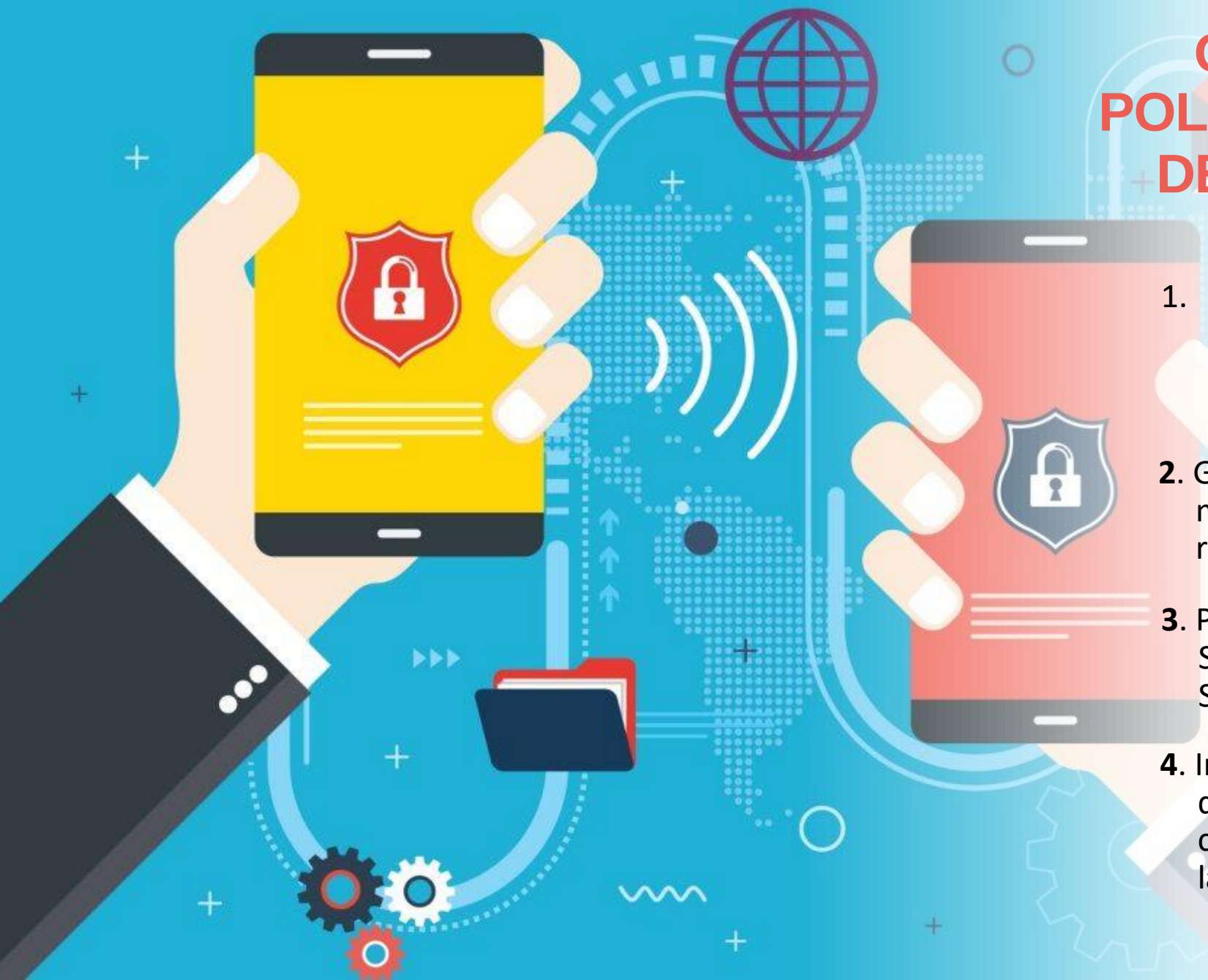
POLÍTICA SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Aprobada mediante el Acta del Comité de Gestión y Desempeño No. 2 del 20 de mayo de 2022.

