AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD

BOGOTÁ D.C. MAYO DE 2021

TABLA DE CONTENIDO

1. OBJETIVO

Establecer los mecanismos para la gestión de incidentes de seguridad internos o externos, mediante la identificación, registro, contención y mitigación de la causa que origine la pérdida de confidencialidad, disponibilidad e integridad sobre uno o más activos de información de la Agencia para la Reincorporación y la Normalización, disponiendo las herramientas que permitan comunicar y tomar las acciones para disminuir, controlar o eliminar su ocurrencia.

2. ALCANCE

Inicia con la identificación de un posible incidente de seguridad, continúa con actividades de contención y mitigación; erradicación, recuperación y finaliza con la documentación de las acciones y lecciones aprendidas.

Este documento es aplicable a todos los eventos o incidentes de seguridad que afecten los principios de confidencialidad, disponibilidad e integridad de los activos de información de la Agencia para la Reincorporación y la Normalización, así como a los empleados públicos, contratistas, pasantes y terceros.

3. DEFINICIONES

ACTIVO DE INFORMACIÓN: Es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la entidad

AMENAZA: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

ATAQUE: Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o de violar alguna política de seguridad de alguna otra manera.

CADENA DE CUSTODIA: es un proceso continuo y documentado aplicado a los elementos Materiales Probatorios, evidencia física y evidencia digital, por parte de los empleados públicos, contratistas y particulares que con ocasión a sus funciones u obligaciones se debe garantizar su autenticidad y capacidad demostrativa que no ha sido alterado (mismidad), mientras que la autoridad competente ordena su disposición final.

CCOCI: Comando Conjunto Cibernético de la FF.MM

CLASIFICACIÓN: La clasificación de un incidente tiene como objetivo principal el recopilar toda la información que pueda ser de utilizada para la resolución del mismo.

El proceso de clasificación debe implementar, al menos, los siguientes pasos:

- **Categorización:** se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de evento o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados.
- **Establecimiento del nivel de criticidad:** dependiendo del impacto y la urgencia se determina, según criterios preestablecidos, un nivel de criticidad especifico.
- **Asignación de recursos**: Debe contarse con los profesionales especializados de infraestructura (redes, servidores, telefonía, seguridad etc.).

CIBERINCIDENTE: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información que es gestionado de acuerdo con los procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quien esté autorizado. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

CSIRT: (Computer Security Incident Response Team) Equipo de respuesta frente a Incidencias de Seguridad Informática, es un grupo de profesionales que recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas.

DISPONIBILIDAD: Propiedad o característica de los activos consistente en que los usuarios o procesos autorizados tiene acceso a los mismos cuando lo requieren.

EQUIPO DE SEGURIDAD INFORMÁTICA Y REDES: conformado por el Profesional de Seguridad informática quien lo lidera y los profesionales de la OTI que se designen para seguridad y redes.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la

política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

EAIS: Equipo de atención de Incidentes de Seguridad, se refiere al equipo especializado que se conforma para la atención del incidente de seguridad de la información. Este grupo estará conformado por el equipo de seguridad informática y redes, el Oficial de Seguridad de la Información de la ARN y el SOC).

HERRAMIENTA DE GESTIÓN: software utilizado para el registro y documentación de casos relacionados con Incidentes de seguridad de la información.

INCIDENTE: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

INCIDENTE DE SEGURIDAD DIGITAL: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos.

- **INCIDENTE DE SEGURIDAD INFORMÁTICA**: Una violación o inminente amenaza de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas estándar seguridad. En el contexto de este procedimiento, una inminente amenaza es definida como una situación en la cual la organización tiene evidencias para creer que un incidente de seguridad va a ocurrir.
- **INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFORMACIÓN: Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos. Inventario de activos.

NIVEL DE CRITICIDAD: el valor asignado a un riesgo o amenaza de acuerdo a la evaluación de incidencia en la confidencialidad, integridad, disponibilidad para la operación de la entidad. Es frecuente que existan múltiples incidencias concurrentes por lo que es necesario determinar un nivel de criticidad para la resolución de las mismas. El nivel de prioridad se basa esencialmente en dos parámetros:

- **Impacto:** determina la importancia del incidente o ciberincidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.
- **Tiempo:** depende del tiempo máximo de demora que acepte el usuario para la resolución del incidente o ciberincidente y/o el nivel de servicio.

NO REPUDIO: Se debe tener la capacidad para probar que una acción o un evento relacionados con los activos de información han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PROCESO DISCIPLINARIO: Es un conjunto de actividades encaminadas a investigar y/o a sancionar determinados comportamientos o conductas de los servidores públicos o particulares que ejerzan funciones públicas, que conlleven incumplimiento de deberes, extralimitación en el ejercicio de derechos y funciones, incurrir en prohibiciones y violación del régimen de inhabilidades, incompatibilidades, impedimentos y conflicto de intereses.

REGISTRO: Documento o evidencia electrónica que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas. Los registros pueden utilizarse, por ejemplo, para documentar la trazabilidad y para proporcionar evidencia de verificaciones, acciones preventivas y acciones correctivas.

SEGURIDAD DIGITAL: es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

SOC: Security Operation Center.

VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN: La vulnerabilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas haciendo uso de un fallo, debilidad, error de configuración, carencia de procedimientos o fallos de diseño en un sistema de información poniendo en riesgo que pueden poner en riesgo la información.

