Contenido

1. OBJETIVO

Asegurar un enfoque coherente y eficaz para la gestión de eventos e incidentes de seguridad de la información, que contemple el evitar o contener el impacto para reducir las consecuencias causadas por los mismos.

2. ALCANCE

Inicia con las actividades de prevención de eventos e incidentes de seguridad, continua con la detección y reporte de evento de seguridad, la categorización y evaluación, la respuesta y comunicación, hasta el cierre del incidente.

3. DEFINICIONES

- **Activo de información**: conocimiento o datos que tienen valor para la Entidad o el individuo.
- **Ciberataque**: acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objeto de la misma o donde el ciberespacio es fuente o herramientas de comisión de un crimen.
- **Ciberespacio**: entorno completo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.
- **Ciberseguridad**: es el desarrollo de capacidades para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.
- **CSIRT (Computer Security Incident Response Team)**: equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos.
- **Evento de seguridad**: ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la Entidad que son esenciales para el negocio.
- **Incidente de seguridad**: ocurrencia de una situación que afecta la protección o el aseguramiento de los datos y aplicaciones de una entidad que son esenciales para el negocio.
- **Investigación forense de seguridad de la información**: aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información.

4. CONDICIONES GENERALES

- La Oficina de Riesgos establece los responsables y actividades para gestionar un evento o incidente de seguridad de la información en cada una de sus etapas, con una respuesta rápida, eficaz y ordenada.
- La Oficina de Riesgos y la Dirección de Tecnología establecerán un plan de continuidad de negocio institucional que considerará la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos, así como la realización de pruebas del plan de continuidad del negocio que simulen la materialización de ataque cibernético.
- La Entidad participa en grupos de interés externos que manejan temas relacionados con incidentes de seguridad de la información.
- La Entidad colabora con las autoridades que hacen parte del Modelo Nacional de Gestión del Riesgo de Seguridad Digital en los proyectos que se adelanten con el propósito de fortalecer la gestión de ciberseguridad en el sector financiero y a nivel nacional.
- La Entidad informa a los beneficiarios de sus servicios sobre las medidas de seguridad y recomendaciones que deberán adoptar, acción que se presenta en la página web del Icetex – sección “Educación en seguridad de la información” de “Atención al Ciudadano”.
- La Oficina de Riesgos y áreas responsables gestionan los eventos e incidentes de seguridad de la información, dependiendo de la situación presentada.
- Los incidentes donde estén involucrados funcionarios son informados a Secretaría General – Procesos Disciplinarios, con el fin de estimar si debe realizarse alguna revisión adicional desde la perspectiva disciplinaria.
- Todos los eventos e incidentes de seguridad de la información se deben reportar al Comité de Seguridad de la Información.
- El Comité de Seguridad de la Información o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los que definen quien realizará pronunciamientos oficiales ante Entidades externas.
- La persona encargada por el Comité de Seguridad de la Información coordina la atención de las necesidades que tengan los entes de control que participen en la atención de un incidente de seguridad de la información.
- Los miembros del Comité de Seguridad de la Información evalúan la necesidad de solicitar apoyo de terceras partes especializadas como:
  - COLCERT: Centro de respuesta a emergencias cibernéticas.
  - CSIRT Gobierno: Equipo de respuesta a incidentes informáticos de MINTIC.
  - Centro Cibernético de la policía: Equipo de respuesta a incidentes y delitos informáticos, para casos como:

- Acceso abusivo a sistemas informáticos
- Violación de datos personales
- Uso de software malicioso
- Suplantación de sitios web
- Transferencia no consentida de activos
- Phishing
- Ingeniería social

Los datos de contacto de los equipos antes descritos son:

- ColCERT(Grupo de Respuesta a Emergencias Cibernéticas de Colombia) por medio de correo electrónico a: contacto@colcert.gov.co Teléfono:(+571) 2959897, malware@colcert.gov.co
- Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional teléfono 4266900 ext.104092.
- MinTic gestión de incidentes, seginf@mintic.gov.co