Para el Departamento Administrativo para la Prosperidad Social (DPS) es de vital importancia la protección de la información, por lo tanto se compromete a salvaguardar la confidencialidad, integridad y disponibilidad de la información, implementando un sistema de gestión de seguridad de la información que genere confianza, permita la gestión del riesgo de seguridad digital, la gestión de incidentes, gestión de activos, que permita generar cultura de seguridad, promueva el mejoramiento continuo en la gestión de la seguridad de la información y contribuya a la generación de valor en la misionalidad de la entidad, en el ejercicio de sus deberes con el Estado y los ciudadanos, lo anterior en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.



OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Establecer mecanismos para gestionar los activos de información, los cuales permitan su identificación, valoración y su respectivo nivel de clasificación.

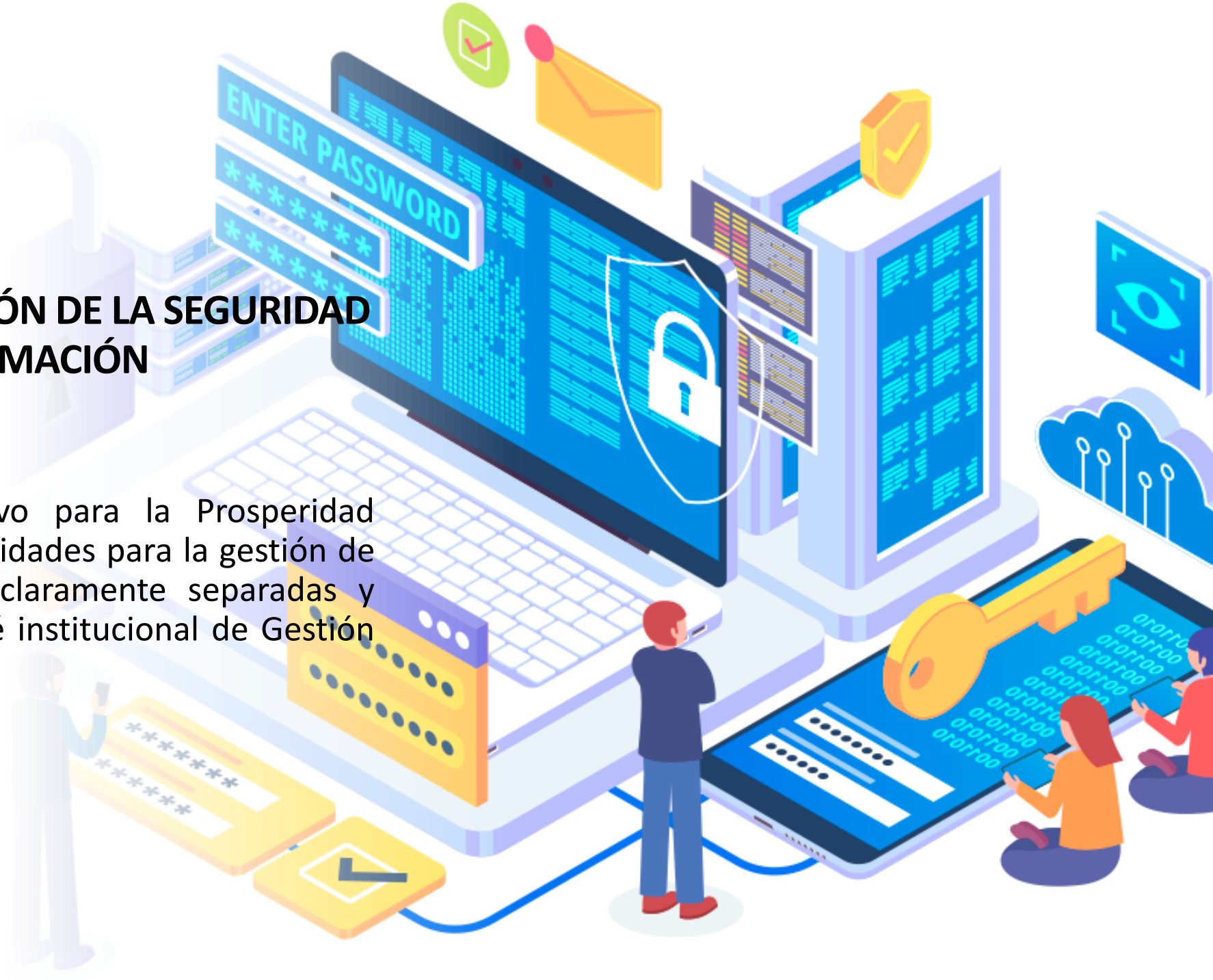
2. Gestionar los riesgos de seguridad digital mediante controles que permitan niveles de riesgo aceptables.

