PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

VERSIÓN 1

EN PROCESO DE APROBACIÓN

SUBDIRECCION DE GESTIÓN Y MANEJO
GRUPO DE SISTEMAS DE INFORMACIÓN Y RADIOCOMUNICACIONES

2018

Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3110
www.parquesnacionales.gov.co

1. CONTROL DE REVISIÓN

SGC	PROCESO DE GESTIÓN DE INFORMACIÓN	Versión 1
03/25/2016	Página 1 de 31	**Confidencial**
05/04/2018		**En proceso aprobación**
La información contenida en este documento es propiedad intelectual de PNN		

El documento comprende Un (1) ejemplar, para la Dirección Central Parques Nacionales Naturales de Colombia, los cuales serán firmados por Parques Nacionales Naturales de Colombia en señal de aceptación de los términos y condiciones descritos en este documento.

2. GENERALIDADES

2.1. Introducción

Los constantes avances en el uso de las tecnologías de la información y las comunicaciones han llevado a las empresas a prepararse para afrontar los riesgos de seguridad a los que puede estar expuesta su información, toda vez que es uno de los activos que ha tomado mayor relevancia en las empresas, lo cual conlleva a implementar controles y acciones que ayuden asegurarla como una forma de anticiparse a los riesgos o eventos que la afecten.

En la mayoría de los casos el impacto de estos riesgos se ve reflejado en la confidencialidad como por ejemplo robo de información clasificada como secreto industrial, la integridad, la cual está relacionada con alteración de información de estados financieros y disponibilidad teniendo en cuenta que puede causar que los servicios tecnológicos o de información de las entidades no esté disponible, lo cual pude causar pérdidas económicas, de relaciones de confianza por los clientes que conllevarían también a la pérdida de imagen o

buen nombre de las empresas ante sus grupos de interés. Riesgos que de no tomarse acciones correctivas definidas pueden llegar a repetirse.

La gestión de incidentes de seguridad de la información es una de esas acciones (controles tecnológicos, capacitaciones, análisis de riesgos, entre otros) que se deben implementar para asegurar y proteger la información de las empresas o entidades, a través de este documento se presentará un modelo de gestión de incidentes de seguridad que pueden implementar aquellas empresas o entidades que estén en la tarea de implementar su Sistemas de Gestión de Seguridad de la Información.

Estudios previos como el realizado por Welivesecurity patrocinado por ESET y publicado en mayo de 2016 han mostrado que el 97% de los incidentes de seguridad se hubieran podido evitar si las entidades implementaran acciones, como controles, capacitaciones a sus empleados en temas de seguridad, entre otros, para proteger su información, incluyendo un modelo de gestión de seguridad de la información. Este estudio es el resultado de 8 años de seguimiento a más de 2000 brechas de seguridad que se realizaron desde el 2002, donde más de mil millones de registros fueron comprometidos.

2.1.1. ¿Que se protege con un Csirt?

Un equipo de respuesta debe de tener como objetivo proteger infraestructuras críticas de la información, en base al segmento de servicio al que esté destinado así deberá de ser su alcance para cubrir requerimientos de protección sobre los servicios que brinda. El CSIRT debe de brindar servicios de seguridad a las infraestructuras críticas de su segmento básicamente.

Las infraestructuras críticas en un país están distribuidas en grandes sectores, los cuales pueden ser:

- Agricultura
- Energía
- Transporte
- Medio Ambiente
- Industrias
- Telecomunicaciones
- Banca / Finanzas
- Gobierno
- Entre Otros

2.1.2. Objetivo General

Definir un modelo de gestión de incidentes de seguridad de la información que permita a Parques Nacionales Naturales de Colombia detectar, reportar, contener y recuperarse de un evento no controlado.

2.1.2.1. Objetivos Específicos

- Identificar y clasificar eventos que pueden llegar a considerarse como incidentes de seguridad de la información.
- Definir un Modelo guía para gestión de los incidentes de seguridad de la información en la Entidad.
- Fortalecer la capacidad del Área de TI en cabeza del grupo GSIR, para gestionar incidentes de seguridad con el fin de que los eventos no se repitan o minimizar su impacto.
- Generar un indicador de medición en la socialización del modelo de gestión de incidentes de seguridad de la información.

3. GESTION DE INCIDENTES

En el campo de la tecnología y la informática todos los eventos que atenten contra la normal operación de la infraestructura o la información, deben entenderse como un incidente y como tal deben gestionarse para encontrar su origen, posibles consecuencias y las soluciones que estos pueden acarrear para la Entidad.

Sin embargo, es preciso aclarar que en los incidentes de infraestructura y los de información deben tratarse por separado, sin llegar al punto que no se puedan relacionarse entre sí. Es decir, que un incidente de infraestructura (operacional) no pueda conllevar a generar un incidente de seguridad de la información porque algunos incidentes de seguridad de la información han sido y pueden ser producto de una falla operacional.