- El procedimiento de gestión de incidentes de seguridad de la información se ha definido en 7 fases para cumplir con el objetivo principal, ellas son:

  o Fase 1: Prevención de eventos e incidentes de ciberseguridad: contiene las actividades de prevención de eventos e incidentes, comprenden acciones que permitan tener la capacidad de limitar o contener de un posible incidente de seguridad, como son: adopción, revisión y actualización de políticas, procedimientos y controles que prevengan la fuga de datos.

  o Fase 2 - Detección y reporte de evento de seguridad: cualquier irregularidad de seguridad que puedan impactar de forma negativa la integridad, confidencialidad y disponibilidad de los activos de información que se encuentran configurados en la misma y su reporte.

  o Fase 3 - Categorización y evaluación: contempla la evaluación de cada evento de seguridad de la información y se determina si el mismo se debe clasificar como un incidente de seguridad de la información.

  o Fase 4 Respuesta y comunicación: el objetivo es atender los incidentes e informar a las áreas responsables y de ser necesario a los entes de control.

  o Fase 5 - Erradicación y Recuperación: establece las actividades de erradicación de rastros del incidente e inicia la recuperación a la normalidad de la operación.

  o Fase 6 - Aprendizaje del evento / incidente de seguridad de la información: el analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.

  o Fase 7 - Cierre del evento / incidente: documentación, custodia y archivo del evento /incidente.

- Se debe recolectar la información y soportes del evento/ incidente durante su gestión, de acuerdo con cada una de las fases.

5. DESCRIPCIÓN

5.1. DIAGRAMA DE FLUJO

(Ver anexo)

5.2. ACTIVIDADES

FASE 1: PREVENCIÓN DE EVENTOS E INCIDENTES DE CIBERSEGURIDAD

Coordinador de Infraestructura - Coordinador de Sistemas de Información / Dirección de Tecnología

5.2.1. Desarrollo de controles de acceso lógico en la plataforma tecnológica, como son:

- Firewall Check Point (protección perimetral de red)
- URL Filtering - Aplication Control Check Point (Filtrado Web)
- IPS McAfee (Sistema de prevención de intrusos)
- Controles administrativos(procesos)
- Control de acceso por VPN (usuario autorizados)
- Requerimientos de accesos a Servicios
- Túnel VPN (Control de acceso a terceros sobre redes seguras)
- VLANS (Control de acceso por segmentación de red y ambientes)

5.2.2. Monitorea fuentes de información tales como sitios web, con el propósito de identificar posibles ataques cibernéticos contra la Entidad.

5.2.3. Monitorea lo servicios tecnológicos que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.

5.2.4. Efectúa mantenimiento y actualización de la documentación de la plataforma tecnológica del Instituto.

5.2.5. Gestiona los parches de seguridad, actualizando mínimo una vez al año o cuando los fabricantes de equipos lo recomienden las actualizaciones de seguridad en sistemas operativos, bases de datos, aplicaciones, otros tipos de software utilizados por los equipos del instituto.

5.2.6. Asegura la plataforma, mejora la seguridad de los diferentes equipos informáticos fortaleciendo sus controles con acciones como:

- Configura la menor cantidad de servicios, para lo cual los Lideres de Proceso y la Oficina de Riesgos procuran proveer a los usuarios únicamente los servicios necesarios.
- Revisa la configuración de seguridad de los equipos de acuerdo con las políticas definidas y autorizaciones particulares que puedan presentarse para atender la operación del Instituto.
- Revisa constantemente las reglas de los equipos de seguridad con herramientas como firewall, detectores de intrusos, consolas de antivirus, entre otros.
- Mantiene centralizada la recolección de registros de eventos de los diferentes dispositivos en una consola de monitorización.

Analista Grupo de Riesgos no Financieros / Oficina de Riesgos

5.2.7. Revisa los permisos de acceso lógico en los sistemas de información y herramientas tecnológicas, a través del procedimiento "Gestión de Accesos y retiro de servicios" (A7-1-05).

5.2.8. Realiza revisión semestral de la actualización de usuarios registrados en las bases de datos, con el fin de mantener permisos solamente a aquellos que lo requieren para sus actividades laborales.

