PLAN GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

TABLA CONTENIDO

1. INTRODUCCION

La Alcaldía de Ibagué, con el ánimo de salvaguardar los activos de información, considerados como elementos fundamentales para el desarrollo de los procesos de la Entidad, ha implementado políticas de seguridad de la información que buscan minimizar el riesgo que se realicen actos que afecten negativamente el desempeño y la imagen de la Entidad, por lo cual, en concordancia desarrolla un modelo de gestión de incidentes de seguridad de la información.

Como referente para el desarrollo del presente plan de Gestión de incidentes, se tomó la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información, que dispuso El Ministerio de las TIC, en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información, la cual está basada en los lineamientos recomendados en Norma la ISO IEC 27001 – 2013 Numeral 16 de la misma, para la gestión de incidentes.

Implementar un plan de gestión de incidentes para la Alcaldía de Ibagué tendrá como beneficio optimizar los procesos que pueden incidir de manera significativa en la continuidad del negocio y por ende en la garantía del cumplimiento de la misión y los propósitos institucionales.

2. OBJETIVOS

2.1 Objetivo General: Establecer acciones y lineamientos, que permita a la Alcaldía de Ibagué, no solo estar en capacidad de responder en forma adecuada ante la ocurrencia incidentes de seguridad que afecten real o potencialmente sus servicios, sino también establecer la forma como pueden ser detectados y evaluados junto con la gestión de las vulnerabilidades, asegurando que los sistemas, redes, y aplicaciones sean lo suficientemente seguros.

2.2 Objetivos Específicos

- Definir roles y responsabilidades dentro de la Entidad como eje puntual para evaluar los riesgos y permita mantener la operación, la continuidad y la disponibilidad del servicio.

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.

- Permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.

- Minimizar los impactos adversos de los incidentes en la organización y sus operaciones de negocios mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente.

- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Esto tiene como objeto incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.

- Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.

- Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.

- Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información

3. MARCO LEGAL

Ver Normograma Versiones y Vigencias

Modelo de Seguridad y Privacidad de la Información.

Manual para la Implementación de la Política de Gobierno Digital

Decreto Por el cual se establecen los lineamientos generales de la política de Gobierno Digital

Decreto Manual de Funciones de la Alcaldía de Ibagué

Decreto por el cual se adopta la estructura organizacional de la alcaldía municipal de Ibagué, se definen las funciones de sus dependencias y se dictan otras disposiciones

Resolución por la cual se conforman y asignan funciones a los grupos internos de trabajo de la administración central municipal de Ibagué"

Políticas Específicas de seguridad de la información.

4. TERMINOLOGIA:

Evento de Seguridad informática: Un evento de seguridad informática es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de medidas de seguridad (safeguards), o una situación previamente desconocida que pueda ser relevante para la seguridad. [ISO 18044].

Un Evento de Seguridad Informática no es necesariamente una ocurrencia maliciosa o adversa.

Incidente de seguridad informática: Un incidente de seguridad informática es la violación o amenaza inminente a la violación de una política de seguridad de la información implícita o explícita. También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad). Un incidente puede ser denunciado por los

involucrados, o indicado por un único o una serie de eventos de seguridad informática. [NIST800-61, ISO 18044].

Se entienden por incidentes de seguridad las violaciones de acceso, intento de acceso, uso inadecuado, divulgación, modificación o destrucción no autorizada de información, cambios no controlados en el sistema, errores humanos, incumplimiento de las políticas de seguridad, pérdida o robo de información o recurso tecnológico, mal funcionamiento, manipulación, sabotaje, virus, códigos maliciosos, negación del servicio, violaciones de confidencialidad, entre otros.

5. ROLES Y RESPONSABILIDADES

Se crea el equipo de Respuesta a Incidencias de Seguridad Informática **CSIRT** (**Computer Security Incident Response Team),** enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica de la entidad la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.

El equipo **CSIRT** de respuesta a incidentes no es normalmente responsable de la prevención de incidentes, es muy importante que se considere como un componente fundamental de los programas de respuesta. El equipo de respuesta a incidentes debe actuar como una herramienta de experiencia en el establecimiento de recomendaciones para el aseguramiento de los sistemas de información y la plataforma que los soporta.

- Definir los procedimientos para la atención de incidentes
- Definir la clasificación de incidentes
- Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información
- Detectar Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- Atender Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- Recolectar y Analizar Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- Realizar Anuncios de Seguridad: Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad

informática a través de algún medio de comunicación (Web, Intranet, Correo).