Un ejemplo de un incidente operacional o de infraestructura podría ser el que una persona no pueda ingresar a su estación de trabajo porque olvido la clave o porque su equipo esta desconectado de la red y otra cosa es que una persona vaya a acceder a una información de la empresa y no pueda hacerlo porque la misma ha sido borrada o tiene cambios.

Para claridad de la relación entre las dos clases de incidentes, se puede mencionar que los usuarios no pueden acceder a la información almacenada en el servidor porque el mismo ha llegado a la capacidad límite de procesamiento de peticiones.

Para tal fin es imprescindible que la Entidad defina políticas de seguridad y entre ellas políticas de backup, que deben especificar qué información es la que debe ser salvaguardada y en que sitio, la periodicidad, el tipo de backup, si incremental, total o parcial.

De igual forma, la Entidad debe pensar en el diseño de su centro de cómputo y si requiere o no un Centro de Cómputo Alterno (CCA), que respalde la infraestructura identificada como crítica.

Así las cosas, las acciones que se deben tener en cuenta para atender un incidente operacional son las que se mencionan a continuación:

- El usuario afectado informe a la mesa de ayuda o a quien haga sus veces el inconveniente o falla que se le presenta.
- La mesa de ayuda valora el incidente y en caso de que los técnicos de la misma puedan resolver la falla, ésta quedará resuelta y cerrada según el caso, de lo contrario, se elevará la petición a nivel funcional o técnico de segundo nivel.
- En el evento que no pueda resolverse en ninguna de las instancias anteriores, el caso sería elevado al nivel de soporte de proveedor del servicio para la compañía en caso de que lo hubiere.

Para el caso de los incidentes de seguridad de la información las etapas macro que deben tenerse en cuenta para su gestión son las que se enuncian a continuación:

- Etapa 1. Planeación y Preparación
- Etapa 2. Detección y Reporte del Incidente
- Etapa 3. Evaluación y Decisión
- Etapa 4. Respuesta
- Etapa 5. Lecciones Aprendidas

Los Sistemas de Gestión de Seguridad de la Información y las mejores prácticas que sobre esta materia se pueden consultar, evocan que las acciones para salvaguardar la información de la entidad, primero deben tener un proceso previo de identificación y análisis de riesgos, esto conlleva a la necesidad de revisar otros conceptos que en se seguridad de la información deben ser aclarados.

En este sentido, el primero de los conceptos que deben quedar claro es el de Amenaza, que se define como la posibilidad de que suceda un evento de tipo natural o humano, ya sea provocado por acción u omisión y que puede causar daño a cualquiera de los sistemas o infraestructura tecnológica.

Dentro de las amenazas de tipo humano se pueden encontrar (fraude por computador, piratas informáticos, phishing, funcionarios insatisfechos, terroristas, competidores de la industria, crimen organizado, entre otros). En las amenazas de tipo natural se encuentran (tormentas eléctricas, terremotos, inundaciones, incendios no provocados).

El siguiente concepto a revisar es vulnerabilidad, que se refiere a las características que condicionan la ocurrencia de las amenazas, es decir, capacidades de los sistemas, infraestructura tecnológica o de las personas que pueden ser aprovechadas por las amenazas. Las vulnerabilidades pueden ser catalogadas de tipo físico, social o económico entre otras.

El impacto es la medición del daño causado por la presencia de una amenaza a un sistema, infraestructura tecnológica o la información misma de la Entidad, por ejemplo, se mencionan las pérdidas financieras, sanciones legales o daño en la imagen corporativa.

Finalmente, el riesgo se define como la probabilidad que ocurra un hecho no controlado, que afecte la normal operación de la entidad o el logro de los objetivos y metas de la organización.

Por lo expresado con anterioridad, se analizarán y modelarán las actividades para la gestión de los incidentes de seguridad de la información, las cuales serán desarrollas al largo de este documento.

3.1. ETAPA 1. PLANEACIÓN Y PREPARACIÓN

En el proceso de planeación y preparación para implementar el modelo de gestión de seguridad de la información se deben considerar los siguientes aspectos:

3.1.1. REVISIÓN, ACTUALIZACIÓN O DEFINICIÓN DE LAS POLTIICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD

En el proceso de definición de un plan de seguridad de la información se debe iniciar con unas generalidades, un alcance, unos objetivos, unos responsables, la identificación de los activos, las áreas a cubrir o proteger con el plan, los riesgos a los que puede estar expuesta la información y los controles que deberán ser implementados y cuáles no lo serán, todo lo anterior recibe el nombre de Política de Seguridad de la Información, dentro de la cual se encuentra la política de gestión de incidentes de seguridad de la información, “Esta Política de Gestión de Incidentes de Seguridad de la Información se integrará a la normativa básica del Organismo, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de la presente política.

Es primordial que, si no se ha definido una política, ésta se establezca como argumento fundamental para la gestión de incidentes, porque la política se convierte en el punto de partida de toda la gestión de seguridad que se haga sobre la información de las empresas.

En el caso de existir una política, se debe hacer un análisis profundo de la misma para evaluar si es necesario hacer una actualización teniendo en cuenta puntos como, por ejemplo, número desbordado de eventos no controlados, evaluación de controles que no sean operativos y sostenibles en el tiempo, desconocimiento de los funcionarios por falta de divulgación sobre las políticas de seguridad definidas.