5.2.9. Brinda sensibilización, por lo menos una vez al año, al personal del Instituto en materia de seguridad digital, incluyendo las políticas de seguridad digital, riesgos, controles y amenazas cibernéticas. Estas campañas de sensibilización ayudan a reducir los errores o pánico en caso de un incidente de seguridad digital.

5.2.10. Actualiza y divulga las políticas de seguridad digital con frecuencia anual, en las capacitaciones y herramientas de sensibilización.

5.2.11. Identifica y mide en la medida de lo posible los riesgos cibernéticos emergentes que puedan afectar a la Entidad y establecer controles para su mitigación, acción que se realiza en el Monitoreo de riesgos de seguridad digital.

FASE 2: DETECCIÓN Y REPORTE DE EVENTO DE SEGURIDAD

Funcionario - Contratista / Procesos ICETEX

5.2.12. Identifica evento de riesgo de seguridad de la información, situación que puede establecerse a través de:

- Alertas de sistemas de seguimiento en el sistema de detección de intrusos.
- Alertas de sistemas de monitorización de redes.
- Análisis de los registros de los dispositivos como servidores, bases de datos, aplicaciones.
- Revisión del estado de vulnerabilidades de los activos de información.
- Escalamiento de eventos de seguridad realizados por entes externos, como son: CSIRT Gobierno, COLCERT, Centro Cibernético de la Policía u otros organismos del Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
- Escalamiento de eventos anómalos identificados por los administrados de tecnologías.
- Escalamiento de eventos anómalos identificados por la Mesa de Servicios.
- Situaciones irregulares identificadas por los usuarios en el manejo de los activos de información.

5.2.13. Determina tipo de evento de riesgo, de la siguiente manera:

- Los eventos relacionados con la plataforma tecnológica se registran en la aplicación de Mesa de Servicio, pasa a 5.2.15.
- Las demás situaciones relacionadas con irregularidades en el manejo de los activos de información se registran en el aplicativo de Gestión de Riesgos, pasa a 5.2.16

Mesa de Servicios / Dirección de Tecnología

5.2.14. Recepciona evento o incidente y revisa situación.

5.2.15. Determina si se trata de un evento de seguridad de la información, procediendo así:

- De ser evento de riesgo de seguridad de la información, reporta a la Oficina de Riesgos y la Dirección de Tecnología, pasa a 5.2.16.
- En caso contrario, lo tratan de acuerdo con el Procedimiento "Gestión de incidentes" (A7-1-13).

FASE 3 - CATEGORIZACIÓN Y EVALUACIÓN

Analista Grupo de Riesgos no Financieros / Oficina de Riesgos

5.2.16. Analiza la situación presentada mediante indagación a los conocedores del mismo, para determinar si es un evento o un incidente de seguridad de la información y su estado, contemplando los siguientes aspectos:

- Identifica el posible riesgo, causas y controles comprometidos, de acuerdo con la matriz de riesgos de seguridad digital, de no estar relacionado en dicha relación, se incorporará en el monitoreo de riesgos de seguridad.
- Determina los procesos y servicios afectados.
- Establece los activos afectados, en caso de ser necesario se apoya con la Dirección de Tecnología o área responsable.
- Evalúa el nivel de peligrosidad del incidente aplicando la tabla Nivel de Peligrosidad potencial, que es análoga a los criterios aplicados por el COLCERT, de acuerdo con el Anexo No. 2 (cuando aplique).

5.2.17. Define si es un evento o incidente de seguridad de la información.

5.2.18. Categoriza el tipo de evento / incidente, para ello se basa en la Tabla de Categorización de Eventos /Incidentes (Anexo No. 1)

5.2.19. Determina el impacto o grado de afectación de la confidencialidad, integridad y disponibilidad de la información de la Entidad, para ello se apoya en:

- La información o análisis realizado por la Dirección de Tecnología. También revisa los incidentes contra los sistemas de tecnología que soportan las

principales funcionalidades, teniendo en cuenta el instante actual como también en la probabilidad futura de la concurrencia del incidente.
- Las entrevistas e indagaciones realizadas a los usuarios, así como los documentos formales como son procedimientos, manuales, normas, entre otros.