- Realizar Auditoria y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- Certificar productos: El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
- Configurar y Administrar Dispositivos de Seguridad Informática: Se encargarán de la administración adecuada de los elementos de seguridad informática.
- Clasificar y priorizar servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- Investigar o Desarrollar nuevas herramientas: el equipo debe realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Conformación del equipo CSIRT:

1. Administrador de Sistema de Seguridad
2. Administradores de los Sistemas de Información
3. Agente Primer Punto de Contacto
4. Analista de Incidente
5. Líder de Grupo de Atención de incidentes
6. Secretaria de las TIC

Usuario Sensibilizado: Servidores Públicos, proveedores, usuarios externos, contratistas o terceros con acceso a la infraestructura de la entidad, quien debe estar informado y concientizado sobre las políticas y procedimientos de seguridad de la información y en particular la guía de atención de incidentes, estos usuarios serán muchas veces quienes reporten los problemas y deberán tener en cuenta lo siguiente:

Agente Primer Punto de Contacto: Es el encargado de recibir las solicitudes por parte de los usuarios sobre posibles incidentes, también debe registrarlos en la base de conocimiento y debe ser el encargado de escalarlos a la persona encargada de la atención según sea el caso.

Este Agente debe contar adicionalmente con capacitación básica en Seguridad de la Información y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes.

Adicionalmente debe contar con una capacitación básica, específicamente en recolección y manejo de evidencia.

Administrador del Sistema: Es la persona encargada para configurar y mantener un activo informático. También debe ser notificado por el agente de primer punto de contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad.

Debe documentar y notificar al agente de primer punto de contacto sobre la actuación o posible solución del mismo. Se recomienda que los administradores cuenten con capacitación en Seguridad de la Información y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes.

Administrador de los sistemas de Seguridad: Persona encargada de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo.

También debe ser notificado por el agente de primer contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer contacto sobre la actuación frente al incidente y la solución del mismo. Se recomienda que el administrador de esta tecnología tenga conocimientos en Seguridad de la Información (con un componente tecnológico fuerte en Redes y erradicación de vulnerabilidades, Ethical Hacking y técnicas forenses) y debe conocer perfectamente la clasificación de Incidentes de la entidad.

Analista del Incidente: debe estar disponible en caso de que un incidente de impacto bajo o medio, en caso de impacto alto que requiera una investigación completa (o uno que amerite acciones disciplinarias o legales o investigación profunda) debe trasladarlo a los Entes respectivos (Fiscalia, Contraloría).

Debe determinar:

- Qué sucedió.
- Dónde sucedió.
- Cuándo Sucedió.
- Quién fue el Responsable.
- Cómo sucedió.

Este actor debe ser un apoyo para los demás actores en caso de dudas sobre los procedimientos y debe ejercer un liderazgo técnico en el proceso de atención de Incidentes de seguridad de la información.

Líder de Grupo de Atención de incidentes: Responde a las consultas sobre los incidentes de seguridad que impacten de forma inmediata, y es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos.

El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Oficina de Comunicaciones, Talento Humano, Oficina Jurídica, Representante de las Directivas para el SGSI).

También debe estar al tanto del cumplimiento de los perfiles mencionados y de revisar el cumplimiento de los procedimientos y mejores prácticas, así como también de los indicadores de gestión, y en capacidad de disparar si lo amerita planes de contingencia y/o continuidad.

Finalmente, el Líder del Grupo de Atención de Incidentes será el responsable del modelo de Gestión de incidentes y debe estar en la capacidad de revisar todos los
incidentes de seguridad y los aspectos contractuales que manejan herramientas de seguridad.

6. ETAPAS DE LA GESTION DE INCIDENTES:

6.1 PREPÁRACION:

Consiste en poner a disposición los recursos necesarios para la atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo

de vida del mismo, creando (si no existen) y validando (si existen) los procedimientos necesarios y programas de capacitación.

6.1.1 Aseguramiento

Esta etapa es responsabilidad de la Secretaría de las TIC o quien haga sus veces, incluye las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones:

- Gestión de Parches de Seguridad: la Alcaldía de Ibagué, debe garantizar las herramientas necesarias para que los administradores de los sistemas de información puedan identificar, adquirir, probar e instalar 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. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el login de eventos.