4 CONTENIDO Y DESARROLLO

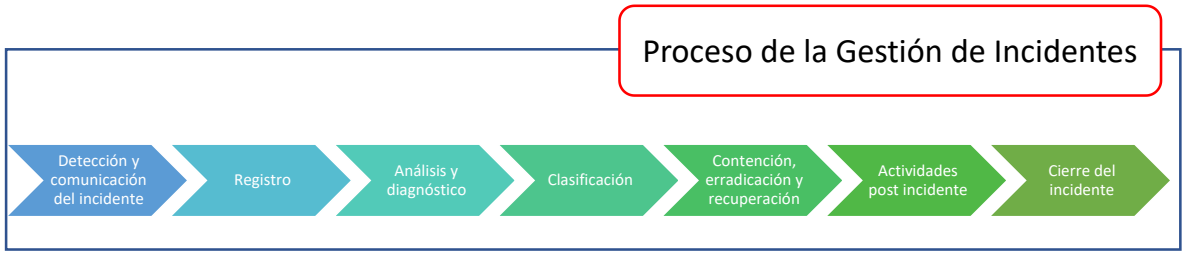
4.1 GENERALIDADES

La gestión de incidentes de seguridad consiste en realizar un seguimiento de los eventos e incidentes de seguridad de la información con el propósito de proteger los activos de información frente a pérdidas de integridad, confidencialidad o disponibilidad de los activos de información en custodia de la entidad.

4.1.1 METODOLOGÍA

Las actividades para la gestión de incidentes de seguridad se describen en la siguiente figura:

El proceso de gestión de incidentes inicia con el registro y clasificación en la herramienta de gestión a continuación, se realiza un diagnóstico por parte de los integrantes del *Equipo de atención de Incidentes de Seguridad*, se definen las acciones para la resolución del incidente; todo lo relacionado con el incidente debe estar documentado en la herramienta de gestión.



Fuente de Información: Propia de OTI

4.1.2 EQUIPOS DE ATENCIÓN DE INCIDENTES DE SEGURIDAD

Este equipo llamado *EAIS* podrá solicitar información o la participación de otros profesionales, especialistas, operadores estratégicos o los procesos requeridos para la atención del incidente de seguridad.

4.1.3 DETECCIÓN Y REPORTE DE INCIDENTES

Todos los empleados públicos y contratistas de la Agencia para la Reincorporación y la Normalización son responsables de notificar cualquier tipo de evento o incidente de seguridad de la información o ciberincidente que afecte el funcionamiento normal de los procesos y los activos de información de la ARN.

Esta notificación se realiza a través de la Mesa de Servicios, utilizando la herramienta Aranda, la cual cuenta con la siguiente información:

Campo	**Herramienta Aranda**
Fecha de reporte	Lo genera la herramienta por defecto
Hora del reporte	Lo genera la herramienta por defecto
Nombres y apellidos completos	Se elige el usuario de acuerdo con directorio activo.
Dependencia	Se elige el usuario de acuerdo con directorio activo.
Cargo	Se elige el usuario de acuerdo con directorio activo.
Correo Electrónico	Se elige el usuario de acuerdo con directorio activo.
Fecha y hora de observación del incidente	Se debe indicar en el campo descripción del incidente
Descripción del incidente	Registrar el detalle de la información presentada
Servicio asociado	Se elige de acuerdo con la parametrización de la herramienta

El usuario debe reunir la información que permita identificar los activos involucrados en la situación a reportar que puede incluir entre otros elementos: capturas de pantalla, correos electrónicos, fotografías, videos, o similar.

4.1.4 REGISTRO

La Mesa de Servicios toma los datos necesarios reportados por los usuarios y realiza el registro correspondiente en la herramienta de gestión generando el respectivo número de caso.

La Mesa de Servicios transfiere el caso al SOC o al especialista responsable, quien realiza el análisis preliminar, y documenta el caso respectivamente.

El SOC teniendo en cuenta la información de las herramientas de monitoreo realiza el registro correspondiente en la herramienta de gestión generando el

respectivo número de caso y transfiere el caso cuando así se requiera al especialista responsable, quien realiza el análisis preliminar, y documenta el caso respectivamente.

4.1.5 ATENCIÓN PRIMARIA DEL CASO

El SOC realiza el análisis del escenario, recopila la información necesaria y emite las recomendaciones pertinentes informando el impacto del mismo y la criticidad del incidente de seguridad de la información, teniendo en cuenta la afectación sobre uno o varios activos de información, de acuerdo a lo descrito en el presente documento

4.2 CLASIFICACIÓN Y CATEGORIZACIÓN DE INCIDENTES DE SEGURIDAD EN LA HERRAMIENTA DE GESTIÓN DE CASOS

Tipo de incidente	Descripción	Categoría	Servicio	Especialista
Denegación de servicio	Incidentes relacionados con ataques de denegación de servicios (DoS) o denegación de servicios distribuida (DDoS).	SOC (Security Operation Center)-Gestión de vulnerabilidades-Denegación de servicio	Gestión de disponibilidad	Soporte ARN Soporte SOC
			Monitoreo SOC	Soporte SOC
Código malicioso	Incidentes provocados por malware (virus, gusanos, troyanos, bombas lógicas, spyware, rootkits, etc.).	Infraestructura. Administración de Plataforma. Seguridad de la Información	Correo- spam-malware.	Soporte ARN Soporte SOC
Hacking	Cualquier actividad o tráfico sospechosos que puedan alterar el funcionamiento del sistema y estén relacionadas con un intento de intrusión. Por ejemplo, tentativas de acceso no autorizado al sistema o escaneo de servicios.	SOC (Security Operation Center)-Gestión de vulnerabilidades-Ataques de ingeniería social Phishing	Gestión de confidencialidad	Soporte SOC Soporte ARN
			Monitoreo SOC	Soporte SOC
Violación de políticas	Uso inadecuado de algún activo de información.	SOC (Security Operation Center)-Prevención de fuga de información- Uso inadecuado de información contenida en repositorios ARN	Gestión de confidencialidad	Soporte SOC Soporte ARN
			Monitoreo SOC	Soporte SOC