La evaluación del impacto se clasifica así:

Definición	Escala
Efecto insignificante en sistemas o infraestructura crítica de la Entidad La Entidad puede proporcionar servicios críticos a los usuarios	Bajo
Mínimos efectos sobre los sistemas o infraestructura crítico y/o servicios La Entidad puede proporcionar servicios críticos a los usuarios pero ha perdido la eficiencia	Medio
Efecto significativo e inmediato sobre los sistemas o infraestructura crítica y usuarios La Entidad ha perdido la capacidad de proporcionar un servicio crítico o un grupo de usuarios del sistema Compromiso de datos personales de los clientes.	Alto
Graves efectos sobre un gran número de sistemas, usuarios o infraestructura crítica para la Entidad La Entidad no puede prestar u ofrecer algunos servicios considerados críticos a los usuarios Compromiso de datos personales sensibles y de niños, niñas y adolescentes.	Crítico

5.2.20. Determina la criticidad del incidente con el fin de priorizar su atención:

Definición	Escala
Interrumpe seriamente la operación de la Entidad, el incidente puede tener velocidad significativa en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo. **Compromete la integridad y/o confidencialidad de los datos personales**.	Alto
Interrumpe en un periodo corto de tiempo los procesos generales de la Entidad, el incidente compromete un activo crítico.	Medio
Interrumpe un breve periodo de tiempo los procesos generales de la Entidad comprometiendo un activo no crítico.	Bajo

FASE 4: RESPUESTA Y COMUNICACIÓN

Analista Grupo de Riesgos no Financieros / Oficina de Riesgos

5.2.21. Determina áreas que deben ser informadas de la situación.

5.2.22. Documenta la evaluación completa del evento o incidente en F393 Formato de reporte y manejo de evento/incidente de seguridad de la información, en la sección Información a diligenciar por la Oficina de Riesgos.

5.2.23. Determina responsables de responder el evento / incidente de acuerdo con la criticidad y el análisis realizado.

5.2.24. Entrega Formato de reporte y manejo de evento/incidente de seguridad de la información a áreas responsables, indicando si se trata de un evento o un incidente, así como su nivel de criticidad:
- Incidente relacionado con aspectos diferentes a tecnológicos: se remite al área responsable, pasa a 5.2.25.
- Incidente relacionado con aspectos tecnológicos: se remite a la Dirección de Tecnología, pasa a 5.2.26.

Área responsable de atención del incidente

5.2.25. Identifica las acciones de respuesta inmediata, dependiendo si es un evento o incidente, así como si es un hecho que está gestándose o ha culminado. Estas acciones son dirigidas a oportunidades de mejora o contención del incidente, desde aspectos de seguridad física, seguridad tecnológica, mejora de procesos.

5.2.26. Ejecuta las acciones de respuesta inmediata.

5.2.27. Determina si es necesario adelantar acciones adicionales.

- De ser negativo, pasa a actividad 5.2.29.
- De requerirse acciones adicionales para no volver a tener incidentes semejantes a futuro o para mitigar el incidente que se está gestionando, se procede a planear acciones posteriores, pasa a actividad 5.2.28.

5.2.28. Ejecuta las acciones de respuesta adicionales.

5.2.29. Registra las acciones realizadas en el Formato de reporte y manejo de evento/incidente de seguridad de la información, en la sección de Información a diligenciar por el responsable de atención al incidente, pasa a acción 5.2.42

Dirección de Tecnología

5.2.30. Analiza los factores a tener en cuenta para la atención del incidente, como son:

- Daño potencial de recursos a causa del incidente.
- Necesidad de preservación de la evidencia.
- Tiempo y recursos necesarios para poner en práctica la estrategia.
- Efectividad de la estrategia.
- Duración de las medidas a tomar.
- Criticidad de los sistemas afectados.
- Características de los posibles atacantes.
- Si el incidente es de conocimiento público.
- Pérdida económica.
- Posibles implicaciones Legales.

