CAPÍTULO 20-10

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

1. Ámbito de aplicación

El presente Capítulo contiene disposiciones, basadas en buenas prácticas, que deben ser consideradas como lineamientos mínimos a cumplir por las entidades para la gestión de la seguridad de la información y ciberseguridad. Se entenderá por seguridad de la información, el conjunto de acciones para la preservación de la confidencialidad, integridad y disponibilidad de la información de la entidad. A su vez, la ciberseguridad comprende el conjunto de acciones para la protección de la información presente en el ciberespacio y de la infraestructura que la soporta, que tiene por objeto evitar o mitigar los efectos adversos de sus riesgos y amenazas inherentes, que puedan afectar la seguridad de la información y la continuidad del negocio de la institución.

Especial importancia toman los riesgos que amenazan la ciberseguridad, en un entorno creciente de conectividad y dependencia de los servicios otorgados a clientes a través de plataformas tecnológicas, lo que conlleva que las entidades, por una parte, deban asegurar la adecuada calidad y disponibilidad de los sistemas utilizados para la prestación de dichos servicios; y por otra, enfrenten una progresiva exposición a los riesgos especialmente cuando estos se asumen en el ciberespacio.

La debida adhesión a los lineamientos dispuestos en esta norma será parte de la evaluación de gestión que realiza este Organismo a los bancos en el ámbito de los riesgos operacionales, atendiendo al volumen y complejidad de sus operaciones. Cabe señalar además, que este Capítulo complementa lo señalado en distintas normativas de la Comisión, como son aquellas establecidas en la letra c) del numeral 3.2 del Título II del Capítulo 1-13 de la Recopilación Actualizada de Normas (en adelante RAN) sobre la evaluación de gestión del riesgo operacional; el Capítulo 20-7 en lo que se refiere a los riesgos que las entidades asumen en la externalización de servicios; el Capítulo 20-8 sobre información de incidentes operacionales; y el Capítulo 20-9 sobre gestión de la continuidad del negocio.

En el Anexo adjunto se incluyen definiciones de los conceptos utilizados en la presente normativa.

2. Elementos generales de gestión

En la evaluación de la gestión de la seguridad de la información y ciberseguridad que realiza este Organismo, un elemento fundamental corresponde al rol del Directorio, en lo relativo a la aprobación de la estrategia institucional en esta materia y la autorización de los recursos presupuestarios suficientes para mitigar los riesgos asociados. Es responsabilidad de esta instancia asegurar que la entidad mantenga un sistema de gestión de la seguridad de la información y ciberseguridad, que contemple la administración específica de estos riesgos en consideración a las mejores prácticas internacionales existentes, el que debe ser concordante con el volumen y complejidad de las operaciones de la entidad.

En ese sentido, serán considerados como elementos necesarios para un adecuado sistema de gestión aspectos tales como:

- El Directorio, o quien haga sus veces, ha definido una estructura organizacional con personal especializado y dedicado, e instancias colegiadas de alto nivel jerárquico, con atribuciones y competencias necesarias para gestionar la seguridad de la información y ciberseguridad, procurando una adecuada segregación funcional entre las diferentes áreas e instancias encargadas de estas materias, con roles y responsabilidades claramente establecidos para cada una de ellas.

- Dentro de la estructura organizacional definida se ha dispuesto una función de riesgo, independiente de las áreas generadoras de riesgos, encargada del diseño y mantención de un adecuado sistema de identificación, seguimiento, control y mitigación de los riesgos de seguridad de la información y ciberseguridad. Además, debe ser parte de esta estructura organizacional la función de un oficial de seguridad de la información y ciberseguridad a cargo de estas materias.

- El Directorio ha dispuesto una estructura de alto nivel para la administración de crisis, con atribuciones administrativas reales, jurídicamente delegadas por el Directorio para conocer y administrar los incidentes de seguridad y ciberseguridad de alto impacto que afecten o pudieran afectar los activos de información, propios o los de sus clientes. Como parte de sus funciones, esta estructura debe definir un plan de actuación frente a este tipo de eventos y mantener canales de comunicación adecuados para informar oportunamente de estos incidentes a las autoridades y a las partes interesadas, ya sean internas o externas a la institución.

- El Directorio ha aprobado políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad que definan al menos, el alcance y los objetivos de la entidad respecto de estas materias; el nivel de tolerancia al riesgo en específico para cada una de ellas; una clara definición de los activos de información a resguardar; criterios para clasificar la información y la existencia de un inventario de activos de información permanentemente actualizado, consistente con el mapa de procesos de la entidad. Estas políticas deben ser ampliamente difundidas al interior de la organización, revisadas y aprobadas al menos anualmente por esta instancia.