- Seguridad en redes: Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente

- Prevención de código malicioso: Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas de actualización al día.

- Sensibilización y entrenamiento de usuarios: Los Usuarios en la Alcaldía de Ibagué, incluidos los administradores de TI deben conocer 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.

Los encargados de los sistemas de información deben establecer las necesidades de capacitación de las personas encargadas de la protección de los datos.

Recursos de Comunicación

Es necesario contar con la siguiente información para una adecuada y oportuna atención de incidentes:

- Información del contacto: Se debe mantener publicada y actualizada la lista de los contactos de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.

- Información de escalamiento: Información del contacto para escalar los incidentes según la estructura.

- Información de los administradores de los distintos servicios, servidores y sistemas de información.

- Contacto con áreas interesadas o grupos de interés (CCP-Centro Cibernético de la Policía Nacional, Fiscalía)

Recursos de Hardware y Software

Para realizar la gestión de incidentes, se debe contar con el siguiente conjunto de herramientas:

- Equipos Forenses.
- Analizadores de protocolos.
- Software de adquisición.
- Software para recolección de evidencia.
- Kit de respuesta a incidentes.
- Software de análisis forense.
- Medios de almacenamiento

Debido a las características de la Alcaldía de Ibagué y de conformidad con los recursos existentes, se plantea usar software libre, con el fin no solo de ahorrar recursos, si no de promover la neutralidad tecnológica A continuación se describen cada una de las herramientas.

- Equipo Forense

  Disponer de un Equipo que contenga software libre para escanear vulnerabilidades, escanear la red, los puertos, mapeadores de red y de puertos, analizadores de protocolos, detección remota de servicios, detección remota de equipos activos y sistemas operativos, identificación de software y versiones, análisis de banners, búsqueda de aplicaciones web, y análisis de la configuración de las redes wifi.

  Todas las acciones que se ejecutan durante el análisis forense, no afectan el disco duro que se está analizando, por lo tanto, no se contamina la evidencia, se debe hacer una imagen del disco duro.

- Analizadores de Protocolos

También se dispondrá de un software libre analizador de paquetes de código abierto, el cual se utilizará para resolver problemas de red, análisis, desarrollo de protocolos de software y comunicaciones, y principalmente para monitorear el tráfico de red, el cual en todo caso debe garantizar neutralidad tecnológica.

- Software de Gestión de Adquisición

Se hará uso del software de almacén, el cual permite la gestión de activos, de tal forma que se pueda observar qué activos están asignados, a quién y su ubicación física. Permite revisar el historial completo del activo. Ver qué activos están actualmente desplegados, pendientes (nuevos en espera de instalaciones de software, reparados), listos para implementar o archivados (perdidos / robados, o rotos).

- Software para recolección de evidencia:

La recolección de evidencia está estrechamente ligada al análisis forense, y en ocasiones son usados como sinónimos, por lo tanto, el software forense gratuito seleccionada también debe garantizar la recolección de evidencia.

- Kit de Respuesta a Incidentes

El Kit de respuesta incidentes, las herramientas de análisis forense, software para recolección de evidencia, y Kit de respuesta incidentes podría ser una sola categoría.

- Software de Análisis forense y medios de almacenamiento

Estos dos puntos quedan cubiertos con los cinco capítulos anteriores

Recursos para el análisis de incidentes

La Secretaría de las TIC debe asegurarse de tener la siguiente información disponible para el análisis de los incidentes:

- Listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.

- Diagrama de red para tener la ubicación rápida de los recursos existentes
- Información actualizada de Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios).
- Se debe tener un análisis del comportamiento de red estándar con la siguiente información: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

Recursos para la mitigación y remediación

Elementos básicos necesarios para esta etapa

Backup de Información

Imágenes de servidores.

6.2 DETECCION, EVALUACION Y ANALISIS

6.2.1 Detección Identificación y Gestión de Elementos Indicadores de un Incidente

Las principales fuentes de detección de incidentes son:

- Los Usuarios
- Monitoreo de la Infraestructura

La notificación o reporte de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, llevar a cabo un adecuado proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

Reporte de usuarios: Los usuarios de los diferentes servicios informáticos, sistemas de información y aplicaciones de la Entidad deben reportar de manera inmediata a la detección de incidentes, a la Secretaría de las TIC o al profesional Universitario de Seguridad Informática.