3.1.2. ESCALA DE CLASIFICACIÓN DE LOS INCIDENTES

Antes de hablar de la escala de clasificación de los incidentes es importante tener claro la diferencia entre un evento y un incidente de seguridad, de acuerdo con la Norma ISO/IEC27035, expresa un evento de seguridad como “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”[1].

Y un incidente, es “Un evento o una serie de eventos inesperados e indeseados, que van contra la seguridad de la información. Tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la confidencialidad, integridad y disponibilidad la información.

Teniendo claro lo anterior, y conociendo que en términos de seguridad se manejan los conceptos de probabilidad e impacto es válido considerar la siguiente fórmula para ayudar a definir la clasificación de los incidentes de seguridad de la información.

Impacto Negativo Producido por el Incidente	**+**	**Criticidad de los Recursos Informáticos Afectados**	**=**	**Criticidad del Incidente**

Donde el “impacto negativo producido por el incidente” está dado por el grado de afectación que el incidente pueda producir para entidad en caso de presentarse; la “criticada de los recursos informáticos afectados” basada en los activos de información e infraestructura tecnológica que es de vital importancia para la operación de la entidad y que entre otras cosas debe permitir o definir una valoración cuantitativa de pérdidas para la organización.

De lo anterior, y acorde con la formula plateada, se puede definir una tabla de clasificación según su criticidad.

[1] GTC-ISO/IEC 27035 Tecnología de la Información. Técnicas de Seguridad. Gestión de Incidentes de Seguridad de la Información. 2012. P. 10

SERVERIDAD	DESCRIPCIÓN
ALTA	Amenaza la integridad y la vida de las personas Afecta el buen nombre de la entidad Afecta las relaciones o negociaciones con grupos de interés Afecta la estabilidad financiera de la entidad Afecta la información de índole personal Pérdida o robo de información catalogado como secreto comercial o industrial Afecta la infraestructura critica para los procesos de la entidad Genera incumplimiento de normas legales
MEDIA	Compromete medianamente el buen nombre de la entidad Afecta medianamente a las personas Impacta un número moderado de sistemas o personas
BAJA	no afecta la integridad o la vida de las personas impacta un número mínimo de equipos no críticos

3.1.3. MATRIZ RACI

La matriz RACI es de vital importancia toda vez que allí se definen o mapean los roles y las responsabilidades de quienes deben participar en los esquemas de seguridad de la información, así como su intervención en cada una de las actividades con motivo de conocer quién toma parte en cada actividad y con qué nivel de participación. En este mapeo la RACI cada letra que forma su nombre es una responsabilidad específica en la actividad por parte de los involucrados.

A continuación, se muestra la nomenclatura a utilizar dentro de la tabla RACI definida para el Modelo de Gestión de Incidentes de Seguridad de la Información para la Entidad.

	RESPONSABILIDAD	DESCRIPCIÓN
R	Responsible	Responsable de ejecutar la actividad
A	Accountable	Encargado del Cumplimiento y la calidad en la ejecución dela actividad
C	Consulted	Aporta conocimiento y/o información para que el responsable ejecute la actividad
I	Informed	Rol que debe ser informado una vez que la actividad ha finalizado

De acuerdo con lo anterior, la Matriz RACI estaría representada de las siguiente Manera:

- Actividad: Nombre de la actividad
- Roles: Nombre de los roles participantes en el lineamiento de Administración de Incidentes, y de Administración de Servicios, Implementados en el Área de Tecnología.

Funciones/Áreas	Dirección General	Subdirección Gestión y Manejo de Áreas protegidas	Subdirección Sostenibilidad y Negocios Ambientales	Subdirección Administrativa y Financiera	Direcciones Territoriales	usuarios/Clientes
Practicas Claves de gestión						
Brecha potencial de seguridad identificada		I/A			I/C	
reportar incidente de seguridad	R	R/I	R	R	R	R
investigar incidente de seguridad		A	C	I	C	C
informar resultado del incidente de seguridad		I/A/C			C	
impacto del incidente		I/A	C	C	C	
definir plan de accion de mejora		I/A/R	C	C	C	
monitorear las acciones implementadas		C/A/I			R	
lecciones aprendidas		I/A/C	I	I	I	

3.1.4. DEFINICION DE LOS FORMATOS

Para lograr una correcta gestión de los incidentes de seguridad de la información en la entidad es imperativo que se definan y oficialicen unos formatos donde se pueda realizar los siguientes registros:

- Formato 1: Reporte de Incidentes (Ver Anexo 1)
- Formato 2: Valoración del Incidente (Ver Anexo 2)
- Formato 3: Informe Resultado de Incidentes (Ver Anexo 3)

Lo anterior, con el fin de llevar un registro pormenorizado de cada uno de los incidentes de seguridad de la información que se presenten.