5.2.31. Determina si se trata de un delito informático, procediendo así:

- De ser positivo, asegura la presentación de la evidencia, continuando con la "Guía para el manejo de posible Delito Informático" (G185), pasa a actividad 5.2.32
- De ser negativo, continua con actividad 5.2.32.

5.2.32. Verifica los registros de los dispositivos de seguridad de la información (Correlacionador de Eventos, IDS, Firewall, Consolas, etc), con el fin fe estimar el alcance del incidente, como también verificar si el evento /incidentes está relacionado con cualquier otra situación.

5.2.33. Identifica las acciones de respuesta inmediata, como pueden ser:

- Evita que el incidente se propague a otros activos de información, por ejemplo: aislar el activo afectado de conexiones de red.
- Suspende servicios en el componente afectado.
- Limita el número de usuarios que pueden tener acceso al activo o inclusive apagar el activo de información para evitar impactos mayores. Después del descubrimiento inicial de un incidente, todos los datos volátiles se deberían recolectar antes de apagar el sistema, servicio y/o red de tecnología afectada, para una investigación forense completa de seguridad digital, la información para recolectar incluye los contenidos de memoria, cache y registros y detalle de cualquier actividad que se esté realizando.
- Fortalece los controles de seguridad existentes para reducir el impacto del incidente en curso.
- Aplica soluciones conocidas para el tipo de incidente: descontaminación de virus, ajuste de privilegios de acceso, cambios en reglas de acceso, etc.
- Activa los procedimientos normales de respaldo y de gestión de crisis.
- Hace seguimiento y mantiene en forma segura la evidencia electrónica en caso de que se requiera para un juicio legal o una acción disciplinaria.
- Determina la necesidad de activar el Plan de Recuperación de Desastres, acción a realizar con el Proveedor de servicios tecnológicos.

5.2.34. Aplica solución planteada de respuesta inmediata y se registra en el formato "Formato de reporte y manejo de incidentes de Seguridad de la Información" (F393) de reporte y manejo de evento/incidente de seguridad de la información, en la sección de Acciones inmediatas.

5.2.35. Determina la necesidad de respuestas adicionales, como son:

- Restauración de sistemas, servicios, redes, aplicaciones o información a su estado normal.
- Búsqueda de la solución con fabricantes o bases de conocimiento, ejemplo: aplicación de parches, actualización del sistema, ajustes de configuración, seguimiento y monitorización del sistema durante un periodo posterior al incidente.
- Aviso inmediatamente la situación a los proveedores que apoyan en la atención de los servicios de los activos de información involucrados, para contener la propagación.

5.2.36. Ejecuta acciones de respuesta adicionales.

5.2.37. Si todas las acciones de respuesta inmediata, acciones posteriores o escalamiento no permiten resolver el incidente, se debe activa el plan de recuperación de desastres.

5.2.38. Realiza seguimiento sobre la efectividad de las acciones implementadas, pasa a actividad 5.2.48.

5.2.39. Registra las acciones adelantadas en el formato F393 de reporte y manejo de evento/incidente de seguridad de la información, en la sección de Acciones inmediatas y acciones posteriores. El formato del incidente lo entrega a la Oficina de Riesgos, pasa a actividad 5.2.40.

Analista Grupo de Riesgos No Financieros / Oficina de Riesgos

5.2.40. Informa el incidente de la siguiente manera:

Clasificación por criticidad del evento o incidente	Informar a:	Momento de informe
Evento de riesgo o incidente calificado como bajo	• Área propietaria del activo de información • Oficina de Riesgos • Dirección de Tecnología • Comité de Seguridad de la Información	Una vez ocurra el evento o incidente Al Comité de Seguridad de la Información se informará en la próxima reunión de este comité
Incidente con compromisos de datos personales	• Área propietaria del activo de información • Oficina de Riesgos • Dirección de Tecnología • Comité de Seguridad de la	Aviso inmediato