	Fuga de información.	SOC (Security Operation Center)-Prevención de fuga de información-Divulgación no autorizada de información digital	Gestión de confidencialidad	Soporte ARN Soporte SOC
			Monitoreo SOC	Soporte SOC
	Potencial Fuga de información.	Infraestructura. Administración de Plataforma. Seguridad de la Información-	Monitoreo SOC	Soporte SOC
	Escalada desautorizada de privilegios	Infraestructura. Administración de Plataforma. Seguridad de la Información	Gestión de seguridad informática	Soporte ARN Soporte SOC
	Alertas correlacionador de eventos	Infraestructura. Administración de Plataforma. Seguridad de la Información-	Monitoreo SOC ARN	Soporte SOC
	Modificación, instalación no autorizada de software	SOC (Security Operation Center)-Gestión de eventos e incidentes de seguridad en tiempo real - Modificación, instalación o eliminación no autorizada de software	Gestión de integridad	Soporte ARN Soporte SOC
			Monitoreo SOC	Soporte SOC
	Eliminación de software no autorizado	Soporte - Equipos de Usuario - Computador … (Portátil o De escritorio)	Desinstalación de software no autorizado Asistentes de Información	Soporte ARN GT
			Desinstalación de software no autorizado Soporte Sitio	Soporte en sitio
Vulnerabilidad	Cualquier tipo de incidente provocado por la explotación de una vulnerabilidad en un sistema informático.	Infraestructura. Administración de Plataforma. Seguridad de la Información-	Administración de vulnerabilidades.	Soporte ARN Soporte SOC
		Infraestructura. Administración de Plataforma. Seguridad de la Información-	Gestión de vulnerabilidades	Soporte SOC

Siniestro de equipo	Gestión de seguridad relacionada con pérdida o hurto de equipos	SOC (Security Operation Center)- Prevención fuga de información (DLP)- Siniestros de equipos	Gestión de confidencialidad	Soporte ARN

Además de estas tipologías, la evolución de las tecnologías y la complejidad de los ataques hace posible contemplar la ocurrencia de otros tipos de incidentes que serán actualizados en la presente guía, en el marco del seguimiento y periodicidad de actualización del presente documento.

4.3 PRIORIZACIÓN Y NIVEL DE CRITICIDAD DE INCIDENTES

El *Equipo de atención de Incidentes de Seguridad* determina el nivel de criticidad del incidente de seguridad se requiere identificar el impacto y el tiempo para su atención, y así determinar la zona de criticidad:

Criterios para calificar impacto del incidente de seguridad: se entiende como las consecuencias que puede ocasionar en la organización

IMPACTO	Descripción	Valoración
MUY GRAVE	Extremadamente Dañino: Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad a nivel de: • Afectación Imagen a Nivel Nacional e Internacional. • Sanciones de entes de control. • Daños totales de la infraestructura tecnológica de la entidad.	ALTO
GRAVE	Moderado: Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad. • Afectación Imagen del proceso o área a Nivel de la entidad. • Sanciones a nivel de Control Interno Disciplinario • Daños parciales de la infraestructura de la entidad.	MEDIO
MENOS GRAVE	Menor: Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad: • Afectación Imagen grupo o área a nivel del proceso. • Hallazgos a nivel procesos identificados por el Grupo de Control Interno de Gestión. • Daños pequeños de la infraestructura de la entidad.	BAJO
MENOR	Ligeramente Dañino: Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad: • Afectación Imagen grupo a nivel área o proceso • Sanciones a nivel grupo. • Daños pequeños de la infraestructura de la entidad.	

Criterios para calificar tiempo de atención del incidente de seguridad:

Tiempo	Descripción
Alto	Atención de forma inmediata (0 - 2) horas
Medio	Atención de forma inmediata (0 - 8) horas
Bajo	Atención de forma inmediata (0 - 24) horas

Zona de criticidad:

Tiempo/ IMPACTO	ALTA	MEDIA	BAJA
ALTO	(A)	(A)	(M)
MEDIO	(A)	(M)	(B)
BAJO	(M)	(B)	(B)

En caso que un incidente de seguridad de la información se considere **MUY GRAVE** (es decir que afecta las operaciones de la Entidad), el oficial de Seguridad Informática informa a la Jefatura de la Oficina de Tecnologías de la Información y a los grupos de respuesta a emergencias cibernéticas de Colombia la ocurrencia de dicho evento y al Oficial de Seguridad de la Información de la ARN, quien deberá informar a la alta gerencia (Dirección General y Secretaría General) para la instalación de la mesa de crisis, en donde se analizará los recursos financieros, humanos y tecnológicos correspondientes a la atención de la emergencia, al igual evaluar las alternativas para la contención, erradicación y solución del incidente, a través de la activación del Plan de continuidad de la ARN.

4.4 ROLES Y RESPONSABILIDADES

Roles	Responsabilidades
EAIS: Equipo de atención de Incidentes de Seguridad	• Poner en marcha el modelo de gestión de eventos e incidentes de seguridad apoyado con una metodología clara y precisa donde se especifique como mínimo las siguientes etapas: preparación; detección y análisis; contención, erradicación y recuperación; actividades pos-incidentes • Revisar los reportes de las herramientas de seguridad para el análisis pertinente y otras fuentes con el propósito de mejorar la gestión de incidentes de seguridad. • Mantener contacto apropiado con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información. • Coordinar las actividades y demás tareas requeridas para atención de incidentes, problemas, solicitudes o escalamientos por parte de: o Personal responsable del servicio de la Mesa de servicios tecnológicos. o Personal responsable del servicio de monitoreo.