3.1.5. PROCEDIMIENTO PARA EL USO DE FORMATOS

Una vez se hayan establecidos los formatos, se debe elaborar un procedimiento donde se especifique a los funcionarios o colaboradores de la entidad el orden de uso de los mismos.

Formato 1: Reporte de Incidentes: Todo análisis de incidentes inicia con la detección y el reporte, para lo cual el formato a ser diligenciado por los funcionarios y colaboradores de la entidad es el de reporte de incidente para dar a conocer al área correspondiente la existencia de un incidente de seguridad de la información.

En este formato se diligencia información relacionada con datos básicos de las personas que está reportando el hecho, como, por ejemplo, Nombre, Cargo, Correo electrónico, No. de teléfono o extensión, entre otros. También se registra información como la fecha y hora del incidente, descripción del incidente, activo de información afectado por el incidente y lugar de los hechos.

Formato 2: Valoración de Incidentes: Registrado el incidente, se procede con la valoración del mismo, es decir, se evalúa o determina el grado de impacto negativo producido por el incidente y la criticidad del recurso o activo de información afectado, esto con el fin de determinar la criticidad del incidente.

Para ello en el formato de valoración se registra la información relacionada con el reporte, entre los que se encuentra la fecha del reporte, no. de solicitud (para hacer el seguimiento) y una breve descripción del incidente, de igual manera se registran datos relacionados con la fecha de valoración del incidente, nombre de la persona o profesional que valora, la valoración dada al incidente y si es del caso una observación relacionada con la valoración.

Formato 3: Resultado de Incidentes: Después de valorado y analizado el incidente es necesario realizar una investigación que permita determinar la causa raíz del mismo, este proceso es realizado por un equipo de personas definidas previamente que son las encargadas de recolectar toda la información relacionada con el incidente y se registra en este formato, además de consignar información de cuales fueron los pasos surtidos en la investigación, que oportunidades de mejora se pueden recomendar, las conclusiones de la investigación y los anexos recopilados por el equipo investigador.

3.2. ETAPA 2. DETECCIÓN Y REPORTE DEL INCIDENTE

Para la detección y reporte de incidentes es acertado definir los procedimientos que todos los colaboradores de la entidad están en la responsabilidad de conocer y aplicar según sea el caso.

3.2.1. DETECCIÓN Y REPORTE DE INCIDENTES

3.2.1.1. Qué se puede considerar un incidente de seguridad

Se considera un incidente de seguridad:

- Incumplimiento de alguno de los lineamientos definidos explícita o implícitamente en la política de seguridad de la información de la Entidad.
- Ejecución de Código Malicioso
- Ataque de virus contra la infraestructura informática
- Uso no autorizado de cuentas de acceso a los sistemas de información
- Fuga de información por cualquier medio
- Uso o acceso no autorizado de privilegios del sistema
- Uso inapropiado de recursos informáticos
- Robo o pérdida de información de carácter confidencial o reservado
- Alteración o modificación de un sitio web de la entidad

Estos incidentes de seguridad de seguridad de la información pueden estar catalogados con su tipo, como se muestra en la siguiente tabla:

TIPOS DE INCIDENTES				
Denegación de Servicio	**Código Malicioso**	**Acceso no Autorizado**	**Uso indebido de recursos**	**Análisis de Vulnerabilidades**
Tiempo de respuesta fuera del conocido **Interrupción de servicios tecnológicos no operacionales**	Virus informático Ramsomware malware	fuga de información borrado de información modificación de información intentos reiterativos de acceso a los recursos captura de información confidencial	uso de recursos para envió de spam promocionar contenido pornográfico violación a las políticas de seguridad y normas de internet	configuraciones por defecto puertas traseras fallas en actualización de software trafico inusual en la red penetración de sistemas

A continuación, se presentará una descripción de cada una de las clasificaciones de los incidentes.

Denegación de Servicio: La denegación de servicio (siglas en inglés: DoS) y denegación de servicio distribuida (siglas en inglés: DDoS) son una amplia categoría de incidentes con un denominador común. Estos incidentes hacen que un sistema, servicio o red dejen de operar a su capacidad prevista y con mucha frecuencia deja sin acceso a usuarios legítimos del sistema o servicio tecnológico afectado. Existen dos tipos de incidentes DoS/DDoS causados por medios técnicos: eliminación y agotamiento de recursos.

Como ejemplo de este incidente se puede mencionar el envío masivo de paquetes a través de le red para llenar el ancho de banda con tráfico de respuesta.

Los incidentes por denegación de servicio (DoS) son aquellos causados porque el número de peticiones lanzado desde un equipo cliente a un servidor excede el límite permitido y eso causa que el servidor afectado deje de estar disponible.

Entre tanto los incidentes generados por denegación de servicios distribuido (DDoS), son similares al DoS con la diferencia que las peticiones vienen de varios equipos haciendo peticiones a un mismo servidor.

Código Malicioso: Identifican un programa o parte de éste insertado en otro programa con la intención de modificar su comportamiento original, usualmente para realizar actividades maliciosas como robo de información y de identidad, alteración o destrucción de la información y los recursos.