	Información • Superintendencia de Industria y Comercio	
Ciberataques	• Área propietaria del activo de información • Oficina de Riesgos • Dirección de Tecnología • Comité de Seguridad de la Información • Superintendencia Financiera de Colombia	Aviso inmediato
Fraude	• Área propietaria del activo de información • Oficina de Riesgos • Dirección de Tecnología • Comité de Seguridad de la Información • Secretaria General	Aviso inmediato

5.2.41. Determina si el incidente debe ser informado a los Entes de Control, de acuerdo con las normas vigentes:

- De ser incidente requerido su informe por los Entes de Control continúa con la actividad 5.2.42.
- De no ser necesario su informe a Entes de Control, pasa a 5.2.49.

5.2.42. Reporta a los entes de control, teniendo en cuenta las instrucciones dadas por el Comité de Seguridad de la información, continúa con la actividad 5.2.49

FASE 5: ERRADICACIÓN Y RECUPERACIÓN

Dirección de Tecnología

5.2.43. Revisa si existe rastro del incidente (caso virus informático). De ser negativo, pasa a actividad 5.2.49, en caso contrario, pasa a actividad 5.2.44.

5.2.44. Estima factores a tener en cuenta para la seleccionar la estrategia de erradicación, como son:
- Tiempo y recursos necesarios para poner en práctica la estrategia.
- Efectividad de la Estrategia.
- Posibles implicaciones legales, revisión de este aspecto con la Oficina de Riesgos.
- Relación costo-beneficio de la estrategia.
- Identificación de los procedimientos de cada sistema Operativo comprometido.
- Identificación de Usuarios o servicios comprometidos para proceder a desactivarlos.

5.2.45. Selecciona estrategia de erradicación.

5.2.46. Ejecuta estrategia de erradicación.

5.2.47. Realiza acciones de recuperación, como los siguientes (cuando aplique): 5.2.5.5
- Tomar copias de respaldo y mantenerlas actualizadas de los dispositivos de seguridad de la Entidad.
- Actualiza e instala parches de seguridad a los sistemas que se vieron comprometidos, entre otras definidas en el Plan de Recuperación de desastres de la Entidad.

5.2.48. Registra las acciones adelantadas en el "Formato de reporte y manejo de incidentes de Seguridad de la Información" (F393) de reporte y manejo de evento/incidente de seguridad de la información, en la sección de Acciones inmediatas y acciones posteriores. El formato del incidente lo entrega a la Oficina de Riesgos, pasa a actividad 5.2.49.

FASE 6: APRENDIZAJE DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Coordinación de Riesgos No Financieros - Dirección de Tecnología

5.2.49. Establece las lecciones aprendidas que se identificaron durante el manejo del incidente y así mismo asegura que se actuará más adelante de acuerdo con las conclusiones identificadas. Las lecciones aprendidas pueden incluir aspectos como:

- Necesidades de controles adicionales o mejorarlos para limitar la frecuencia, daño y costo de futuros sucesos.
- Mejoramiento de los contenidos de planes de sensibilización y toma de conciencia.
- Actualización de procedimientos o políticas de seguridad digital.
- Actualización de registro de riesgos o causas de riesgos (amenazas o vulnerabilidades).
- Cambios en el procedimiento de gestión de incidentes.
- Identificación de acciones preventivas para reducir la probabilidad de nuevos incidentes.
- Identificación de áreas o activos de información más vulnerables.
- Identificación de posibles patrones de acción de atacantes informáticos.

5.2.50. Documenta las lecciones aprendidas en el formato F393 de Reporte y manejo de evento/incidente de seguridad de la información, sección Lecciones Aprendidas. Pasa a 5.2.50.

FASE 7 - CIERRE DEL EVENTO / INCIDENTE

Coordinación de Riesgos No Financieros – Oficina de Riesgos

5.2.51. Revisa el completo y correcto diligenciamiento del incidente usando el "Formato de reporte y manejo de incidentes de Seguridad de la Información" (F393) adjuntado los soportes documentales de cada fase desarrollada. En caso de tener vacíos campos del formato F393 o falta de soportes, los complementa y/o obtiene soportes.