El reporte puede ser vía telefónica, correo electrónico o personal, en todo caso se debe recepcionar y diligenciar la información en la base de datos

establecida. Se sugiere que en lo posible se presenten evidencias tales como pantallazos, e imágenes del incidente.

Los usuarios del sistema que detecten los incidentes de seguridad deben abstenerse de ejecutar acciones propias y deben reportarla de inmediato al contacto indicado.

Monitoreo de infraestructura

La Secretaría de las TIC debe realizar revisión continua del funcionamiento de los activos de información, para prevenir problemas, eventos no deseados e incidentes de seguridad de la información.

Es necesario contar con una serie de elementos indicadores que alerten que posiblemente ha ocurrido un incidente:

- Alertas en Sistemas de Seguridad
- Caídas de servidores
- Reportes de usuarios
- Informe Software antivirus
- Funcionamiento de los sistemas fuera de lo normal
- Tráfico de red excepcionalmente intenso
- Falta de espacio en el disco, o reducción considerable del espacio libre
- Utilización excepcionalmente alta de la CPU
- Creación de nuevas cuentas de usuario
- Uso o intento de uso de cuentas de administrador
- Cuentas bloqueadas
- Gran número de correos electrónicos rebotados con contenido sospechoso

Los siguientes elementos pueden alertar sobre la futura ocurrencia de un incidente, de tal forma que se preparen procedimientos para minimizar el impacto:

- Logs de servidores
- Logs de aplicaciones
- Logs de herramientas de seguridad
- Otras herramientas que permitan la identificación de un incidente de seguridad.

La Secretaría de las TIC, debe aplicar las siguientes actividades a fin de garantizar la detección de incidentes de seguridad:

1. Verificar la utilidad de Administración (Visor de Eventos) del sistema operativo de cada equipo Servidor que hacen parte del Datacenter.
2. Activar el módulo de auditoria del Gestor Base de Datos Oracle
3. Realizar acciones correctivas sobre los sucesos registrados
4. Verificar el registro de todas las acciones de autenticación con éxito y fallidos estén guardadas en archivo tipo log.
5. Verificar la transaccionalidad de datos de entrada exitosos y fallidos sean registradas en el log.
6. Verificar la operatividad y funcionabilidad acciones plan de contingencia (Recreación copias de seguridad)
7. Verificar la operatividad Plan de Manejo de Riesgo
8. Verificar la eficacia de los planes de mejoramiento

Una vez se detecta el incidente, ya sea por parte del usuario final o del administrador del sistema, se genera el reporte respectivo.

6.2.2 Análisis

Las actividades de análisis del incidente involucran otra serie de componentes, es recomendable tener en cuenta los siguientes:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.
- Los administradores de TI deben tener conocimiento total sobre los comportamientos de la Infraestructura que están Administrando.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).
- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.
- Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) ya que esto facilita la correlación de eventos y el análisis de información.
- Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.
- Crear matrices de diagnóstico e información para los administradores menos experimentados.

- Determinar el alcance, las posibles consecuencias e impactos del incidente de seguridad en cuanto al desarrollo de los procesos, la confidencialidad, integridad y disponibilidad de la información, daños físicos a la infraestructura tecnológica y la percepción pública.
- Determinar la naturaleza del incidente en lo que respecta a la intención del atacante y a la amenaza existente.
- Determinar la causa raíz del incidente y establecer los controles y procedimientos para prevenir o mitigar su repetición en el futuro.
- Identificar la fuente del ataque y el atacante, y elaborar un perfil de este.

6.2.3 Evaluación

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad.

La severidad del incidente puede ser:

Alto Impacto: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales de la Entidad. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

Medio Impacto: El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

Bajo Impacto: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

Priorización de los incidentes de seguridad y tiempos de respuesta.

Una vez se tiene conocimiento de la incidencia se procede a priorizarlas de acuerdo al impacto y posibles consecuencias que atenten contra la continuidad de los procesos y cumplimiento de los objetivos de la Entidad.

El Comité de atención a desastres e incidentes informáticos, una vez tiene conocimiento del incidente, procede a realizar la verificación, análisis y evaluación de los mismos y establece niveles de prioridad de acuerdo al tipo de incidente y complejidad en las acciones de respuesta, Ver Plan de respuesta.

Nivel de prioridad: Depende del valor o importancia dentro de la Alcaldía y del proceso que soporta el o los sistemas afectados.