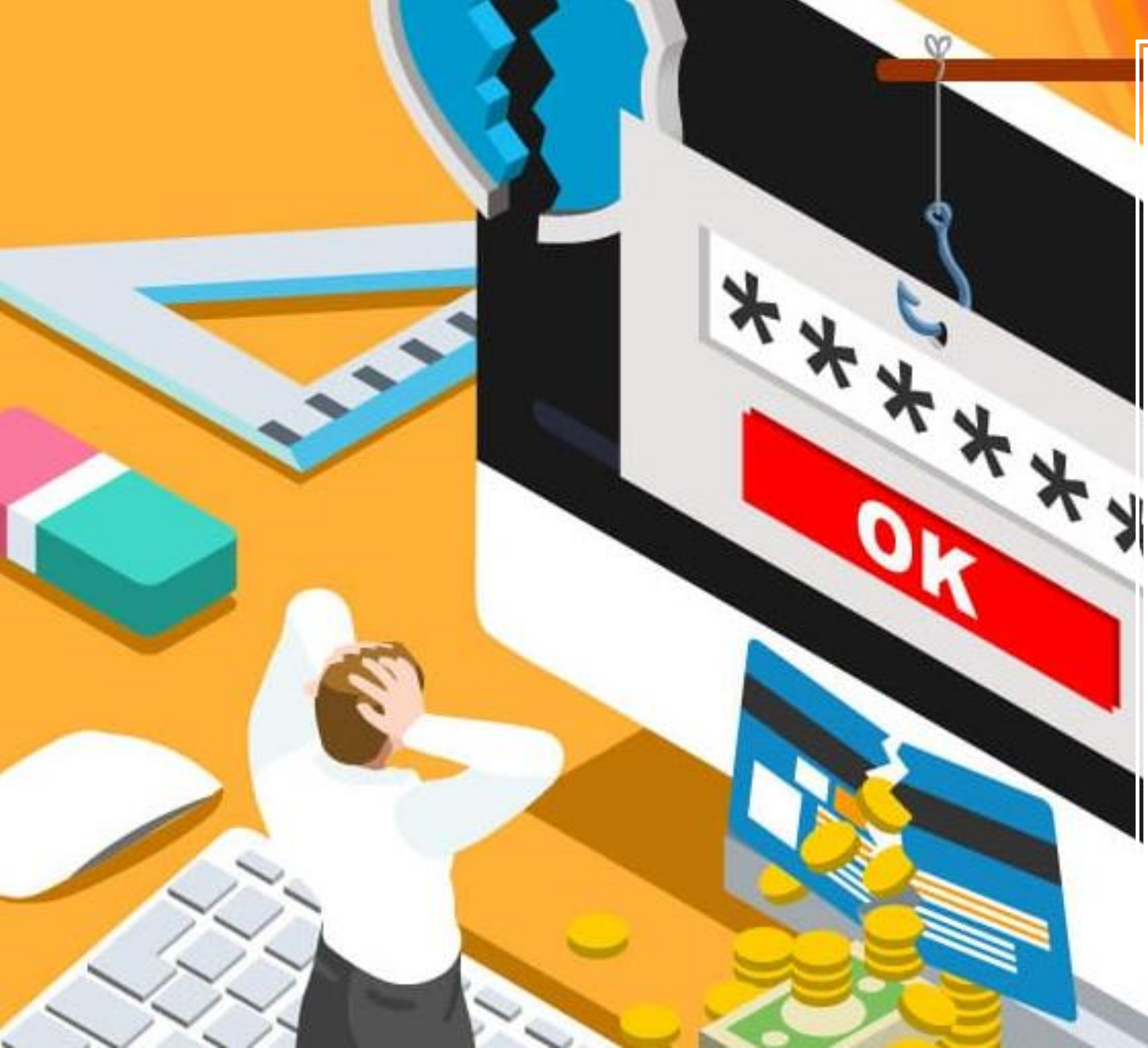
3. Prevenir y gestionar los incidentes de Seguridad de la Información en Prosperidad Social.