	○ Personal responsable del servicio de monitoreo de redes. ○ Dueños o responsables de los activos de información ○ Personal designado por la ARN para iniciar requerimientos y /o escalamientos ○ Jefatura de la OTI ○ Coordinaciones de servicios de TI en la ARN ○ Administradores y técnicos de soporte de los servicios de TI ○ Asistentes de información de la ARN. ○ Proveedores o terceros autorizados por la ARN. • Contener los incidentes de seguridad detectados, teniendo en cuenta la experticia necesaria en aplicar políticas y configuraciones necesarias a los dispositivos de seguridad, dispositivos de red, servidores o estaciones de trabajo, de tal manera que se detenga y minimice el impacto de un ataque cibernético. • Remediar el impacto materializado en la infraestructura tecnológica de la ARN, que se dé como consecuencia de ataques cibernéticos,
SOC	• Detectar potenciales incidentes de seguridad de la información, para lo cual deberá monitorear y verificar los elementos de control. • Atender o escalar los casos reportados por la mesa de servicios. • Crear los casos en las herramientas correspondientes para aquellos incidentes recurrentes o repetitivos y que requieran ser escalados al siguiente nivel. • Participar en las actividades descritas en el procedimiento de incidentes de seguridad, la toma de la información, la cadena de custodia y el acompañamiento necesario ante las instancias correspondientes. • Generar reportes de incidentes de seguridad periódicos y urgentes con el contenido técnico detallado para su mitigación y/o remediación en el corto y mediano plazo. • Generar reportes de eventos y documentar análisis de tendencias y recomendaciones relacionadas con seguridad, para que la entidad pueda tomar acciones preventivas y/o correctivas. • Realizar las actividades posteriores al incidente tales como documentar lecciones aprendidas y registrar la información que corresponda en la base de conocimiento.
Grupo de infraestructura y soporte	• Aplicar políticas y configuraciones necesarias a los dispositivos de seguridad, dispositivos de red, servidores o estaciones de trabajo, de tal manera que se detenga y minimice el impacto de un ataque cibernético. • Aprovisionar el software, hardware y dispositivos necesarios para el desarrollo del proceso de gestión de incidentes de seguridad.
Oficial de Seguridad de la Información	• Retroalimentar el adecuado tratamiento a los incidentes de seguridad de la información detectados o reportados. • Hacer un seguimiento periódico a los incidentes de seguridad presentados en la Mesa de Seguridad por parte del Oficial de Seguridad informática
Mesa de Seguridad	• Apoyar las acciones para brindar capacitación y sensibilización a los servidores públicos y colaboradores y demás partes interesadas en

	cuanto al reporte de incidentes de seguridad de la información y vulnerabilidades de los sistemas de información con los que cuenta la Entidad. • Evaluar los informes presentados por la Oficina de Tecnologías de la información relacionados con la gestión de incidentes de seguridad y toma las decisiones necesarias para asegurar la protección de la información.
Administradores de los componentes de la infraestructura	• Activar los "logs" y que permitan la revisión de eventos y propender por que existan las copias de respaldo de los mismos, de acuerdo con las políticas que se definan para su conservación. • Gestionar los cambios necesarios en los componentes de la infraestructura con el fin de mitigar y contener eventos e incidentes de seguridad que se presenten, así como asegurar la funcionalidad de los mismos (recuperación).
Empleados públicos, contratistas y pasantes	• Tomar conciencia de su responsabilidad de reportar eventos y debilidades de seguridad de la información tan pronto como sea posible a través de la Mesa de servicios. • Asistir a las capacitaciones y participar en las campañas de sensibilización que se realicen al interior de la entidad. • Reportar oportunamente los incidentes o eventos de seguridad de la información y cualquier comportamiento anormal que se presente en la Entidad o en sus activos de información.
Grupo de Gestión Administrativa y Dueños de los activos de información	• Hacer la valoración económica del activo de información involucrado en un evento/incidente de seguridad de la información.

4.5 CONTENCION, ERRADICACIÓN Y RECUPERACIÓN

Es importante para la ARN implementar una serie de actividades que permita tomar decisiones oportunamente para mitigar y evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad sobre los activos de la información.
Esta actividad se divide en cuatro (4) componentes:

4.5.1 IDENTIFICACIÓN

Para detectar eventos que puedan derivar en la materialización de un incidente de seguridad, determinar su alcance y los sistemas afectados, uno de los principales mecanismos es el análisis de logs, registros y fuentes de información.

Otras fuentes de información para identificar incidentes de seguridad son una fuente de información externa, un usuario externo, un reporte de un CSIRT, así como de los grupos de respuesta a emergencias cibernéticas de Colombia tales como Colcert y CCOCI o de otro organismo, etc.

Dentro de este proceso de identificación, es importante relacionar cuál activo o activos de información fueron afectados.