Nivel Criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas
Bajo	0,25	Sistemas que apoyan a una sola Dependencia o proceso de una Entidad
Medio	0,50	Sistemas que apoyan más de una dependencia o proceso de la Entidad
Alto	0,75	Sistemas pertenecientes al área de tecnología y estaciones de trabajo de usuarios con funciones críticas
Superior	1,00	Sistemas Críticos. La operación es crítica para la Entidad cuando al no contar con ésta, la función del proceso no puede realizarse

Tabla Niveles de criticidad del impacto

Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Nivel Impacto	Valor	Definición
Inferior	0,10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo
Medio	0,50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información
Superior	1,00	Impacto alto en uno o más componentes de un sistemas de información

Tabla Niveles de Impacto Actual y Futuro

La prioridad se obtiene mediante la siguiente fórmula

Nivel de Prioridad= (Impacto actual*2,5) + (Impacto futuro *2,5) + (criticidad del sistema *5)

Y el resultado se compara con la siguiente tabla para determinar el nivel de prioridad de atención:

Nivel de Prioridad	Valor
Inferior	00,00 - 02,49
Bajo	02,50 - 03,74
Medio	03,75 - 04,99
Alto	05,00 - 07, 49
Superior	07,50 - 10, 00

Tabla: Niveles de prioridad del incidente

Tiempos de respuesta

El tiempo de respuesta establecido en la siguiente tabla es aproximado al tiempo máximo para que el incidente sea atendido dependiendo del nivel de prioridad, y no corresponde al tiempo de solución del incidente, dado que la complejidad de la atención varía dependiendo del tipo de incidente y del activo de información impactado.

Nivel de Prioridad	Tiempo de Respuesta
Inferior	3 horas
Bajo	1 hora
Medio	30 minutos
Alto	15 minutos
Superior	10 minutos

Tabla: tiempos máximos de respuesta

Qué hacer	Cómo hacerlo	Quien lo hace	Cuando lo hace
Notificación o reporte del incidente	vía telefónica o personal. informatica@ibague.gov.co Teléfono 2611182 ext 167,166,131,250	Usuario, tercero o contratista, o Administrador de TI	Inmediatamente tiene conocimiento del incidente
Registro del incidente o evento	Toma los datos necesarios y realiza el registro en el formato correspondiente si se puede solucionar de inmediato se documenta la solución aplicada entre otros.	Primer punto de contacto (Profesional Universitario de Seguridad Informática	En el momento del reporte del incidente o evento
Identificar el tipo de incidente	Identificar el tipo de incidente, de acuerdo a la tabla de clasificación de incidentes, Verificar las	Primer punto de contacto (Profesional	Inmediatamente al reporte del incidente y

Qué hacer	Cómo hacerlo	Quien lo hace	Cuando lo hace
	evidencias, realizar pruebas para determinar la veracidad de la incidencia , las causas y el impacto	Universitario de Seguridad Informática)	según la tabla de tiempos de respuesta
Escalar el incidente	Informar a la persona encargada de atender el incidente para que tome las decisiones correspondientes.	Segundo punto de contacto (Profesional Universitario de Seguridad Informática)	Inmediatamente al reporte del incidente según la tabla de tiempos de respuesta
Aplicar la estrategia de Contención	Proceder a realizar las acciones contención tabla de clasificación y estrategias de respuesta	Profesionales y técnicos del Grupo de Infraestructura Tecnológica, Administrador de SI	Inmediato al reporte del incidente
Recolectar la evidencia	Para recolectar la evidencia tener en cuenta lo siguientes criterios • Información basada en la red: Log's de IDSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación.	Profesionales y técnicos del del Grupo de Infraestructura Tecnológica, Administrador de SI, Responsable de la Seguridad	Desde el conocimiento del incidente
	• Información Basada en el Equipo: Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red. • Otra información: Testimonio de funcionario o contratista que reporta el evento o incidente		
Manejo De la Evidencia	La información debe ser almacenada y custodiada, debe cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas. Esta información incluye: • Cantidad de incidentes presentados y tratados. • Tiempo asignado a los incidentes. • Daños ocasionados. • Vulnerabilidades explotadas. • Cantidad de activos de información involucrados. • Frecuencias de ataques.	Responsable de seguridad	Al cierre del proceso