5.2.52. Almacena la información recolectada correspondiente al evento /incidente de seguridad de la información en la base de datos en el Aplicativo de Gestión de Riesgos, donde se garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas. Cuando existan documentos físicos se envían al archivo de acuerdo con el procedimiento de Gestión de Archivo.

5.2.53. Retroalimenta a las personas que reportaron el evento de seguridad de la información sobre los resultados después de que el evento o incidente haya sido tratado.

5.2.54. Informa a la Mesa de Servicio la solución el evento/ incidente y sea actualizado en el sistema dispuesto para tal fin (cuando aplique).

5.2.55. Efectúa seguimiento al cumplimiento y cierre de las acciones posteriores que se planearon.

DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CODIGO
Formato de reporte y manejo de incidentes de Seguridad de la Información	F393
Manual Plan de recuperación de desastres	M17
Procedimiento de Administración de archivos de gestión	A8-3-01
Guía para el manejo de posible delito informático	G185
Procedimiento Gestión de accesos y retiro de servicios	A7-1-05
Procedimiento Gestión de incidentes	A7-1-13

Anexo No. 1
Categorización de eventos / incidentes de seguridad digital (ISO27035 y de CoICERT)

Categoría	Descripción Pérdida de seguridad digital causado por	Ejemplos
Desastre natural	Desastres naturales que están fuera del control humano	Terremotos, inundaciones, derrumbes, etc.
Disturbios sociales	Inestabilidad social	Ataque terrorista, guerra, etc.
Daño físico	Acciones físicas accidentales o deliberadas	Incendio, agua, electrostática, ambiente nefasto, robo de equipos, robo de medios, etc.
Fallas de infraestructura	Fallas en los sistemas y servicios básicos que apoyan el funcionamiento de los sistemas de información	Radiación electromagnética, interferencia electrónica, fluctuación de tensión, radicación térmica, etc.
Falla técnica	Fallas en los sistemas de información o en instalaciones no técnicas relacionas, al igual que problemas humanos no intencionales que dan como resultado la no disponibilidad o destrucción de los sistemas de información.	Fallas de hardware, mal funcionamiento de hardware, sobrecarga, etc.
Incidente de malware, Código dañino, Daño de la información Modificación no autorizada	Malware: Programas maliciosos creados o divulgados en forma deliberada. Un programa malicioso se inserta en los sistemas de información para afectar la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistemas operativos. Código dañino, Daño de la información, Modificación no autorizada: Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	Virus informativos, gusanos troyanos, botnet, ataques combinados, páginas web con código maliciosos, sitio hosting con códigos maliciosos, etc.
Ataque técnico, Denegación del servicio.	Ataque técnico: Ataque a sistema de información, a través de redes u otros medios técnicos, ya sea mediante el aprovechamiento de vulnerabilidades de los sistemas de información. Denegación del servicio: Ataques dirigidos a dejar fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.	Escaneo de redes, aprovechamiento de vulnerabilidades, aprovechamiento de puertas traseras, intentos de ingreso, interferencia, denegación de servicio, denegación [Distribuida] del Servicio DoS/DDoS, Fallo (Hardware/Software), Error humano, Sabotaje.
Intrusiones, que corresponde a ataques externos o internos.	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.	Compromiso de cuenta de usuario, Defacement (desfiguración), Cross-SiteScripting (XSS), Cross-Site Request Forgery (CSRF) Falsificación de petición entre sitios cruzados, Inyección SQL, Spear Phishing, Pharming (DNS), Ataque de fuerza bruta, Inyección de archivos Remota, Explotación de vulnerabilidad del software, Explotación de vulnerabilidad de hardware.
Violación de reglas, Política de seguridad digital	• Violación de reglas de forma accidental o deliberada. • Incidentes relacionados por violaciones de usuarios de las políticas de seguridad digital	Uso no autorizado de recursos, violación de derechos de autor, Abuso de privilegios por usuarios, acceso a servicios no autorizados, sistema desactualizado, otros.
Puesta en riesgo de la información	Poner en riesgo en forma accidental o deliberada las funciones de los sistemas de información en cuanto a	Abuso de derechos, denegación de acciones, operaciones equivocadas, interceptación, espionaje, chuzadas de