Algunas fuentes de información a considerar son las siguientes:

- Consolas de antivirus.
- Sistemas de Detección / Prevención de Intrusión (IDS/IPS).
- Alertas de correlacionador de eventos.
- Registros de auditoría para detectar intentos de acceso no autorizados.
- Registro de conexiones bloqueadas en el firewall.
- Registro de conexiones realizadas a través de proxy.
- Registros en la herramienta DLP (Data Loss Prevention).
- Consumos excesivos y repentinos de memoria o disco en servidores.
- Anomalías de tráfico como picos de consumo a horas no habituales.
- Cuentas de usuario inusuales en el sistema o especialmente privilegiadas.
- Carpetas ocultas o con tamaños, nombres o ubicaciones sospechosas, que pueden indicar algún tipo de fuga de información o registro por parte de algún malware.
- Carpetas con permisos inusuales, carpetas huérfanas y que puedan determinar algún tipo de intrusión o rootkit.
- Entradas sospechosas en el registro, principalmente en el caso de infecciones por malware en sistemas Windows.
- Sesiones abiertas en la máquina desde otros equipos, anomalías en las tablas ARP, carpetas compartidas inusuales, o un elevado número de conexiones con TCP activado de manera anómala.
- Tareas programadas o actividad sospechosa en los registros de auditoría y
- logs que indique un funcionamiento anormal del sistema o intentos de intrusión.
- Reporte del antivirus de alguna herramienta habitualmente instalada en el sistema de identificación de rootkits, de control de integridad de ficheros, firma de los binarios, etc.
- Logs de Servidores y de Aplicaciones
- Listado de puertos lógicos/físicos conocidos y de los puertos utilizados.
- Arquitectura de la red de TI actualizada.
- Inventarios de activos de información.
- Volcados de memoria y archivos de paginación.
- Servidores (Web, DHCP, Email, Mensajería Instantánea, VoIP Servers, FTP o cualquier servicio de filesharing), almacenamiento en red, medios tanto internos como externos que contemplan: Dispositivos USB, Firewire, CD/DVD, PCMCIA, Discos Ópticos y Magnéticos, Discos Duros Extraíbles, Memorias SD y MicroSD etc., Dispositivos celulares, PDAs, Cámaras Digitales, Grabadoras de video y audio.

- Información relevante que permita la identificación de un incidente.

4.5.2 RECOPILACIÓN DE EVIDENCIAS

Para recopilar la evidencia necesaria los usuarios responsables de los elementos deben colaborar con la diligencia y no pueden alterar la información; para dicha actividad se debe tener en cuenta lo dispuesto en el documento *Manual del Sistema de Cadena de Custodia* emitido por la Fiscalía Nacional de la Nación apoyado en la documentación de manejo de evidencia forense del SOC.

El Oficial de Seguridad Informática en conjunto con el SOC deben coordinar la recopilación y conservación de las evidencias, con el fin de reducir la probabilidad de que estas se modifiquen después y sean consideradas no admisibles ante un ente judicial. Dependiendo de la evidencia que se genere en el tratamiento del incidente, se determinará el lugar en donde se conservarán (Se determinarán de acuerdo con la clasificación de la información) para garantizar la integridad, disponibilidad y confidencialidad de las mismas.

Las actividades de tipo forense enmarcadas en la cadena de custodia deben incluir al menos lo siguiente:

- Establecimiento del perímetro de seguridad para que nadie pueda acercarse y altere la escena
- Tratamiento al equipo afectado, el cual no debe apagarse si está encendido, así como tampoco debe encenderse si se encuentra apagado, lo anterior con el fin de no alterar o borrar información
- Registro de información que rodea la evidencia (entorno)
- Registro fotográfico del entorno de la evidencia
- Recolectar la evidencia
    - Fecha y hora del sistema
    - Lista de puertos abiertos
    - Volcado de la memoria RAM
    - Rutas estáticas
    - Rutas dinámicas
    - Algoritmos de enrutamiento habilitados
    - Listas de acceso
    - Mecanismo de seguridad habilitados
    - Salvar la información de los registros
- Rotular los elementos que hacen parte de la evidencia
- Almacenamiento y custodia segura de la evidencia
- Generar una copia maestra del original para a partir de esta, generar las imágenes que se requieran toda vez que el análisis de datos nunca se debe

realizar en la imagen original. Posterior a esto se realiza la verificación de la integridad de la imagen (hash).

- Preservación de la evidencia. Una vez recolectada la evidencia, se debe garantizar su integridad, procediendo de la siguiente manera:

  - Embalar y sellar la evidencia bajo condiciones adecuadas en función al tipo de evidencia, hacer uso de fundas antiestáticas, contenedores acolchados, etc.; se debe sellar el contenedor, indicando los datos de la persona que realizado dicha actividad.
  - En la medida de lo posible debe guardarse en un empaque de plástico para evitar daños por efectos ambientales como polvo, temperatura, humedad y salinidad.
  - Las copias generadas de los elementos materia de prueba (EMP) deben contener los respectivos archivos hash de la información recopilada.
- Almacenar la información en sitio seguro.

Se debe almacenar la evidencia obtenida en un sitio con medidas de seguridad como: un espacio con llave que pueda garantizar que el acceso a ella sea limitado, garantizando su integridad, disponibilidad, confidencialidad, mismidad y exactitud.

Una vez que se ha identificado un incidente de seguridad, los equipos afectados y se han aislado los mismos del resto de la red, se debe tener en cuenta, dentro de la estrategia de contención, la preservación de evidencias para el análisis forense del incidente y, dentro de dicha preservación, deben extraerse los datos volátiles de la memoria antes de proceder al apagado del sistema.

La información almacenada en la memoria del equipo puede resultar muy importante para el proceso de análisis en casos de malware o de intrusiones y, si se apaga el sistema, se perderían, por lo que en la medida de lo posible se deben aplicar técnicas forenses para su adquisición antes de apagarlo. Si se requiere recopilar evidencia debe tomarse en cuenta lo descrito en el Manual del Sistema de Cadena de Custodia emitido por la Fiscalía General de la Nación.