4. Implementar mecanismos de comunicación que contribuyan al fortalecimiento de la cultura de la seguridad de la información en la Entidad.

1. POLÍTICA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El Departamento Administrativo para la Prosperidad Social estructura las responsabilidades para la gestión de la seguridad de información, claramente separadas y asignadas, incluyendo el Comité institucional de Gestión y Desempeño.





2. POLÍTICA DE SEGURIDAD DEL RECURSO HUMANO

El Departamento Administrativo para la Prosperidad Social asegura que los servidores públicos, contratistas y pasantes comprendan sus responsabilidades durante la relación laboral o contractual; también garantiza el entendimiento de lo anterior, mediante la debida instrucción, socialización y suscripción de acuerdos de confidencialidad.

3. POLÍTICA GESTIÓN DE ACTIVOS

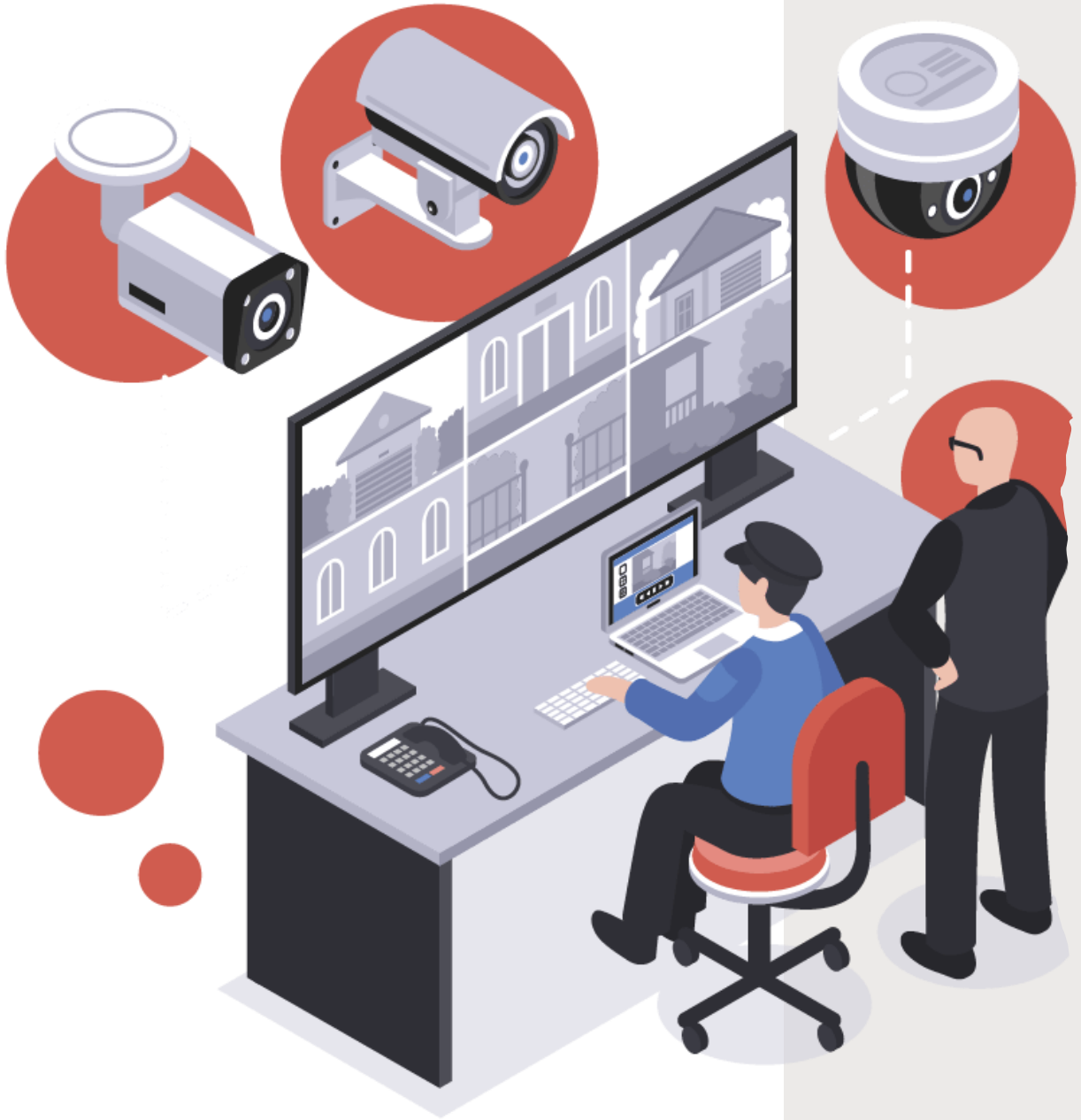
Los activos de información del Departamento Administrativo para la Prosperidad Social son inventariados, revisados periódicamente y asignados a un responsable; sobre estos activos se establecen niveles de protección, acceso y procedimientos para su utilización

