**PARTE I**

**INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS**

**TÍTULO IV**

**DEBERES Y RESPONSABILIDADES**

**CAPÍTULO V:**

**REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD**

**CONTENIDO**

1. **ÁMBITO DE APLICACIÓN**
2. **DEFINICIONES**
3. **OBLIGACIONES GENERALES EN MATERIA DE CIBERSEGURIDAD**
4. **ETAPAS**
   1. Prevención
   2. Protección y Detección
   3. Respuesta y Comunicación
   4. Recuperación y Aprendizaje
5. **REPORTE DE INFORMACIÓN A LA SFC**

4.1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos.

4.1.8. Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, tal como un SIEM.

4.1.9. De acuerdo con la estructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad.

4.1.10. Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad en el sector financiero y a nivel nacional.

4.1.11. Informar a los consumidores financieros de la entidad sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad.

**4.2. Protección y detección**

Las entidades deben desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Las entidades deben:

4.2.1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.

4.2.2. Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.

4.2.3. Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.

**4.3. Respuesta y comunicación**

Aún con las medidas de seguridad adoptadas, las entidades deben desarrollar e implementar actividades para mitigar los incidentes relacionados con ciberseguridad. Para hacerle frente a esta situación las entidades deben:

4.3.1. Establecer procedimientos de respuesta a incidentes cibernéticos tales como: desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP o cualquier otro que determine la entidad.

4.3.2. Evaluar los elementos de la red para identificar otros dispositivos que pudieran haber resultado afectados.

4.3.3. Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, directamente o a través de CSIRT sectoriales, los ataques cibernéticos que requieran de su gestión.

4.3.4. Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.

4.3.5. En la medida de lo posible, preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

**4.4. Recuperación y aprendizaje**

Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Las entidades deben:

4.4.1. Ajustar sus sistemas de gestión de riesgo y de seguridad de la información como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.

4.4.2. Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector.

**5. REPORTE DE INFORMACIÓN A LA SFC**

**El reporte de incidentes a la SFC se debe realizar utilizando la taxonomía única de incidentes cibernéticos (TUIC), que se encuentra definida y publicada en la página web de esta Superintendencia. Con el propósito de consolidar el modelo nacional de seguridad digital, las entidades excluidas del presente capítulo también podrán reportar sus incidentes al ColCERT usando dicha taxonomía.**

**Así mismo, todas las comunicaciones, reportes de incidentes, alertas tempranas y boletines informativos relacionados con seguridad de la información y ciberseguridad se deben etiquetar usando el protocolo Traffic Light Protocol (TLP), el cual se encuentra publicado en la página web de esta Superintendencia. Dichas comunicaciones se deben remitir desde las cuentas de correo configuradas para este fin. Las entidades también lo podrán usar para el envío de otro tipo de información.**