4.5.3 CONTENCIÓN Y MITIGACIÓN

a) Estrategias de contención

Identificado el incidente, hay que contenerlo y mitigar sus efectos usando la información obtenida anteriormente. Para ello es necesario definir la extensión, el tipo de equipos afectados y buscar las características comunes para aislar el

incidente en función de esos patrones. Las principales recomendaciones para la contención y mitigación de un incidente de seguridad y que pueden aplicarse son:

- Desconectar el equipo o segmento de red del resto de redes de la entidad: Esto puede hacerse si se trata de un equipo aislado directamente desconectando el cable de red del mismo o aislando un segmento de red en una VLAN o similar.
- En caso de tratarse de algún equipo crítico puede aislarse únicamente el tráfico estrictamente necesario permitiendo solamente el tráfico crítico para el funcionamiento del sistema.
- En el caso de una vulnerabilidad que permita alguna intrusión o algún tipo de denegación de servicio se deben aplicar todas las recomendaciones de mitigación proporcionadas por el fabricante del producto, e instalar los parches recomendados.
- Desconectar de la red el o los servidores que estén siendo víctimas de un ataque informático con el fin de no borrar, modificar o perder posible evidencia.
- Bloqueo del tráfico de los puertos específicos en cualquier sentido de transferencia.
- Cambio de prioridad en aplicaciones o en asignación de ancho de banda.
- Interrupción de actividades u operaciones afectadas por el incidente.
- Bloquear cuentas de usuario
- Incorporación de reglas de filtrado en el firewall
- Cambio de contraseñas

Ejemplos de estrategias de contención a incidentes

Incidente	Ejemplo	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuenta
Código Malicioso	Infección con virus	Desconexión de la red del equipo afectado
Acceso no autorizado	Compromiso del Root	Apagado del sistema
Reconocimiento	Scanning de puertos	Incorporación de reglas de filtrado en el firewall
Código Malicioso	Propagación de un malware, patrón de comportamiento de una denegación de servicio o intento de intrusión mediante fuerza bruta	Bloqueo de cuentas de correo, de acceso a unidades compartidas, de conexiones salientes. Modificación de políticas o reglas en firewall en el IDS/IPS es posible configuración de reglas de filtrado para denegaciones de servicio o intentos de intrusión.

b) Estrategias de Erradicación y Recuperación

Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier efecto derivado por el incidente ya sea en la infraestructura centralizada como en la infraestructura de usuario final, para esta actividad se debe cumplir lo siguiente:

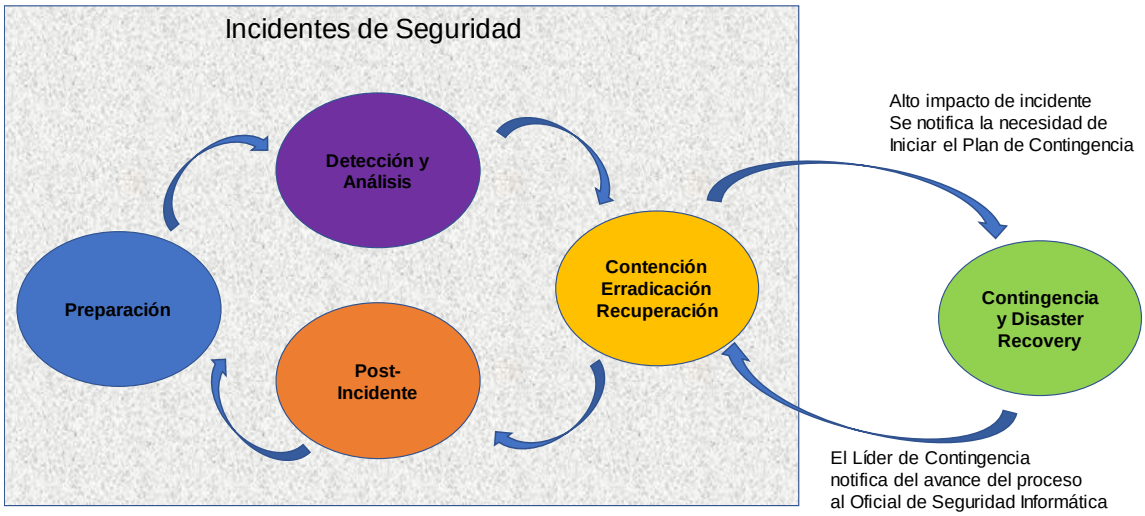
- Detectar la causa del incidente analizando con los líderes de servicios, proveedores tecnológicos, oficial de seguridad informática y coordinador del grupo de infraestructura y soporte u otros profesionales involucrados.
- Analizar el despliegue de medidas adicionales cuando así se requiera, como herramientas de monitoreo de seguridad en la infraestructura tecnológica física y virtual de la entidad.
- Actualización de firmware para las herramientas de hardware y software, ya sea propiedad de la ARN o de los proveedores de TI, con el fin de proteger los servicios afectados contra una reactivación del incidente o afectación a otros servicios.
- Evaluar las amenazas de los servicios afectados por parte de los líderes de los servicios y/o proveedores de servicios, generando las evidencias necesarias de dicha gestión.

Posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el líder del servicio o componente del servicio, deben restablecer la funcionalidad de los sistemas afectados, y realizar un fortalecimiento de la seguridad del sistema que permita prevenir incidentes similares en el futuro.

Ejemplos de estrategias de erradicación de incidentes

Incidente	Ejemplo	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Procedimiento para restauración del servicio de Red
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

Para cada recuperación del servicio, se debe implementar las estrategias de recuperación de servicios de acuerdo al escenario del incidente que se ha materializado, en el marco de los planes de contingencia de servicios de TI.
En algunas ocasiones durante el proceso de gestión de Incidentes de Seguridad se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.



