. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC
MITRE	Categorizacion de Vulnerabilidades	https://cwe.mitre.org/	Análisis de vulnerabilidades	**Estrategia de comunicación:** Monitoreo automatizado + análisis técnico por NOC-SOC. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC
CISCO Talos	Reporte de vulnerabilidades	https://talosintelligence.com/vulnerability_reports	Reacción ante vulnerabilidades	**Estrategia de comunicación:** Consumo automático de reportes de vulnerabilidades. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC
CISCO Talos	Clasificacion de Reputacion de Direcciones por Actividad de Spam	https://talosintelligence.com/reputation_center/email_rep	Análisis de vulnerabilidades	**Estrategia de comunicación**: Consumo automático de reportes de vulnerabilidades. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC
Wazhu / Virus Total	Boletines emiten alertas sobre vulnerabilidades insurgentes y de día 0.	https://www.incibe.es/incibe-cert/newsletter/confirm/combined/91754/1759498205/PYgbYStsso2QDsutcBw8ZlZopEM7-Vy65tqxvJiwDfg https://www.ibm.com/docs/es/i/7.5.0?topic=security-bulletins https://learn.microsoft.com/es-es/security-updates/	Revisión de boletines emiten alertas sobre vulnerabilidades insurgentes y de día 0.	**Estrategia de comunicación:** Intercambio de información sobre vulnerabildiades, amenazas Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC
ISP Claro	Información sobre fallas de red / coordinación de respuesta antes eventos de red	https://www.claro.com.co/institucional/soporte-tecnico-claro/	Información sobre fallas de red / coordinación de respuesta antes eventos de red	**Estrategia de comunicación**: Intercambio de información / según necesidad contacto con mesa de soporte Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo NOC-SOC
Fiscalía General de la Nación	Entidad del Estado encargada de investigar y acusar ante los jueces las conductas que revisten las características de delito, incluyendo los delitos informáticos, la violación de datos personales, el acceso abusivo a sistemas informáticos, el daño informático, la interceptación de datos y demás conductas tipificadas en la Ley 1273 de 2009.	https://www.fiscalia.gov.co/colombia/ Línea Nacional: 122	• Presunta comisión de delitos informáticos que afecten los activos de información de SISA o de sus clientes (Ley 1273 de 2009).• Violación de datos personales con posible connotación penal.• Acceso abusivo a sistemas de información internos o de terceros administrados por SISA.• Daño informático, fraude informático o suplantación digital.• Incidentes de Seguridad de la Información que requieran denuncia formal ante autoridad judicial.	**Estrategia de comunicación:** Comunicación formal y reactiva mediante denuncia oficial (portal web, presencial o correo institucional). / Activación a través del proceso de gestión de incidentes de SI. Envío de evidencia (logs, reportes, análisis forense) bajo lineamientos legales. Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)	Equipo Seguridad de la Informacion
Procuraduría General de la Nación	Entidad encargada de vigilar el cumplimiento de la Constitución, las leyes, las decisiones judiciales y los actos administrativos, así como de ejercer control disciplinario sobre los servidores públicos y particulares que ejerzan funciones públicas. Facilita la consulta de antecedentes disciplinarios y el trámite de actuaciones administrativas relacionadas con la función pública.	procuraduria.gov.co/Pages/Consulta-de-Antec	• Consulta de antecedentes disciplinarios de colaboradores, contratistas o proveedores que ejerzan funciones asociadas a la operación de SISA.• Procesos de vinculación, contratación o auditoría que requieran validación de antecedentes disciplinarios.• Requerimientos formales de autoridades de control relacionados con investigaciones administrativas.• Apoyo a procesos internos de cumplimiento, ética y control disciplinario, cuando aplique.	**Estrategia de comunicación**: Comunicación formal mediante consultas en plataformas oficiales y atención a requerimientos. Interacción en procesos de: verificación de antecedentes auditorías requerimientos disciplinarios Ver necesidades y expectativas en: Grupos de interés especial (Ver: SI-F-037 CONTACTO AUTORIDAD-GRUPOS)+}	Equipo de Talento Humano Equipo Seguridad de la Informacion