Qué hacer	Cómo hacerlo	Quien lo hace	Cuando lo hace
	• Pérdidas.		
Identificar las fuentes de ataque	Se debe tener identificadas las posibles fuentes de ataque: • Empleados Descontentos. • Baja Concientización. • Crecimiento de Redes. • Falta de Previsión de Contingencias. • Desastres Naturales. • Inadecuada protección de la Infraestructura. • Confianza creciente en los sistemas • Virus. • Vulnerabilidades de la seguridad perimetral. • Robo de Información confidencial. • Violación a la privacidad. • Ingeniería social. • Denegación de Servicios. • Hacking	Analista de Incidente	Desde el conocimiento del incidente
Evaluar el impacto	Evaluar el impacto del incidente en la infraestructura tecnológica y en el desarrollo de los procesos de la Entidad. Cuando el impacto sea alto o superior que ponga en riesgo la estabilidad, seguridad y resiliencia del sistema, se informa al Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional.	CSIRT	Según la tabla de tiempos de respuesta
Delegar responsabilidades	Asignar las acciones de erradicación de la incidencia al personal del Grupo de Infraestructura Tecnológica dependiendo de la competencia	Secretario de las TIC	Durante las doce horas siguientes al reporte de la evaluación del impacto
Verificar existencia de recursos	Verificar la disponibilidad de recursos necesarios para la recuperación tales como manuales, backups de sistemas operativos, aplicativos, bases de datos, antivirus, equipos, sistemas eléctricos, servicios de internet, de correo	Profesionales y técnicos del Grupo de Infraestructura Tecnológica, Administrador de SI	Inmediatamente después de la delegación
Disponer de la logística	Asignar los recursos físicos, tecnológicos, comunicaciones, transporte y demás necesarios para	Secretario de las TIC	Durante las doce horas siguientes al reporte de la

Qué hacer	Cómo hacerlo	Quien lo hace	Cuando lo hace
	la ejecución del plan de recuperación		evaluación del impacto
Aplicar la estrategia de erradicación	Realizar las acciones de la estrategia de erradicación (tabla de clasificación y estrategias de respuesta	Profesionales y técnicos del Grupo de Infraestructura Tecnológica, Administrador SI	Según la tabla de tiempos de respuesta
Comunicar a los usuarios	Informar a los usuarios del proceso a intervenir, indicando el tiempo probable de suspensión del sistema, el cual dependen del nivel de complejidad del incidente, previamente establecido en el procedimiento.	Profesional de seguridad	Una vez de conozca la disponibilidad de recursos.
Aplicar la estrategia de recuperación	Realizar las acciones de la estrategia de recuperación (tabla de clasificación y estrategias de respuesta	Profesionales y técnicos del Grupo de Infraestructura Tecnológica, Administrador de SI	Según la tabla de tiempos de respuesta
Comunicar el restablecimiento del servicio	Informar a los usuarios la puesta en marcha del sistema	Profesional en seguridad	Inmediatamente a la terminación de las acciones de restauración
Pruebas	Monitorear el comportamiento del sistema durante tres horas y se deja registrado en bitácora	Responsable de seguridad	Inmediatamente a la terminación de las acciones de recuperación
Retroalimentación	Se aplica una encuesta sobre el funcionamiento del sistema o del Hardware	Profesional en seguridad	Inmediatamente a la terminación de las pruebas
Cerrar el proceso	Presentar un informe del incidente, de las acciones de respuesta aplicadas o acciones correctivas, proponer las acciones preventivas y de mejorar para evitar reincidencias	Profesional en seguridad. Primer punto de contacto	Posterior a las pruebas a satisfacción

6.3 CONTENCIÓN ERRADICACIÓN Y RECUPERACIÓN

Para evitar la propagación del incidente, disminuir el impacto sobre los activos de información, y garantizar la confidencialidad, integridad y disponibilidad de la información, en la Alcaldía de Ibagué, se establecen las siguientes actividades:

6.3.1 Contención: busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI.

Una vez se apliquen las estrategias de contención, se procede a la recolección de la evidencia, para lo cual se debe tener en cuenta:

- ✓ Autenticidad: Quien haya recolectado la evidencia debe poder probar que es auténtica.
- ✓ Cadena de Custodia: Registro detallado del tratamiento de la evidencia, incluyendo quienes, como y cuando la transportaron, almacenaron y analizaron, con tal fin de evitar alteraciones o modificaciones que comprometan la misma.
- ✓ Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