Fuente: Ministerio de Tecnologías de la Información. Seguridad y privacidad de la información. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Versión 1.2. 6 de noviembre de2016

c) Estrategias y controles de prevención

Después de que el incidente ha sido contenido se debe realizar una gestión de controles para prevenir que se presenten circunstancias similares en el futuro para esta actividad se puede tener en cuenta lo siguiente:

Gestión de Parches de Seguridad	Contar con una gestión de vulnerabilidades (Sistemas Operativos, Bases de Datos, Aplicaciones, otro Software Instalado), esta gestión ayudará a los administradores en la identificación, adquisición, prueba e instalación de los parches.
Aseguramiento de plataforma	Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones por default (usuarios, contraseñas y archivos compartidos). Revisión periódica de logs de la infraestructura de TI y de los sistemas de información. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el login de eventos. Todos los elementos que hacen parte de la infraestructura critica, deben estar incluidos en las herramientas de monitoreo y correlacionadores de eventos.
Seguridad en redes	Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente.

	Los dispositivos como IDS o IPS deben contar con las firmas y actualizaciones vigentes. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.
Prevención de código malicioso	Todos los equipos de la infraestructura (tanto servidores como equipos de usuario final) deben tener activo antivirus, antimalware con las firmas de actualización al día.
Sensibilización y entrenamiento de usuarios	Los usuarios finales incluidos los administradores de TI deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad.
Otras acciones	• Validar el aislamiento del equipo afectado. • Eliminar el posible malware y deshabilitar las cuentas de usuario afectadas. • Identificar y mitigar todas las vulnerabilidades que se explotaron. • Determinar las causas y los síntomas del incidente para determinar las medidas de mitigación más eficaces. • Identificar y eliminar todo el software utilizado por los atacantes. • Recuperar la última copia de seguridad limpia. • Identificar servicios utilizados durante el ataque.

4.5.4 DOCUMENTACIÓN DE LECCIONES APRENDIDAS

Las lecciones aprendidas apoyan la atención de futuros incidentes de seguridad y/o contribuyen a solucionar nuevos incidentes con similares características. Asimismo, permite conocer a los atacantes, sus estrategias y sus patrones en las denegaciones de servicio. Las nuevas vulnerabilidades que afectan los sistemas más críticos de la organización.

Esta información permite conocer la naturaleza y tipo de incidente, las características del mismo y los vectores de infección para robustecer la parametrización de los sistemas de seguridad, así como para fomentar campañas de sensibilización adaptadas a la entidad, conocer sus puntos más débiles y saber cómo protegerlos.

Es importante que esta documentación sea detallada, que incluya aspectos tales como: acciones realizadas durante la atención de la incidencia. causa raíz identificada, acciones realizadas para reestablecer el servicio. número de caso de

proveedor o tercero tiempo total de indisponibilidad y número de usuarios afectados, qué herramientas se utilizaron y cómo, las investigaciones realizadas y sus resultados, el personal que participó, la documentación de apoyo utilizada para resolver el incidente, la línea temporal de las acciones seguidas, etc.

a) Acciones administrativas

Los incidentes de seguridad que ameriten acciones de tipo legal o penal, deben ser investigados por las personas idóneas de los organismos competentes para la recolección de la información que garanticen la admisibilidad y cadena de custodia de las pruebas recolectadas. Estos incluyen los establecidos en el Código Disciplinario Único. Aquellas personas que estén involucradas directa o indirectamente en posibles incidentes de seguridad, serán tratados por los mecanismos establecidos por Control Interno Disciplinario para adelantar las investigaciones requeridas.

Las investigaciones especiales adelantadas por los Entes de Control relacionadas con la Seguridad de la información deben ser notificadas a la Jefatura de la Oficina de Tecnologías de la Información y al Oficial de Seguridad de la Información de la ARN.

En el caso que se presente un incidente de Seguridad de la Información en el cual sea necesario la verificación de si existe o no participación de algún empleado público o contratista de la ARN en los hechos, debe ser reportado a Control Interno Disciplinario, mediante comunicación remitida por SIGOB. Si lo requiere, el Grupo de Control Interno Disciplinario, puede solicitar el apoyo a la Oficina de Tecnologías de la Información y a la Mesa de Seguridad.

4.6 PLAN DE COMUNICACIÓN Y NIVELES DE ESCALAMIENTO PARA LA GESTIÓN DE INCIDENTES

En el marco de la gestión de los incidentes de seguridad de la información, es necesario tener en cuenta los siguientes niveles de escalamiento.

Origen	Impacto	Responsable de acciones	Responsable de tratamiento (*)	Ejecutor de solución (*)
• Usuario • Tercero • Contratistas • Elementos de detección de incidentes.	Alto	• Mesa de Seguridad de la ARN • Oficial de Seguridad de la Información • Oficial de Seguridad Informática. • Jefe de la OTI	Oficial de Seguridad Informática.	• Líderes Técnicos de Servicios TI • Proveedor de servicios de conectividad

• Grupo de Infraestructura y Soporte • Grupo de Sistemas de Información		• Grupo de Infraestructura y Soporte. • Proveedor de Servicios - SOC		• Proveedor servicios de nube privada • Proveedores de Servicios de Software.
	Medio	• Oficial de Seguridad de la Información • Oficial de Seguridad Informática. • Jefe de la OTI • Grupo de Infraestructura y Soporte. • Grupo de Sistemas de Información • Proveedor de Servicios - SOC		
	Bajo	• Oficial de Seguridad Informática. • Jefe de la OTI • Grupo de Infraestructura y Soporte. • Proveedor de Servicios - SOC		

(*) Los nombres y números de contacto de los profesionales se encuentran definidos en la Matriz de escalamiento de la Mesa de servicios

En caso que se requiera, se debe realizar el escalamiento a Control Interno Disciplinario, Talento Humano o quien realice sus funciones para aplicar las acciones correspondientes.