4. POLÍTICA DE CONTROL DE ACCESO

El Departamento Administrativo para la Prosperidad Social establece las medidas de control de acceso a nivel de red, sistema operativo, base de datos, aplicaciones y acceso físico para garantizar confidencialidad de la información.

5. POLÍTICA DE CRIPTOGRAFÍA

El Departamento Administrativo para la Prosperidad Social utiliza algoritmos criptográficos fuertes para la protección de los activos de información, claves, aplicaciones, redes de telecomunicaciones, datos sensibles y demás que considere relevante.

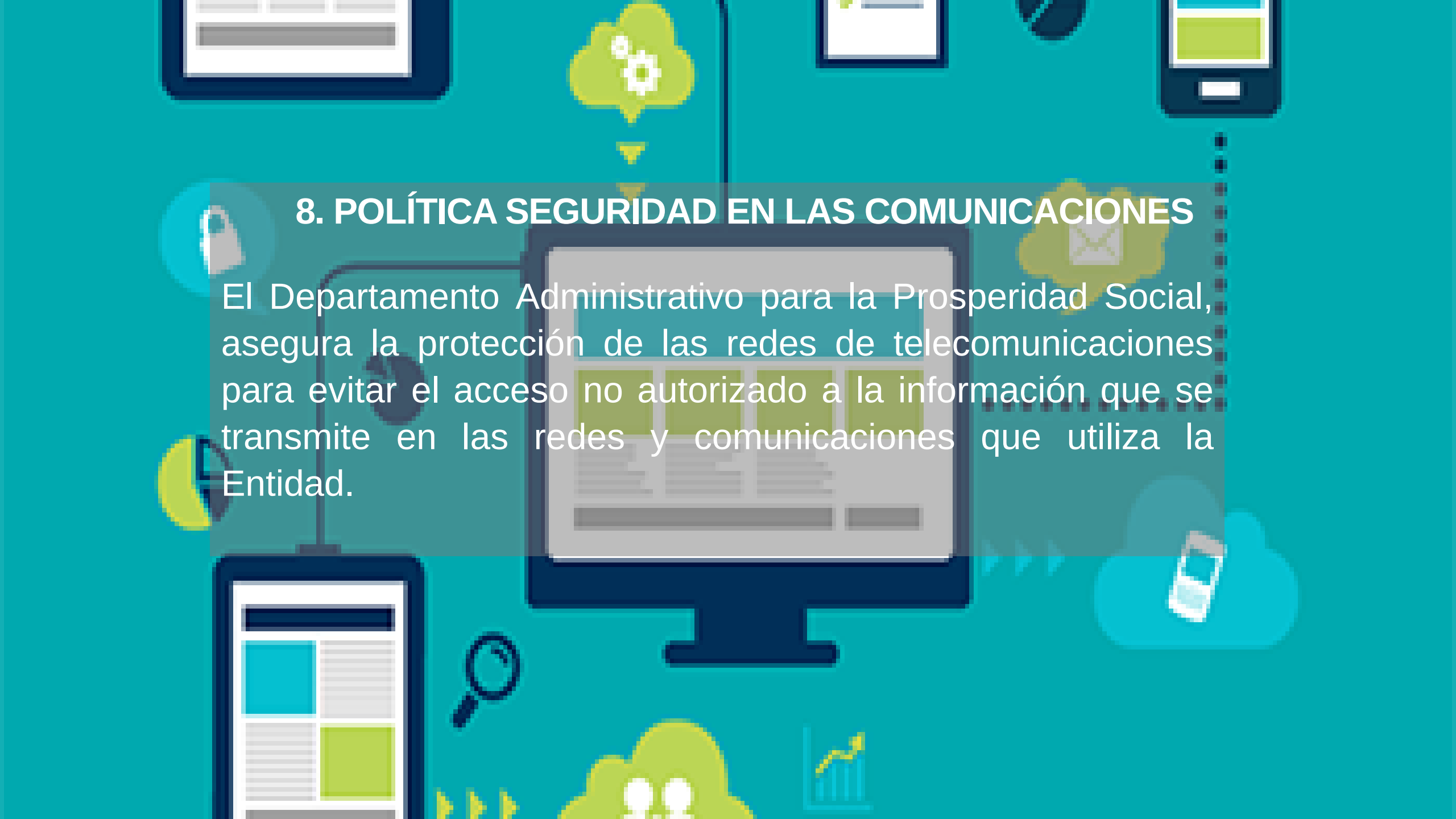


6. POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO

El Departamento Administrativo para la Prosperidad Social, establece controles para prevenir el acceso físico no autorizado y los daños por amenazas ambientales en las distintas sedes, para garantizar la disponibilidad, integridad y disponibilidad de la información.

7. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

El Departamento Administrativo para la Prosperidad Social establece los procedimientos y responsabilidades de administración y seguridad pertinentes a cada ambiente tecnológico, de forma que garantice una debida gestión de cambios, gestión de la capacidad, copias de respaldo, trazabilidad de logs, gestión de vulnerabilidad, control de software operacional, separación de ambientes de desarrollo y protección contra código malicioso.



8. POLÍTICA SEGURIDAD EN LAS COMUNICACIONES

El Departamento Administrativo para la Prosperidad Social, asegura la protección de las redes de telecomunicaciones para evitar el acceso no autorizado a la información que se transmite en las redes y comunicaciones que utiliza la Entidad.

9. POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

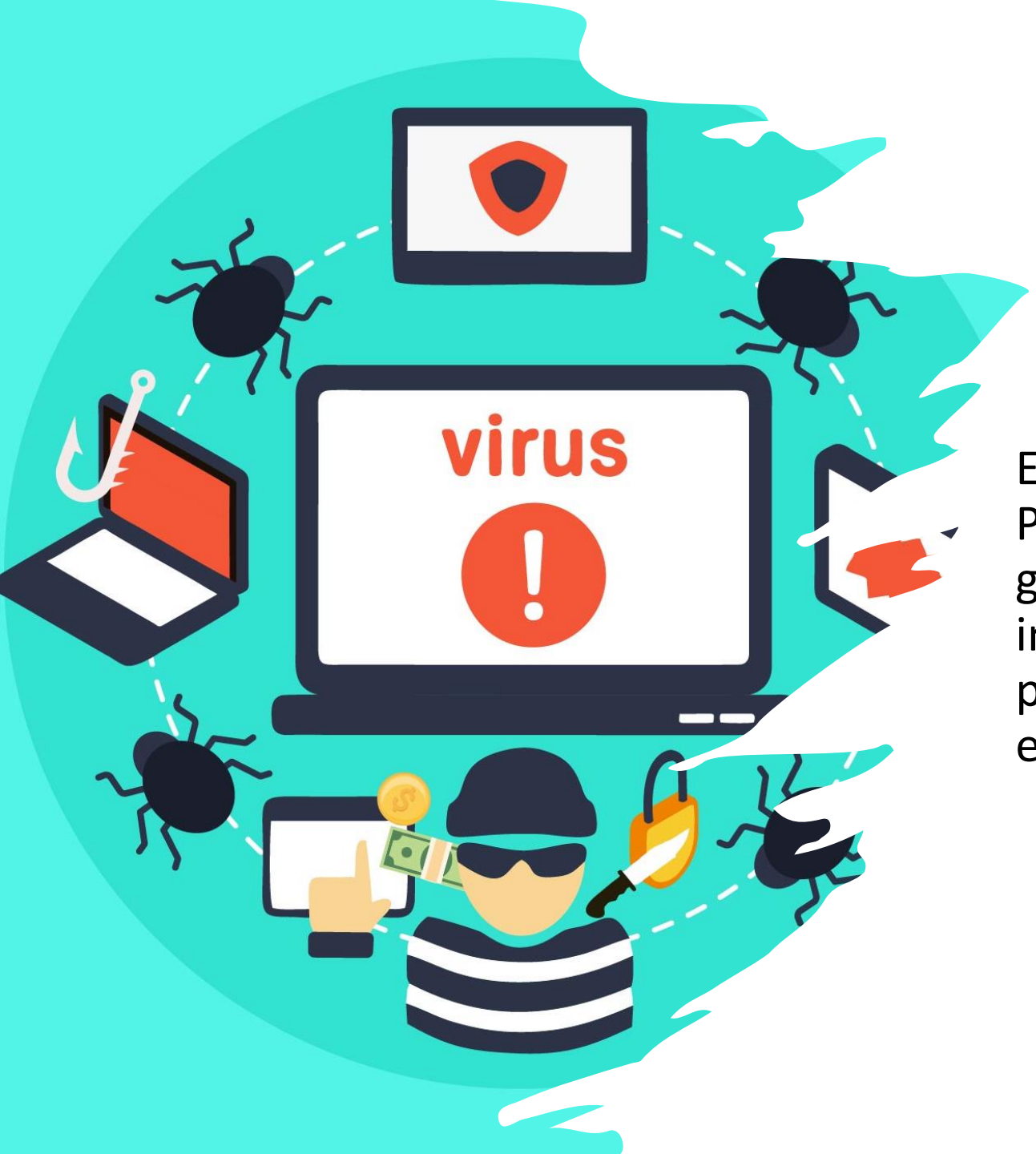
El Departamento Administrativo para la Prosperidad Social realiza análisis e implementación de los requerimientos de seguridad en los sistemas de información desarrollados internamente y/o adquiridos, que incluyen validación de Usuarios, datos de entrada y salida y el procesamiento de los mismos.

Los propietarios de los sistemas de información deben considerar los requerimientos de seguridad necesarios para mantener la integridad, confidencialidad y disponibilidad, durante todo del ciclo de vida de los mismos y la incorporación de controles relevantes.