- El Directorio, como parte del nivel de tolerancia definido, ha aprobado los niveles de disponibilidad mínimos que espera asegurar en los servicios otorgados a través de plataformas tecnológicas, a fin de otorgar una adecuada prestación de servicios a los clientes.

- El Directorio se asegura de informarse periódica y adecuadamente respecto de los riesgos a que está expuesta la entidad en términos de seguridad de la información y ciberseguridad, así como del cumplimiento de sus políticas e incidentes de seguridad de la información y ciberseguridad, con el fin de mejorar su gestión y prevención.

- El Directorio ha aprobado políticas de conducta interna, de manera que todos los empleados y/o personas externas que presten servicios a la entidad utilicen de manera responsable las tecnologías de la información y comunicación puestas a su disposición.

- La entidad promueve una cultura de riesgos en materia de seguridad de la información y ciberseguridad. Esto a través de planes formales de difusión, capacitación y concientización a todos los empleados, los que deben estar en concordancia con las funciones desempeñadas, considerando una periodicidad establecida y oportuna. En el caso de las externalizaciones, la entidad debe asegurarse que el personal asignado adhiera a las políticas establecidas en este ámbito de la institución contratante.

- Los activos de información de la entidad cuentan con un adecuado resguardo en términos de la seguridad física y ambiental, como por ejemplo: la protección de las áreas sensibles de negocios, operativas y dependencias técnicas, dentro de las que se encuentran los centros de datos, fuentes de energía alternativa y respaldos de datos y aplicativos.

- La entidad, como parte de la gestión de sus servicios críticos externalizados, ha implantado un proceso de verificación periódica de la aplicación y cumplimiento de sus políticas de seguridad de la información y ciberseguridad, de manera de garantizar la adecuada protección de los activos de información que son utilizados o administrados por proveedores externos. Asimismo, monitorea permanentemente la infraestructura conectada con proveedores externos, y analiza e implementa medidas para detectar y mitigar potenciales amenazas a la ciberseguridad de la entidad.

- La entidad se asegura de evaluar oportunamente los riesgos asociados a la seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades y/o definir nuevos procesos.

- La entidad realiza inversiones en tecnologías de procesamiento y seguridad de la información y ciberseguridad, que responden a una estrategia definida para estos efectos, que permiten mitigar los riesgos operacionales y tecnológicos y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.

- La entidad gestiona sus alertas o amenazas e incidentes de seguridad de la información y ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación de impacto de estos eventos, y resguardar la confidencialidad, disponibilidad e integridad de sus activos de información.

- El proceso de gestión de la seguridad de la información y ciberseguridad implementado por la entidad asegura el cumplimiento de las leyes y normativas vigentes, entre las que se encuentran, por ejemplo, la protección de los datos de carácter personal y los derechos de propiedad intelectual. Este aspecto deberá también ser exigido a sus proveedores que utilicen sus plataformas.

- La entidad realiza auditorías al proceso de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.

3. Proceso de gestión de riesgos de seguridad de la información y ciberseguridad

La implementación de un apropiado proceso de gestión de los riesgos es fundamental para apoyar el sistema de seguridad de la información y ciberseguridad instaurado por la entidad. Para ello este proceso debe considerar, al menos, la identificación, el análisis, la valoración, el tratamiento y la aceptación o tolerancia de los riesgos a que están expuestos los activos de información de la entidad, así como su monitoreo y revisión permanente.

En línea con lo anterior, se deben considerar al menos los siguientes aspectos:

- Identificación de sus activos de acuerdo con la definición y alcance contenido en la política de seguridad de la información y ciberseguridad. El nivel de detalle utilizado en la identificación y caracterización del activo debe ser suficiente para la adecuada gestión de los riesgos asociados, considerando, por ejemplo, su ubicación física y función, entre otros aspectos.

- Identificación de las amenazas que puedan dañar los activos de información, así como de sus vulnerabilidades, con relación a las amenazas conocidas y los controles existentes. La identificación de amenazas y vulnerabilidades se refuerza con información obtenida de diferentes fuentes, tanto internas como externas.

- Evaluación de los controles existentes de manera de conocer su efectividad y suficiencia.

- Identificación de las consecuencias que puedan tener en los activos de información las pérdidas de confidencialidad, integridad y disponibilidad.