	seguridad Digital.	teléfonos, divulgación, enmascaramiento, ingeniería social, phishing, robo, perdida, adulteración o modificación de datos, errores en datos, análisis de flujo de datos.
Contenidos peligrosos	Propagación de contenido indeseable a través de redes de información lo que pone en peligro la seguridad nacional, la estabilidad social y/o la seguridad y beneficios públicos.	Contenido ilegal, contenido que provoca pánico, contenido malicioso, contenido abusivo, entre otros.
Obtención de información, puede ser a través de ingeniería social.	Acciones encaminadas a recolectar información de la infraestructura tecnológica con el posible objetivo de preparar ataques informáticos.	Identificación de vulnerabilidades (scanning), Sniffing, Ingeniería social, phishing
Compromiso de la información, Divulgación de información sensible según procedimiento	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Acceso no autorizado a información, modificación y borrado no autorizada de información, Publicación no autorizada de información, Exfiltración de información.
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	Suplantación / Spoofing, Uso de recursos no autorizado, uso ilegítimo de credenciales, Violaciones de derechos de propiedad intelectual o industrial.
Contenido Abusivo, Contempla la categoría de Uso indebido de activos de información, uso Indebido de Software	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Spam (Correo Basura), Acoso / extorsión / mensajes ofensivos, Pederastia / racismo / apología de la violencia / delito, etc.
Otros incidentes	No clasificados en ninguna de las categorías de incidentes anteriores.	Mala gestión del conocimiento, perdida o daño de la documentación y daños sobre activos de información.

Anexo No. 2 Niveles de peligrosidad de ciberincidentes

NIVEL	AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
CRITICO	Ciberespionaje	APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo
MUY ALTO	Interrupción de los Servicios IT / Exfiltración de datos / Compromiso de los servicios	Códigos dañinos confirmados de Alto Impacto RAT, troyanos enviando datos, rootkit, etc.) Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
ALTO	Toma de control de los sistemas/ Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación	Códigos dañinos de Medio Impacto(virus, gusanos, troyanos). Ataques externos– compromiso de servicios no esenciales (DoS/DDoS). Tráfico DNS con dominios relacionados con APTs o campañas de malware. Accesos no autorizados / Suplantación / Sabotaje. Cross-Site Scripting / InyecciónSQL. Spear phising / pharming	Capacidad para exfiltrar información valiosa. Capacidad para tomar el control de ciertos sistemas.

NIVEL	AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
MEDIO	Logro o incremento significativo de capacidades ofensivas/ Desfiguración de páginas web / Manipulación de información	Descargas de archivos sospechosos. Contactos con dominios o direcciones IP sospechosas. Escáneres de vulnerabilidades. Códigos dañinos de Bajo Impacto (adware, spyware, etc.) Sniffing / Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de algún sistema.
BAJO	Ataques a la imagen / menos precio / Errores y fallos	Incumplimiento de Políticas. Spam sin adjuntos. Software desactualizado. Acoso / coacción/ comentarios ofensivos. Error humano/ Fallo Hardware o Software.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.

Modificaciones

Descripción de cambios

Se modifica el objetivo, el alcance, se eliminan las definiciones activo, análisis de riesgo, auditoría, control y CCOC, las definiciones de CCP, ColCERT, CSIRT, CSIRT PONAL, se trasladan a las condiciones generales en las terceras partes especializadas en caso de necesitar apoyo.

Las condiciones generales se redactan nuevamente.

Se redefinen las actividades del procedimiento

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2020-1-27	2	Se modifica el objetivo, el alcance, se eliminan las definiciones activo, análisis de riesgo, auditoría, control y CCOC, las definiciones de CCP, ColCERT, CSIRT, CSIRT PONAL, se trasladan a las condiciones generales en las terceras partes especializadas en caso de necesitar apoyo. Las condiciones generales se redactan nuevamente. Se redefinen las actividades del procedimiento
2017-12-19	1	-