1. OBJETIVO

Definir las tareas para la clasificación, priorización y escalamiento de incidentes de seguridad de la información, en apoyo y complemento al procedimiento de Gestión de Incidentes de Seguridad de la Información.

2. ALCANCE

Comprende la definición de parámetros y umbrales de capacidad para asegurar el desempeño requerido del sistema y a los cuales se les realizará el seguimiento de uso de los recursos.

3. DEFINICIONES

Gusano Informático: Es un tipo de programa de software malintencionado cuya función principal es infectar otros equipos mientras permanece activo en los sistemas infectados.

Keylogger: Es un tipo de tecnología de vigilancia utilizada para monitorear y registrar cada pulsación de tecla escrita en el teclado de una computadora específica. Este tipo de software malicioso también está disponible para su uso en teléfonos inteligentes, como iPhone de Apple y dispositivos Android.

Phishing: El phishing es una forma de fraude en la que el atacante intenta obtener información como credenciales de inicio de sesión o información de cuenta, haciéndose pasar por una entidad o persona de buena reputación en correo electrónico, mensajería instantánea u otros canales de comunicación.

Ransomware: El ransomware es un software malicioso utilizado por cibercriminales para secuestrar los datos de la víctima y pedir un pago para la recuperación de los mismos. El pago es generalmente exigido a través de BitCoins u otras monedas virtuales para ocultar la identidad del cibercriminal.

Tailgating: También conocido como piggybacking, es una violación de seguridad física en el que una persona no autorizada sigue a un individuo autorizado con el fin de obtener acceso a un área restringida

4. CONTENIDO

4.1. LINEAMIENTOS O POLÍTICAS DE OPERACIÓN

a. Se debe exigir a todos los Funcionarios y Contratistas que usan los servicios y sistemas de información de la Entidad, que observen y reporten cualquier debilidad que comprometa la seguridad de la información.

b. El Equipo de Respuesta a Incidentes de Seguridad de la Información podría estar conformado por los integrantes de la Mesa de Servicio y del GIT Apoyo Informático que cuenten con los siguientes roles:

- Oficial de seguridad de la información o quien haga sus veces.
- Líder de la Mesa de Servicio.
- Responsable del Incidente.
- Coordinador del GIT Apoyo Informático.

c. Se deben adelantar medidas para la prevención de incidentes tales como:

- Análisis periódico de riesgos de seguridad de la información.
- Auditorías internas periódicas.
- Aplicar las lecciones aprendidas de los eventos e incidentes de seguridad de la información para reducir la posibilidad o impacto de incidentes futuros.
- Realizar campañas periódicas de sensibilización a Funcionarios y Contratistas acerca de las políticas de seguridad de la información, procedimientos de seguridad de la información y lecciones aprendidas producto de la gestión de incidentes de seguridad de la información.
- Administración de actualizaciones.
- Aseguramiento (hardening) de servidores expuestos hacia internet.
- Seguridad en la red.
- Protección contra código malicioso.
- Gestión de vulnerabilidades técnicas.

4.2. DETERMINACIÓN DE SÍ ES UN INCIDENTE O EVENTO DE SEGURIDAD DE LA INFORMACIÓN

Para determinar si el evento reportado es un incidente de seguridad de la información, se deben tener en cuenta las siguientes definiciones:

Evento de Seguridad de la Información: Es la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información, la falla de las salvaguardas o una situación desconocida previamente que puede ser pertinente para la seguridad. En resumen, el evento se clasifica como “Evento de seguridad” cuando la confidencialidad, integridad o disponibilidad de la información no se ha comprometido aún o su probabilidad de afectar negativamente la información del negocio es baja.

Incidente de Seguridad de la Información: Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer (o ya ha comprometido) de forma negativa las operaciones del negocio y de amenazar la seguridad de la información.

Ejemplos:

- Interrupción de los servicios tecnológicos (o petición de servicio), comunicada por usuario o generada automáticamente por aplicaciones
- Fallo de sistema de almacenamiento, falla en equipos de seguridad perimetral, caída del canal WAN, entre otros.
- Presencia de malware, virus o comportamiento anómalo de los equipos.
- Fuga, pérdida o robo de información.
- Acceso físico y lógico no autorizado.

4.3. CLASIFICACIÓN DE INCIDENTES

Las categorías para clasificar incidentes de seguridad de la información se describen continuación:

- **Acceso físico no autorizado:** Acceso a las instalaciones de la Entidad sin autorización o sin el debido registro en recepción.

