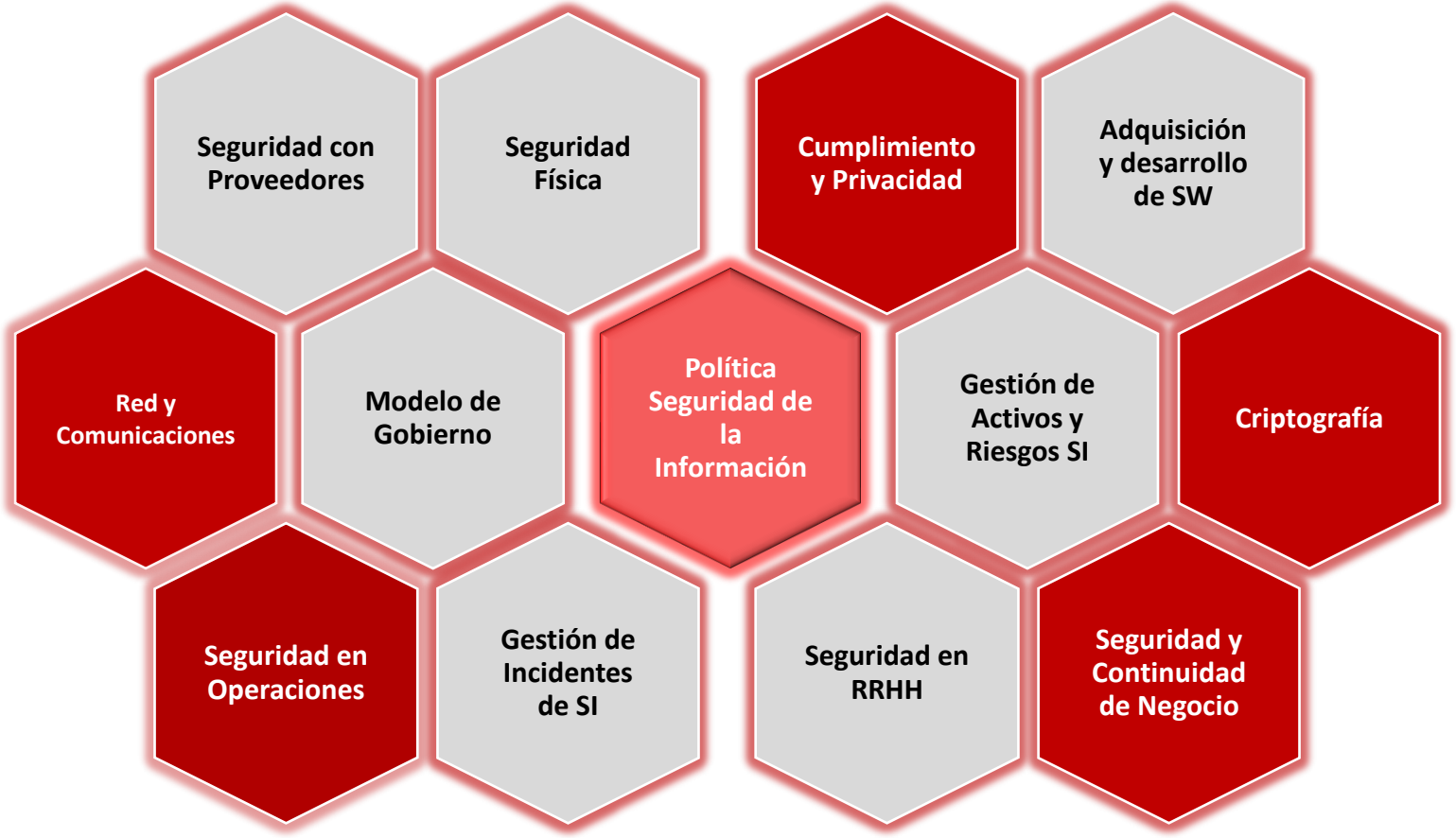
Lineamientos de Ciberseguridad y seguridad de la información

La **CCB** ha definido e implementado lineamientos y prácticas de ciberseguridad y seguridad de la información en los siguientes dominios



Lineamientos de Ciberseguridad y seguridad de la información

La **CCB** cuenta con un Modelo de gobierno donde se tienen definidos los roles y responsabilidades de las distintas instancias que lo conforman.