Durante el proceso de recolección de evidencias es necesario realizar las siguientes acciones:

- ✓ Registrar información que rodea a la evidencia.
- ✓ Tomar fotografías del entorno de la evidencia.
- ✓ Tomar la evidencia.
- ✓ Registrar la evidencia.
- ✓ Rotular todos los medios que serán tomados como evidencia.
- ✓ Almacenar toda la evidencia de forma segura.
- ✓ Generar copias de seguridad de la evidencia original.
- ✓ Realizar revisiones periódicas para garantizar que la evidencia se encuentra correctamente conservada

6.3.2 Erradicación y Recuperación: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

CLASIFICACION Y TRATAMIENTO DE INCIDENTES

CLASE DE INCIDENTE	CONCEPTO	TIPO DE INCIDENTE	TRATAMIENTO
Denegación del Servicio	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. **DoS** son aquellos causados porque el número de peticiones lanzado desde un equipo cliente a un servidor excede el límite permitido y ello causa que el servidor afectado deje de estar disponible. **DDoS**: varios equipos haciendo peticiones a un mismo servidor. El ciberataque busca desconectar el sitio web o al menos hacerlo tan lento que los visitantes dejen de intentar usarlo. Esto se logra saturando el sitio web con tráfico malicioso, ya sea dirigido a la red o al servidor. (Inundación UDP, DNS, HTTP, SYN flood)	* Tiempo de respuesta fuera del normal. * Interrupción de servicios tecnológicos * Envío masivo de miles mensajes de correo electrónico (“mail bombing”), provocando la sobrecarga del servidor de correo y/o de las redes afectadas. * Syb Flood * Ataque a través de equipo Zombis *Ataque contra algunos sistemas de Windows para disminuir su rendimiento *Activación programas bacterias para consumir la memoria y la capacidad del procesador * Error Humano	**CONTENCION** * Bloquear o redirigir los paquetes del ataque * Buscar nuevos canales de comunicación entre el servicio y sus usuarios. * Cambiar la URL de la página * Detener las IPS Invalidas * Terminar conexiones o procesos no deseados en servidores y enrutadores y sintonizar sus configuraciones TCP / IP. * Testing de servidor **ERRADICACION** * Involucrar el proveedor de ISP, -Filtrado. * Restitución del servicio caído **RECUPERACION** *volver el servicio al estado original.
Acceso no Autorizado	Consiste en intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red. Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información	* Intentos reiterativos de acceso a recursos. *Ataque de fuerza Bruta *Captura de cuentas de usuario y contraseña mediante herramientas como el keyloggers * Divulgación no autorizada de información personal. * Intrusión física a las instalaciones * Consultas no autorizadas * Intento de acceso no autorizado a base de datos * Acceso no autorizado a carpetas privadas * Creación de usuarios sin autorización	**CONTENCION** * Apagado del Sistema * Bloqueo de la cuenta **ERRADICACION** *Implementar bloqueos automáticos por exceso de intentos. * Cambio de contraseñas *Uso de contraseñas seguras * Determinar los puntos de acceso usados por el atacante e implementar las medidas adecuadas para evitar futuros accesos. * Las medidas pueden incluir la deshabilitación de un módem. * control de acceso en el firewall * aumento de las medidas de seguridad físicas. **RECUPERACION** * Activar las cuentas de usuario *Habilitar el sistema

CLASIFICACION Y TRATAMIENTO DE INCIDENTES			
CLASE DE INCIDENTE	**CONCEPTO**	**TIPO DE INCIDENTE**	**TRATAMIENTO**
Modificación de Recurso no Autorizado	Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.	*Borrado de Información *Modificación de información * Modificación, instalación o eliminación no autorizada de software	**CONTENCION** * Bloqueo de la cuenta **ERRADICACION** * Corrección de efectos producidos * Sustitución de los archivos comprometidos con versiones limpias **RECUPERACION** * Restauración de copias de seguridad * Instalar versiones actualizadas de software
Uso inapropiado de recursos	Un incidente que involucra a una persona que viola alguna política de uso de recursos:	* Abuso de privilegios o de políticas de seguridad* Fuga de Información* Mal uso y abuso de los servicios tecnológicos (correo, internet, intranet)* Captura de información confidencial* Infracciones de derecho de autor y piratería* Destrucción o alteración física de los componentes de red* Destrucción o alteración de la información de configuración* Uso prohibido del recurso de red* uso indebido de información crítica* Robo o pérdida de información* Robo o pérdida de equipos	**CONTENCION** * Identificación del atacante * Bloquear el usuario *Aislarlo del recurso tecnológico **ERRADICACION** *Restauración de copias de seguridad * Reconfigurar la seguridad de la base de datos * Informar a Control Disciplinario * Fortalecer y divulgar las políticas de seguridad **RECUPERACION** * Restaurar los servicios o los componentes de red
Código Malicioso	Programa o parte de éste insertado en otro 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.	* Virus Informático * Ransonware * Malware	**CONTENCION** * Aislar equipo de la red **ERRADICACION** *Corrección de efectos producidos. * Remover código malicioso * Limpiar/Wiping/Zeroing * Localizar la copia de seguridad limpia más reciente antes del incidente. * Mejora de las defensas * Análisis de Vulnerabilidad * Instalación de parches. **RECUPERACION** * Restauración de backups
Reconocimiento			**CONTENCION**