Actualmente los códigos maliciosos se usan para realizar ataques dirigidos. Esto se hace algunas veces modificando un código malicioso existente, creando una variante que muchas veces no reconocen las tecnologías para detección de códigos maliciosos.

Estos códigos maliciosos pueden estar dados por virus, ransomware o gusanos, entre otros.

Un ransomware está definido como un software que al momento de instalarse en el equipo víctima, permite que éste sea bloqueado por quien está generando el ataque, a tal punto que el usuario real de equipo perdería todo control sobre el mismo.

Acceso no Autorizado: Consiste en intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red. Un ejemplo de este tipo de incidentes es acceso a la información por ataque de fuerza bruta.

3.2.1.2. Como reportar un Incidente

En el caso que un funcionario, temporal o tercero contratista considere o identifique que se está presentando un incidente de seguridad debe proceder a su reporte a la mesa de servicio o quien la entidad delegue para este fin a través de los siguientes medios o canales:

Enviando correo electrónico a la mesa de ayuda o a quien se delegue para la recepción de estas solicitudes con la siguiente información como mínimo:

- Nombre de quien reporta
- Cargo de quien reporta
- Teléfono o E-mail
- Fecha del reporte
- Fecha del incidente
- Equipo o sistema afectado
- Descripción del incidente

Si la entidad dispone de una intranet, se debe hacer uso del formato para registro de reporte definido para web. (Ver anexo 1)

En caso de que la entidad, disponga de una línea (extensión telefónica) de atención de requerimientos, lo colaboradores de la misma deben comunicarse a través de esta línea donde un operador o agente de mesa de servicio le recibirá la comunicación y registrará información adicional de ser necesario.

3.2.2. RECOLECCIÓN Y CONSERVACIÓN DE INFORMACIÓN

3.2.2.1. Recolección de información

En esta etapa se debe recopilar información relacionada con:

- Alcance del Incidente
- Que activos de información fueron afectados
- Qué o cómo se originó el incidente
- Impacto en las actividades o en la operación dela entidad

Para el proceso de recolección y retención de información y/o evidencias que puedan ser utilizadas como parte de la investigación para hallar la causa del evento y/o incidente de seguridad se debe realizar siguiendo los lineamientos y las buenas prácticas de la custodia de evidencias digitales (Técnicas Forenses), tomando como marco general la legislación colombiana, en tal sentido se deberán desarrollar las siguientes actividades como parte de la recolección de esta información.

- La Captura de la información será realizada por la coordinación de seguridad de la información o quien delegue para esta función, con la colaboración del administrador de los servicios de red y demás involucrados en el proceso.

  Esta información o evidencia podría hacer parte de una investigación judicial en caso de que se llegar a configurarse un delito informático, por lo cual las acciones ejecutadas para recolectar la información se deben hacer bajo las estrictas medidas de seguridad para evitar que la información o evidencia sufra algún tipo de alteración y pueda perder su validez legal.

  En término legales, un delito informático se define como un acto ilícito, es decir fuera de la ley, perpetrado para recopilar, destruir, alterar información o cualquier sistema de información con el ánimo de obtener usufructo o por generar daño.
- En la medida de lo posible al realizar la captura de la información y/o evidencia se debe hacer con el uso de herramientas que no modifiquen ni el entorno ni la prueba en sí, salvaguardando su integridad.
- En la recolección de la información y/o evidencias se deben tener en cuenta aspectos como:
  - *Información del host*: es aquella información que se puede recopilar como por ejemplo fecha y hora del sistema, identificación de aplicaciones en ejecución, puertos abiertos, ultimas copias de respaldo realizada e historial de archivos copiados, entre otros.

- *Información de red*: información relacionada con los logs de monitoreo, servidores de autenticación y logs de firewall, entre otros.
- *Información de Personas*: obedece a la información que se pueda recopilar de las personas que conocieron o identificaron el evento o incidente.
- *Información Adicional*: cualquier información que pueda estar directa o indirectamente relacionada con el incidente y que pueda ayudar a resolverlo.

En el caso que hechos resultantes de seguimiento del incidente impliquen acciones de acuerdo con lo establecido por la Ley, o las disposiciones definidas por la empresa o entidad, estas serán determinadas por el área de la entidad que tenga esta competencia.

3.2.2.2. Conservación de información

Una vez se ha hecho la recopilación de la información y/o evidencias del incidente se deben aplicar los conceptos de:

a) *Autenticidad*: Es el proceso de demostrar que la información y/o evidencia recopilada no ha sufrido ningún tipo de cambio el proceso de recolección, es decir, que la información es original u autentica.
b) *Cadena de Custodia*: Se debe llevar un registro detallado del tratamiento que ha sufrido la información y/o evidencia recolectada.

   Este tema vale la pena precisar, que se debe tener en cuenta lo dispuesto en el Manual de Procedimientos para Cadena de Custodia, definido por la Fiscalía General de la Nación de la República de Colombia, toda vez que desde los términos jurídicos y para que la evidencia recopilada sea válida para adelantar un proceso judicial en contra de algún colaborador o contratista se debe comprobar que la información no ha sufrido ningún tipo de cambio desde su captura hasta el momento de entregarlo al ente jurídico correspondiente.
c) *Validación*: En caso de requerirse se debe demostrar que la información que se entrega sea la misma recolectada.