- La entidad realiza un proceso de análisis de riesgo, que considera elementos como la evaluación de la probabilidad de ocurrencia de incidentes y su consecuencia o impacto en los activos de información, en base al grado de daño o costos causados por un evento de seguridad de la información y de ciberseguridad, determinando así su nivel de riesgo.

- La entidad efectúa un proceso de valoración del riesgo, entendido como una actividad donde se compara el nivel de riesgo determinado previamente contra los criterios de valoración y de tolerancia, previamente definidos.

- La entidad elabora un plan de tratamiento del riesgo, entendido como una actividad donde los riesgos priorizados en la etapa de valoración, permiten establecer los controles para reducir, aceptar, evitar o transferir los riesgos.

- La entidad lleva a cabo un proceso formal tendiente a asegurar que los riesgos resultantes sean concordantes con la tolerancia a los riesgos definida.

- La entidad lleva a cabo un proceso formal tendiente a comunicar los riesgos a la organización.

- La entidad revisa con al menos una periodicidad anual, su proceso de gestión de riesgos de seguridad de la información y ciberseguridad, de manera de identificar oportunamente la necesidad de efectuar ajustes en las metodologías y/o herramientas utilizadas.

4. Elementos particulares a considerar para la gestión de la ciberseguridad

Si bien el diseño, implementación y mantención del proceso de gestión de riesgos de seguridad de la información y ciberseguridad establecido en el Título II de este Capítulo proporciona directrices para la gestión de los riesgos, dada la relevancia de los riesgos cibernéticos, las entidades deben realizar una especial diligencia para gestionarlos.

Un elemento esencial de este proceso de diligencia es la determinación de los activos críticos de ciberseguridad, esto es, aquellos activos de información lógicos que son considerados críticos para el funcionamiento del negocio, incluidos los componentes físicos tales como *hardware* y sistemas tecnológicos que almacenan, administran y soportan estos activos, los que de no operar adecuadamente, exponen a la entidad a riesgos que afecten la confidencialidad, integridad y disponibilidad de la información.

Un segundo elemento, se refiere a las funciones de protección de estos activos, la detección de las amenazas y vulnerabilidades, la respuesta ante incidentes y la recuperación de la operación normal de la entidad. Para gestionar estas etapas se deben considerar aspectos tales como:

4.1 Protección de los activos críticos de ciberseguridad y detección de amenazas y vulnerabilidades

- La institución cuenta con un inventario de activos de ciberseguridad críticos clasificados desde una perspectiva de confidencialidad, integridad y disponibilidad.

- La entidad cuenta con un proceso de gestión del cambio que permite que las modificaciones realizadas a la infraestructura de Tecnologías de la Información (TI) sean efectuadas de manera segura y controlada, y que los cambios realizados son controlados y monitoreados.

- La entidad cuenta con un apropiado proceso de gestión de capacidades, que le permite asegurar que la infraestructura TI cubre las necesidades presentes y futuras, considerando el volumen y complejidad de las operaciones de la entidad.

- La entidad cuenta con un proceso de gestión de la obsolescencia tecnológica que le permite mantener una infraestructura TI con estándares de desempeño de seguridad apropiados a los objetivos y necesidades de la entidad.

- La entidad cuenta con un proceso de gestión de configuraciones que permite asegurar adecuados controles a los elementos configurables de la infraestructura TI; y su acceso es controlado y monitoreado.

- La entidad ha implementado un programa de gestión de parches para asegurar que éstos sean aplicados tanto al *software* como al *firmware* de manera oportuna.

- Las redes informáticas se encuentran adecuadamente protegidas de ataques provenientes de Internet o de otras redes externas, a través de la implementación de herramientas que se complementan, tales como: *firewalls*, *firewalls* de aplicaciones *web* (WAF), sistemas de prevención de intrusos (IPS), sistemas de prevención de pérdida de datos (DLP), sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus y anti-*malware*.

- Las redes informáticas se encuentran segmentadas de manera de implementar controles diferenciados, considerando aspectos como grupos de usuarios, tráfico de datos encriptado, tipo de servicios y sistemas de información, a fin de proteger las comunicaciones y los activos críticos de ciberseguridad, así como aislar la propagación de los efectos adversos que podrían derivarse de ciberataques a la infraestructura tecnológica.

- La segmentación de redes alcanza los diferentes ambientes dispuestos por la entidad, entre los que se encuentran aquellos de desarrollo, de pruebas y de producción.

- Los controles establecidos permiten proteger, detectar y contener ataques a la infraestructura TI realizados a través del uso de códigos maliciosos.