CLASIFICACION Y TRATAMIENTO DE INCIDENTES			
CLASE DE INCIDENTE	**CONCEPTO**	**TIPO DE INCIDENTE**	**TRATAMIENTO**
	se emplea para designar la acción de analizar, por medio de un programa, el estado de los puertos de una máquina conectada a través de una red de comunicaciones. Detecta si un puerto está abierto, cerrado o protegido por un cortafuegos o firewall. Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos.	* Escaneo de puertos * Intento de conexiones arbitrarias a través de un puerto	*Identificación y cierre de puertos **ERRADICACION** * Incorporación de reglas de filtrado en el firewall **RECUPERACION**
Vandalismo	Deformación o cambio producido de manera intencionada a la **página web**. Ataque al sitio web que cambia la apariencia visual del sitio. Los defacement ingresan al servidor web y reemplazan el sitio web alojado por uno propio.	*Ataque por Injection de scripts maliciosos * Modificación del sitio web	**CONTENCION** * Suspensión del servicio web **ERRADICACION** * Aplicar parches de seguridad faltantes * Reparar el sitio web **RECUPERACION** *Restaurar el servicio web
Daños Físicos	Son los sucesos del entorno y la naturaleza que causan daños a los activos de información, pueden ser causados por el hombre, la naturaleza o por averías del hardware y la infraestructura.	* Fuego * Inundaciones * Daños de hardware por fallos en el suministro de energía eléctrica * Terremotos y eventos naturales	**CONTENCION** * Uso de extintores * Llamada a los bomberos si es el caso * Desconectar y retirar equipos **ERRADICACION** * Restaurar copias de seguridad* Mantenimiento técnico de equipos para su recuperación * Datacenter alterno *Activación del plan de continuidad del negocio **RECUPERACION** * Reinstalar equipos y dejar en funcionamiento.

6.4 ACTIVIDADES POST-INCIDENTE

Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.

- ✓ Organizar reuniones.
- ✓ Mantener la documentación.
- ✓ Crear bases de conocimiento.
- ✓ Integrar la gestión de incidentes al análisis de riesgo.
- ✓ Implementar controles preventivos.
- ✓ Elaborar tableros de control.

Lecciones Aprendidas

Posterior a un incidente grave, y periódicamente después de los incidentes menores, es necesario la mejora de las medidas de seguridad y el proceso de gestión de incidentes, por lo tanto, es útil mantener un adecuado registro de lecciones aprendidas que permitan conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.

- Los procedimientos documentados

- Evaluar si se tomaron las medidas o acciones que podrían haber impedido la recuperación.

- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.

- Acciones correctivas pueden prevenir incidentes similares en el futuro.

- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

Este proceso de lecciones aprendidas puede evidenciar que hace falta un paso o que haya una inexactitud en los procedimientos, lo cual se convierte en una oportunidad de mejora.

7.CONTROL DE CAMBIOS

VERSION	VIGENTE DESDE	OBSERVACION
1	10/07/2019	VERSION 1
2	30/10/2019	Actualización Marco Legal y Roles y Responsabilidades
3	29/10/2021	• Actualización marco Legal • Actualización nombre del proceso: de Gestiónde Infraestructura Tecnológica a Sistema Integrado de Gestión • Reorganizació nnumeración

Elaboró	Revisó	Aprobó
Profesional Universitario	Asesor	Secretario(a) de Tic