3.3. ETAPA 3. EVALUACIÓN Y DECISIÓN

3.3.1. Evaluación de los Incidentes de Seguridad de la Información

El área de Tecnología de la Información (TI) o de Seguridad de la Información o quien se designe para el registro de los eventos o incidentes de seguridad que sean reportados por los por lo colaboradores o empleados de la empresa, debe:

- Informar a la persona que reporta que la solicitud ha sido recibida y se le dará el trámite correspondiente.
- Registrar el incidente en el sistema o base de datos destinado para este fin y generar un número para identificar el reporte.
- Buscar una aclaración o ampliación del incidente por parte de la persona que lo reporta o registrar información adicional de otras personas que hayan podido conocer del incidente.
- Evaluar si se cataloga como incidente de seguridad, o si es un incidente de tipo operativo y hacer el escalamiento correspondiente del mismo.
- Reportar el equipo de respuesta CSIRT si el evento fue catalogado como incidente de seguridad de la información.

Por otra parte, adicionalmente después de registrar la fecha y la hora de lo sucedido, también debe complementar el registro del evento con la siguiente información:

- Que se observó y que se realizó (mencionar si utilizó alguna herramienta).
- Ubicación exacta de posibles evidencias del evento.
- Describir como se recolecto la evidencia inicial del evento.
- Detallar si se tuvo algún tipo de custodia o almacenamiento de la evidencia inicial.

3.3.2. Declaración del Incidente

La responsabilidad de si un evento se declara como incidente de seguridad de la información debe ser del equipo de respuesta una vez le sea notificada la identificación y reporte del evento por parte del punto de contacto que se haya definido por el área de TI, de Seguridad de la Información o quien se designe.

Para ello el profesional o persona del CSIRT que le sea escalado o informado el evento debe:

- Confirmar el recibo del reporte de incidente con la mayor información que haya sido recopilada por el punto de contacto.
- Validar si el evento se encuentra en el sistema o base de datos de registro de eventos o incidentes de seguridad y registrarlo en caso que el punto de contacto no lo haya hecho.
- Tener aclaraciones del evento o incidente con el punto de contacto de ser necesario.
- Validar y analizar el contenido del reporte enviado por el punto de contacto.
- Revisar si es posible recolectar información adicional del evento o incidente con personas que puedan estar relacionada o que hayan conocido de la situación.

Si se determina que el evento es un incidente de seguridad de la información, los miembros del equipo de respuesta CSIRT deben llevar a cabo una evaluación posterior donde se defina:

- En que consiste el incidente.
- Cómo, qué o quién lo originó.
- Que puede afectar.
- Determinar el impacto real de negocio para la empresa o entidad.
- Si el impacto es severo, se debe declarar la alerta de crisis.
- Identificar el activo o sistema o información que haya sido vulnerado o modificado.
- Efectos secundarios que pueda dejar el incidente, por acceso físicos no asegurados, brechas en el sistema de información.
- Validar y monitorear las actividades que hasta ese momento de hayan realizado con el incidente.

3.4. ETAPA 4. RESPUESTA

3.4.1. Detectar, Responder, Resolver y Recuperarse de un Incidente

En lo relacionado con los incidentes de seguridad de la información generalmente son generados por personal que no ha seguido o aplicado los procedimientos de TI definidos en la entidad, sin embargo, también existen situaciones donde los eventos o incidentes son provocados por agentes externos a la entidad.

Por esta razón es que se debe definir un procedimiento que permita a la entidad detectar, resolver, atender y recuperarse de los eventos que puedan generar una pérdida en la operación de su negocio.

3.4.2. Detectar un Incidente

La primera parte en un esquema de gestión de incidentes de seguridad de la información tiene que ver con la detección u ocurrencia de evento de seguridad y toda la información relacionada con el mismo.

Como parte de las actividades que se deben tener en cuenta para detectar un incidente por parte del personal o terceros o de manera automática son las siguientes:

- Monitorización de alertas generadas por herramientas como IDS/IPS, programas de antivirus, sistemas de seguimiento de registros.
- Alertas generadas por sistemas Data Loss Prevention (DLP).
- Alarmas por bloqueo reiterado de cuentas de usuario.
- Alertas de seguimiento y monitoreo a sistemas de red, Firewalls, análisis de flujo de redes y filtrado de contenidos, entre otros.
- Análisis de información con el registro de dispositivos, equipos, servicios y otros sistemas.
- Reportes de usuarios
- Notificaciones hechas por terceras persona o externas como por ejemplo CSIRT, servicios de seguridad de la información, PSI, proveedores de servicios de telecomunicaciones.