Lineamientos de Ciberseguridad y seguridad de la información

La **CCB** establece las prácticas y procedimientos para la gestión de activos de información y los riesgos de ciberseguridad y seguridad de la información asociados; su validación y la definición de medidas de protección para mitigar estos riesgos.

Lineamientos de Ciberseguridad y seguridad de la información

La **CCB** cuenta con prácticas y procedimientos para la gestión de incidentes de seguridad de la información, para su identificación, evaluación, y atención, con el fin de minimizar los efectos adversos para la Entidad.

Lineamientos de Ciberseguridad y seguridad de la información

La **CCB** dispone de prácticas asociadas a los procesos y condiciones de vinculación, desarrollo del empleo y terminación de la relación laboral bajo estándares de seguridad, para contar con personal confiable en la Entidad.

LINEAMIENTOS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

La **CCB** dispone de mecanismos de control de acceso electrónico en sus sedes y controles de seguridad física para proteger los bienes de la Entidad. El mantenimiento e implementación de estos mecanismos de protección son de responsabilidad del Jefe de seguridad física y su equipo de trabajo.

Lineamientos de Ciberseguridad y seguridad de la información

La **CCB** cumple con la reglamentación de propiedad intelectual, privacidad y protección de datos personales vigente en el país asegurando la protección de sus signos distintivos, validando que ante requerimientos de cambios en estos o el requerimiento de nuevos signos distintivos se estén respetando los derechos de propiedad intelectual de terceros, e implementando los controles de protección requeridos sobre datos personales.

Lineamientos de Ciberseguridad y seguridad de la información

En la **CCB** se establecen los controles de seguridad de la información frente al acceso de los proveedores y contratistas a la información de la Entidad, así como disposiciones sobre recuperación, contingencia y continuidad de los servicios contratados. La Entidad en la relación con proveedores, protege los datos recolectados de estos en la base de datos de la Entidad.

Lineamientos de Ciberseguridad y seguridad de la información

La **CCB** cuenta con prácticas en procura de contar con controles de seguridad en redes y comunicaciones. La Dirección de Infraestructura tecnológica de la Vicepresidencia de Tecnología y la Dirección de Ciberseguridad y Seguridad de la Información deben identificar e implementar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red utilizados por la Entidad.

LINEAMIENTOS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

En la **CCB**, la implementación de un nuevo software, así como la actualización de este debe estar planeada, administrada, y formalmente documentada asegurando que durante su ciclo de vida los riesgos de ciberseguridad y seguridad de la información asociados sean mitigados.

LINEAMIENTOS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

La **CCB** promueve prácticas para asegurar que las operaciones en la Entidad se realizan bajo parámetros seguros, considerando aspectos para la gestión de cambios, la protección contra malware, el respaldo de la información y la gestión de vulnerabilidades técnicas.

LINEAMIENTOS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

La **CCB** identifica los datos que deben ser cifrados y utiliza las herramientas y mecanismos idóneos para esta acción.

LINEAMIENTOS DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN

La **CCB** cuenta con prácticas referentes a la continuidad de las operaciones críticas a partir de la planificación, implementación, revisión y evaluación de actividades de contingencia, continuidad y recuperación. Como parte de continuar operando ante un evento adverso que interrumpa las operaciones, se establecen los requerimientos de seguridad en la continuidad de la Entidad con el fin de mantener los niveles mínimos de ciberseguridad y seguridad para el negocio ante un evento de interrupción.