- **Acceso lógico no autorizado:** Acceso no autorizado a sistemas de información, servidores, equipos de cómputo o dispositivos de red de la Entidad.

- **Código Malicioso:** Programas utilizados por usuarios malintencionados para obtener acceso no autorizado y control de equipos de cómputo, servidores, sistemas de información; capturar contraseñas o información

confidencial tecleada por el usuario; secuestrar la información de equipos de cómputo, servidores, dispositivos móviles; entre otros. Esta categoría incluye virus informáticos, gusanos informáticos, ransomware, keyloggers, entre otros.

- **Datos Personales:** Pérdida de confidencialidad, integridad y/o disponibilidad de activos relacionados con datos personales y su información asociada.

- **Denegación de Servicio:** Pérdida de disponibilidad de sistemas, redes u otros servicios tecnológicos.

- **Ingeniería Social:** Método de ataque en el que se engaña a un usuario para obtener acceso a la información y servicios de la Entidad, mediante técnicas tales como phishing, vishing, ransomware, tailgating, entre otras.

- **Uso Inadecuado de Activos:** Violaciones a las políticas de uso aceptable de los activos.

4.4. PRIORIZACIÓN DE INCIDENTES

Es frecuente que existan múltiples incidentes concurrentes, razón por la cual es necesario determinar un nivel de prioridad para la resolución de los mismos. El nivel de prioridad se basa esencialmente en dos parámetros:

4.4.1. Impacto

Será definido por el valor del activo o activos afectados. Para ello, se tendrá en cuenta la valoración del activo según el inventario de activos de información.

- **Menor:** El incidente afecta activos de información con nivel de importancia bajo, que no impacta directamente los objetivos estratégicos de la Entidad.

- **Moderado**: El incidente afecta activos de información con valoración media, que puede afectar los objetivos de un proceso o de seguridad de la información.

- **Mayor**: El incidente afecta activos de información con nivel de importancia alto, impactando directamente los objetivos estratégicos y/o de seguridad

de la información.

- **Bloqueante**: El incidente afecta activos de información con nivel de importancia crítico, impactando directamente los objetivos estratégicos y/o de seguridad de la información. Se incluyen en esta categoría aquellos incidentes que afecten la imagen, reputación o que involucren aspectos legales.

4.4.2. Urgencia

Depende del tiempo máximo en el cual se debe resolver el incidente:

- **Baja:** El incidente no afecta el normal funcionamiento de la Entidad y el tiempo de espera puede ser prolongado.

- **Media**: El tiempo de respuesta por parte de los afectados es moderado, dado que interrumpe actividades que no son críticas para la entidad y afecta a una persona o a un grupo pequeño de personas.

- **Alta**: El tiempo de respuesta por parte de los afectados es corto, dado que afecta gravemente la seguridad de la información e involucra uno o varios procesos de la Entidad.

- **Crítica**: El tiempo de respuesta por parte de los afectados es mínimo, dado que afecta gravemente la seguridad de la información e involucra a terceros (por ejemplo, entes de control, ciudadanos).

4.4.3. Prioridad de los incidentes

La siguiente tabla corresponde al diagrama de prioridades en función de la urgencia y el impacto del incidente:

URGENCIA		IMPACTO			
		Menor	Moderado	Mayor	Bloqueante
	1	2	3	4	
Crítico	4	4	8	12	16
Alta	3	3	6	9	12
Media	2	2	4	6	8
Baja	1	1	2	3	4

4.4.4. Tiempos de atención de los incidentes

Se debe tener en cuenta el tiempo de respuesta del incidente de acuerdo con el nivel de prioridad, así:

- **Crítica:** Antes de 1 hora.
- **Alta:** Entre 1 y 3 horas.
- **Media:** Entre 3 y 12 horas.
- **Baja:** entre 12 y 24 horas.

4.4.5. Escalamiento de Incidentes de seguridad de la información

Para la atención de incidentes de seguridad de la información, la Entidad cuenta con los siguientes niveles:

- **Primer Nivel:** Es la atención a eventos e incidentes brindada por Soporte Técnico y que en primera instancia se puedan solucionar mediante validaciones y asistencias remotas.

- **Segundo Nivel:** Atención especializada por parte de los Administradores TIC's que pertenecen al GIT de Apoyo Informático de la Entidad.

- **Tercer Nivel:** Comprende la atención especializada asumida por el proveedor (comunicaciones, desarrollo, infraestructura tecnológica, hosting) o personal especializado, por ejemplo, analistas forenses.