Eventos que deben ser monitoreados y que llegan a ser considerados causas de incidentes de seguridad de la información:

- Incumplimiento de alguno de los lineamientos definidos explícita o implícitamente en la política de seguridad de la información de la empresa o entidad.
- Ejecución de código malicioso.
- Robo de contraseñas.
- Ataque de virus contra la infraestructura informática.
- Uso no autorizado de cuentas de acceso a los sistemas de información
- Fuga de información por cualquier medio
- Uso o acceso no autorizado de privilegios del sistema.
- Uso inapropiado de recursos informáticos.
- Robo o pérdida de información de carácter confidencial o reservada.
- Alteración o modificación de un sitio de web de la empresa o entidad

Los eventos de seguridad de la información pueden ser detectados directamente por personas que observen algo inusual y que le causa preocupación, ya sea que tenga relación con aspectos técnicos, físicos o procedimentales. La detección puede ser, por ejemplo, de detectores de fuego/humo, o alarmas para intrusos (ladrones) con alertas que notifican en lugares designados previamente para acción humana.

Estos eventos en primera instancia pueden ser detectados por:

- Usuarios.
- Gerentes de línea o de seguridad.
- Clientes.
- Departamento de TI, centro de monitoreo de redes, o de operaciones de seguridad.
- Mesa de ayuda de TI, de acuerdo con los reportes que pueda recibir.
- Proveedores de servicio.
- CSIRT
- Personas que pueden detectar anomalías durante las ejecuciones diarias de su trabajo.

3.4.3. Responder un Incidente

Para responder de forma eficaz a los incidentes se tiene que llevar acabo lo siguiente:

- La comunicación de puntos débiles y eventos en la seguridad de la información, con la finalidad de asegurar que se realizan correctamente las acciones correctivas oportunas para hacer frente a posibles incidentes
- Mediante el empleo de los medios adecuados de gestión, es necesaria la comunicación de la evolución y control de sucesos de seguridad de información para contrarrestar la aparición de incidentes o amenazas en la información.
- La gestión de incidentes de seguridad de la información y mejora continua, con el objetivo de asegurar la aplicación para gestionar los posibles incidentes.
- Se debe proceder con la asignación de responsabilidades y procesos de gestión para asegurar una respuesta veloz, estructurada y eficaz para hacer frente a los incidentes de la seguridad de la información.
- Estudio y análisis de los incidentes de seguridad de la información mediante dispositivos adecuados para la inspección de tipos, volúmenes, impactos o costos.
- Es necesaria la colección o recopilación de evidencias cuando comienza una actuación contra una persona u organismo, posterior a un incidente de seguridad de la información, de acuerdo con las normas de la jurisdicción aplicables.
- Asignar recursos internos e identificar recursos externos para responder a un incidente.
- Escalamiento de eventos anómalos detectados por el área de TI a los niveles superiores.
- Escalamiento de eventos anómalos detectados por la mesa de ayuda, a un nivel superior.
- Validar técnicamente la posibilidad de interrumpir o clausurar rápidamente y en forma confiable el sistema, servicio y/o red de información atacada, con el fin de contener el incidente.

3.4.4. Resolver un Incidente

Para resolver los incidentes de seguridad se debe analizar la prioridad de los mismos, es decir, validar el impacto que puede ocasionar en la organización como, por ejemplo:

- Aquellos que atenten contra el recurso más importante de toda organización como lo son las personas.
- Atender aquellos incidentes que amenacen la integridad de la información sensible de la entidad.
- Concentrarse en los incidentes que atenten contra la integridad de otro tipo de información de importancia para la entidad.
- Resolver los incidentes que pueden afectar los sistemas de información de la organización.
- Atender los incidentes que causan interrupción o caídas en los servicios dispuestos por la entidad para sus usuarios.

3.4.5. Recuperarse del Incidente

Una vez se haya recolectado y analizado la información, se haya identificado la causa de incidentes y se hayan tomado acciones para su contención, el equipo de respuesta a incidentes debe surtir actividades como:

- Identificar todos los archivos pertinentes en el sistema, servicio y/o red, incluidos archivos normales, archivos con contraseña o protegidos de otra manera, y archivos encriptados.
- Recuperar tanto como sea posible los archivos eliminados descubiertos, y otros datos.
- Examinar la integridad de los archivos para detectar archivos con Troyanos y archivos que no estaban originalmente en el sistema
- Determinar la actividad de los usuarios y/o aplicaciones en un sistema/servicio/red.
- Extraer el contenido de archivos ocultos, temporales e intercambiados usados tanto por las aplicaciones como por el software del sistema operativo.
- Identificar el personal que deba participar en la recuperación del sistema o dispositivo afectado, por ejemplo, administradores de red, base de datos, sistema operativo, sistemas de información.
- Estimar los tiempos de recuperación, acorde con el incidente presentado y con los tiempos establecidos.
- Activar planes de recuperación y procesos de recuperación de ser necesario

3.5. ETAPA 5. LECCIONES APRENDIDAS

En un esquema de gestión de incidentes de seguridad de la información cuando estos han sido atendidos, solucionados y cerrados, e involucra el aprendizaje de conocimiento o la manera de cómo fueron manejados o tratados estos incidentes, se debería tener en cuenta una serie de actividades que permiten definir lecciones aprendidas involucradas con los incidentes de seguridad en la entidad.