4.6.1 CÓMO REPORTAR UN INCIDENTE ANTE CSIRT

Una vez identificado el incidente de seguridad digital por el Oficial de Seguridad Informática deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como **Muy Grave y Grave** por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación del CSIRT Gobierno.

Los incidentes catalogados, como **Menos Grave y Menor**, deben ser comunicados al CSIRT Gobierno en el formulario establecido una vez sea

gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos

Mesa de servicio CSIRT Gobierno
Contactando a la mesa de servicio, llamando a la línea gratuita 018000910742, Opción 2, seguridad digital.
Correo electrónico:
Enviando un mensaje de correo electrónico a través de la lista de distribución seguridaddigital@reincorporacion.gov.co informando el incidente al buzón csirtgob@mintic.gov.co, adjuntando el Formato de Reporte de Incidentes debidamente diligenciado.
Mesa de servicio CSIRT Ponal
Contactando a la mesa de servicio, llamando a las líneas (571) 5159090/ 5159586

Enviando un mensaje de correo electrónico a través de la lista de distribución seguridaddigital@reincorporacion.gov.co informando el incidente al buzón ponal.csirt@policia.gov.co

4.6.2 CÓMO REPORTAR UN INCIDENTE AL COLCERT

En el evento de que algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Entidad, haya sido vulnerado o comprometido se debe realizar el reporte de acuerdo con las siguientes indicaciones dicho reporte está a cargo de los profesionales de la OTI que hacen:

A) **Para reportar un incidente o vulnerabilidad debe escribir a:**
Correo electrónico: contacto@colcert.gov.co
Clave PGP/GPG: verificar la clave en el siguiente link
http://www.colcert.gov.co/?q=contenido/reportar-un-incidente
Para enviar una muestra de malware se podrá escribir a:
Correo electrónico: malware@colcert.gov.co
Clave PGP/GPG: verificar la clave en el siguiente link
http://www.colcert.gov.co/?q=contenido/reportar-un-incidente

Adicionando la siguiente información:
Nombre(s) y Apellido(s)
País
Zona horaria
Número de Teléfono
Correo electrónico
Nombre de la Entidad (si aplica)

Número de Teléfono de la entidad (si aplica)
Número de Móvil
Tipo de Organización: Gobierno
Tipo de Sector: Presidencia

Información del host(s) objetivo(s):
Nombres de los hosts y direcciones IPs
Función del sistema (web server, mail server, etc.)
Sistema(s) Operativo(s)
Aplicaciones involucradas en el incidente

Información del host(s) origen:
Nombres de los hosts y direcciones IPs
Función del sistema (web server, mail server, etc.)
Sistema(s) Operativo(s)
Aplicaciones involucradas en el incidente

Información del Incidente:
Fecha y hora (Timestamp)
Zona horaria del Incidente
Tipo de Incidente:
Taxonomía (seleccione la clase y el tipo que aplique al incidente) teniendo en cuenta el siguiente enlace:
http://www.colcert.gov.co/sites/default/files/Taxonomia_colCERT.pdf

Descripción adicional
Si desea enviar información de logs u otro tipo de información por favor utilizar la llave pública que está publicada en el siguiente link:
Clave PGP/GPG: verificar la clave en el siguiente link
http://www.colcert.gov.co/?q=contenido/reportar-un-incidente
Después de realizar el reporte recibirá el número de ticket asignado al correo electrónico indicado.

B) **Formas de Reportar un Phishing:**

- En su gestor de correo, puede crear un nuevo mensaje, arrastrar y soltar el correo electrónico de phishing en el nuevo mensaje. Dirija el mensaje a phishing-report@colcert.gov.co y envíelo.
- En su gestor de correo también puede abrir el mensaje de correo electrónico * y seleccionar Archivo> Propiedades> Detalles. Aparecerán los encabezados del correo electrónico. Puede copiarlos como normalmente copia el texto e incluirlo en un nuevo mensaje a phishing-

report@colcert.gov.co Si no puede reenviar el mensaje de correo electrónico, como mínimo, envíe la URL del sitio web de phishing.
- Puede reportar el phishing enviando un correo electrónico a phishing-report@colcert.gov.co

4.6.3 INCIDENTES CONSIDERADOS DELITOS INFORMÁTICOS

Si el incidente es considerado un delito informático y requiere de una denuncia penal según lo establecido en la ley 1273 de 2009 debe comunicarse a:

CAI Virtual (información unidades en delitos informáticos a nivel nacional) Web: Email: https://caivirtual.policia.gov.co/

Fiscalía General de la Nación

- Unidades de Reacción Inmediata URI
- Salas de Atención al Usuario SAU
- Casas de Justicia

5 DOCUMENTOS DE REFERENCIA

- Procedimiento de Gestión de incidentes
- TI-M-01 Manual del Sistema de Gestión de Seguridad de la información
- Manual del Sistema de Cadena de Custodia
- Manual para cambio de contraseñas de usuarios en directorio activo y portal Azure (Documento de consulta de la Mesa de Servicios)
- Directorio OTI
- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información de MinTIC https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150509_G21_Gestion_Incidentes.pdf
- Resolución 00500 de 2021 emitida por MinTIC
- Formato Reporte de Incidentes - CSIRT Gobierno V3