10. POLÍTICA DE RELACIONES CON LOS PROVEEDORES

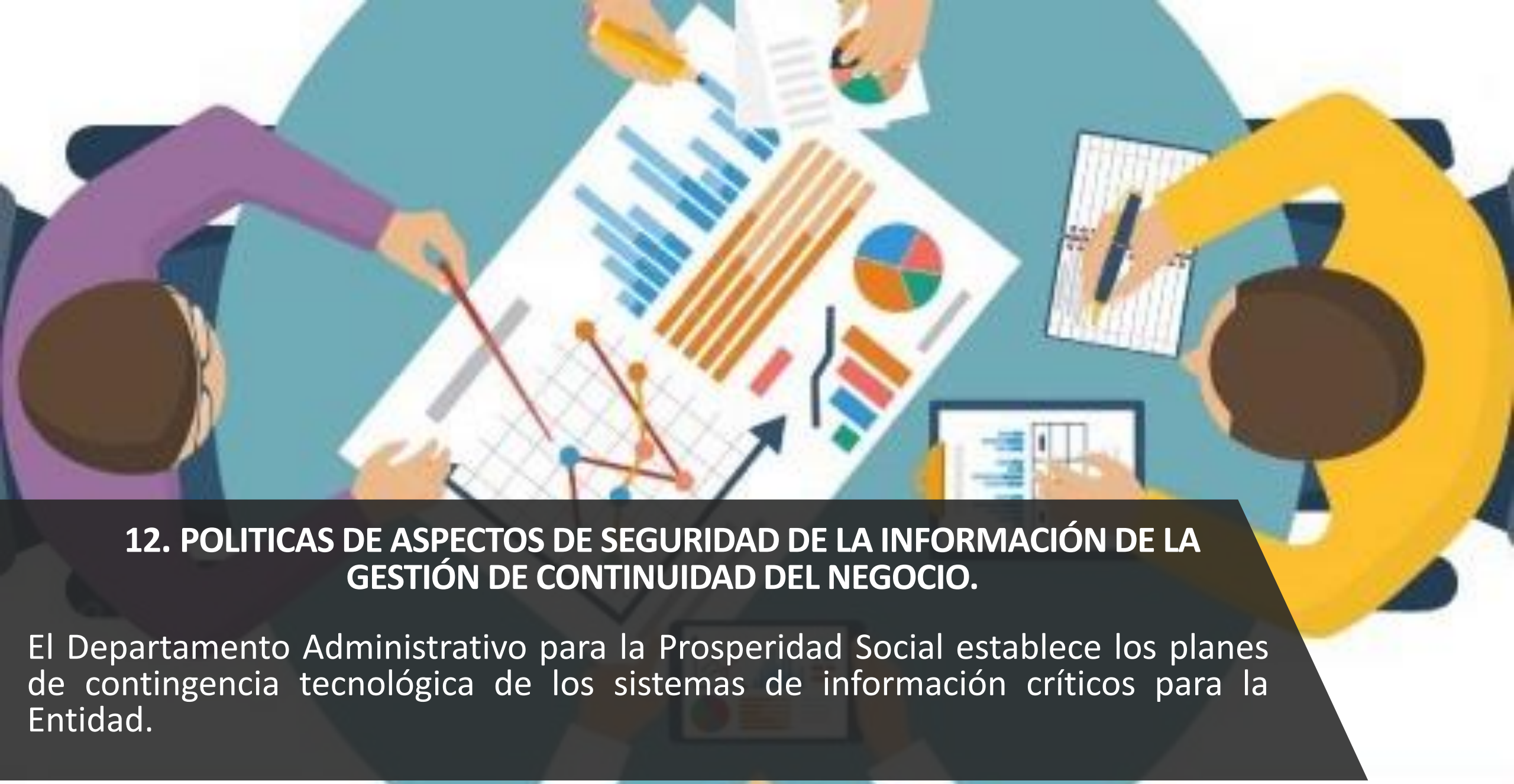
El Departamento Administrativo para la Prosperidad Social establece e implementa lineamientos y controles para que los proveedores, contratistas y terceros adopten un manejo seguro de la información acorde al Sistema de Gestión de Seguridad de la Información - SGSI de la Entidad.

Estableciendo un marco de colaboración equilibrado que preserve la confidencialidad, integridad y disponibilidad de la información de la Entidad.



11. POLÍTICA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

El Departamento Administrativo para la Prosperidad Social promueve la debida gestión de los incidentes de Seguridad de la información, estableciendo el procedimiento, para el manejo, y atención de estos.



12. POLITICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO.

El Departamento Administrativo para la Prosperidad Social establece los planes de contingencia tecnológica de los sistemas de información críticos para la Entidad.

13. POLÍTICA DE CUMPLIMIENTO

El Departamento Administrativo para la Prosperidad Social cumple con los requisitos legales internos y externos aplicables a la Seguridad de la Información que gestiona, incluye entre otros los derechos de propiedad intelectual, protección de datos personales, tiempos de retención de registros, privacidad de información, uso debido de los recursos de procesamiento, y recolección de evidencia y auditorías.

TODOS DEBEMOS CUMPLIR CON LAS POLÍTICAS Y LINEAMIENTOS DEL SGSI

Conoce el Manual del Sistema de Gestión de Seguridad M-GTI-1 Disponible en Kawak:

https://kawak.com.co/dps/gst_documental/doc_visualizar.php?v=2624&m=16

Las políticas se encuentran publicadas en la Intranet de la Entidad.

Sistema de Gestión de Seguridad de la Información S.G.S.I Prosperidad Social