Estas actividades se realizan con el objetivo de crear una base conocimiento que permita a la Entidad enfrentar un evento similar con mayor diligencia y a su vez implementar un modelo de mejora continua para gestión de incidentes de seguridad de la información.

3.5.1. Actividades Previas

Las actividades previas a tener en cuenta en un proceso de lecciones aprendidas están enmarcadas en las descripciones que se hacen a continuación.

- Actividad para ejecutar un análisis forense de seguridad de la información, si así se requiere, teniendo en cuenta que de ser necesario aplicar esta técnica, se debe revisar si los resultados permitieron identificar el origen real del suceso.
- Revisar, identificar y definir planes de mejoramiento en la implementación de controles de seguridad de la información (existentes o complementarios).
- Evaluar la eficacia de los procesos, formatos y estructura organizacional para responder a un incidente de seguridad de la información.
- Actividad para compartir y comunicar los resultados en la gestión de incidente de seguridad de la información.

La etapa de lecciones aprendidas se realiza con el fin de identificar lo bueno, lo malo y lo por mejorar en la detección, reporte, contención y recuperación de un incidente de seguridad de la información en la Entidad.

3.5.2. Identificación de Lecciones Aprendidas

Una vez cerrado el incidente de seguridad de la información que fue identificado, contenido y erradicado, es de vital importancia para la entidad que identifique y adquiera conocimiento rápidamente de las lecciones recibidas del manejo y tratamiento del incidente y se asegure de que se actuó de acuerdo con las conclusiones. Por otra parte, pueden existir también lecciones por aprender de la evaluación y resolución de vulnerabilidades de seguridad de la información reportadas.

Estas lecciones pueden ser en los siguientes aspectos:

- Actualización por requisitos nuevos o modificados de los controles de seguridad de la información, los cuales pueden ser tipo técnico, humano o de procesos, lo cual según su resultado puede conllevar a la actualización del material de concientización y porque no de las directrices o políticas de seguridad de la información dentro de la entidad.
- Actualización de la base de conocimiento de las vulnerabilidades y amenazas de seguridad de la información, conforme al resultado de la evaluación de riesgos de la entidad y de seguridad de la información existente en la misma.
- Posibles cambios en el esquema de gestión de incidentes de seguridad de la información, así como sus procesos y procedimientos, formularios de reporte y base de datos de incidentes de seguridad de la información.

Por otra parte, basado en los incidentes de seguridad de la información gestionada por la entidad, también se debería identificar tendencias o patrones de preocupación con el fin de implementar acciones que permitan anticiparse a un riesgo que derive en un incidente de seguridad. Por lo tanto es indispensable una vez aprabado el plan de Riesgos de seguridad y privacidad de la informacín implementar los siguientes formatos de resgistro de incidents como parte del Sistema de gestion de calidad o implemetar la ISO 27001 en Parques Nacionales Naturales para controlar los riesgos.

4. ANEXO 1: FORMATO REGISTRO DE INCIDENTES

FORMATO REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			Versión: x.x Fecha: xx/xx/xxxx Responsable:
INFORMACIÓN GENERAL DEL REPORTE			
Fecha y hora del reporte:			
Nombre de quien reporta:			
Cargo:		Dependencia y Extensión:	
Sede:		E-mail	

INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del incidente:	
Lugar o sede del incidente:	
No. de Solicitud:	
Descripción del Incidente	

RECURSO INFORMÁTICO AFECTADO
Nombre del Recurso:
Ubicación Física:
Información que contiene:
Fecha de la última copia de seguridad:

5. ANEXO 2: FORMATO VALORACIÓN DE INCIDENTES

FORMATO VALORACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: x.x. Fecha: xx/xx/xxxx Responsable:
INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del reporte:	
No. de solicitud:	
Descripción del Incidente	

INFORMACIÓN DE VALORACIÓN DE INCIDENTE	
Fecha y hora de valoración:	
Nombre de quien valora:	
Valoración del incidente:	
Observaciones de la valoración:	

6. ANEXO 3: FORMATO RESULTADO GESTIÓN INCIDENTE

REPORTE DEL RESULTADO DE LA INVESTIGACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: x.x Fecha: xx/xx/xxxx Responsable:
Objetivo:	
Alcance:	El resultado reflejado en este documento solo debe ser conocido por las personas autorizadas

INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del reporte:	
No. de solicitud:	
Descripción del Incidente	

INFORMACIÓN DE VALORACIÓN DE INCIDENTE	
Fecha y hora de valoración:	
Nombre de quien valora:	
Valoración del incidente:	

INFORMACIÓN EQUIPO INVESTIGADOR		
NOMBRE	CARGO	E-Mail

CAUSAS

PASOS EJECUTADOS EN LA INVESTIGACIÓN

OPORTUNIDADES DE MEJORA			
No.	**DESCRIPCIÓN**	**RESPOSABLE**	**FECHA DE FINALIZACIÓN**

CONCLUSIONES

ANEXOS