- Los controles establecidos permiten mitigar los riesgos derivados del uso de dispositivos móviles y del trabajo a distancia realizado por personal interno o externo; así como también los dispositivos *IoT* (Internet de las Cosas por sus siglas en inglés).

- Los controles establecidos mitigan los riesgos derivados de la adquisición, integración o desarrollo de aplicativos y sistemas, así como su puesta en producción.

- La gestión de identidades y de acceso físico y lógico contempla adecuados controles para resguardar las áreas de acceso restringido, los privilegios otorgados a los usuarios de los sistemas, los derechos de accesos a los servicios de red, a los sistemas operativos, a las bases de datos y a las aplicaciones de negocios, entre otros aspectos.

- La entidad cuenta con adecuadas herramientas para controlar, registrar y monitorear las actividades realizadas por los usuarios en general sobre los activos críticos, así como de aquellos con privilegios especiales.

- Los canales electrónicos dispuestos por la entidad, con los que interactúan los clientes y usuarios, cuentan con apropiados mecanismos de control de accesos, de manera de mitigar, entre otros, los riesgos de suplantación o uso indebido por parte de terceros, de los productos y servicios puestos a su disposición.

- La entidad ha dispuesto normas y procedimientos que establecen la información que requiere ser protegida a través de técnicas de cifrado, así como los algoritmos criptográficos permitidos o autorizados, controles que se utilizan tanto para la transmisión como para el almacenamiento de la información, en orden de proteger su confidencialidad e integridad.

- La entidad ha implementado adecuados resguardos para la conservación, transmisión y eliminación de la información, en conformidad con lo establecido en las políticas internas y la legislación vigente.

- La entidad ha dispuesto herramientas de monitoreo continuo que le permitan en forma proactiva identificar, recolectar y analizar información interna y externa respecto de nuevas amenazas y vulnerabilidades que puedan afectar sus activos de ciberseguridad.

- La entidad cuenta con un proceso de administración de respaldos que le permite asegurar la integridad y la disponibilidad de su información y de sus medios de procesamiento, ante la ocurrencia de un incidente o desastre, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio. Los respaldos de la información se debiesen generar, mantener y utilizar en ambientes libres de códigos maliciosos, y adecuadamente controlados. A su vez, la entidad realiza al menos anualmente pruebas de restauración de sus respaldos, con el fin de verificar que la información crítica puede ser recuperada en caso de que los datos originales se pierdan o se dañen.

- La entidad evalúa mecanismos de cobertura destinados a cubrir los costos asociados a eventuales ataques cibernéticos.

- La entidad cuenta con un *Security Operation Center* (SOC), propio o a través de un servicio externo, que opera las 24 horas del día, con instalaciones, herramientas tecnológicas, procesos y personal dedicado y entrenado, a fin de prevenir, detectar, evaluar y responder a amenazas e incidentes de ciberseguridad.

- La entidad identifica y evalúa regularmente los vectores de ataque a los cuales pudiera estar expuesta su infraestructura tecnológica, como por ejemplo la manipulación o interceptación de las comunicaciones, *phishing*, *malware*, elevación de privilegios, inyección de código, denegación de servicios, ingeniería social, etc.; distinguiendo claramente entre aquellos que pueden afectar la infraestructura física, la infraestructura lógica o el equipamiento de usuarios finales (*endpoint*).

- La entidad realiza en forma regular, con el suficiente alcance y profundidad, pruebas de seguridad a su infraestructura tecnológica para detectar las amenazas y vulnerabilidades que pudieran existir, tales como *pentesting* y/o *ethical hacking*. Sus resultados son gestionados por las respectivas áreas, según sus responsabilidades, y comunicados al Directorio, al menos semestralmente, quedando evidencia en las actas de los análisis y acuerdos adoptados de las acciones a seguir.

4.2 Respuesta y recuperación de las actividades ante incidentes

- La entidad prueba, al menos anualmente, los planes necesarios para enfrentar adecuadamente los escenarios que puedan afectar la ciberseguridad, así como los equipos para dar respuesta a los ciberincidentes que se pudieran materializar. Estos planes son actualizados cada vez que se registran cambios o se materialicen eventos que amenacen la ciberseguridad.

- La entidad cuenta con un plan definido de actuación, que dependiendo de la severidad de un incidente de ciberseguridad permite escalar la situación a la alta administración para la toma de decisiones.

- La entidad cuenta con un plan de comunicaciones, liderado por la alta administración, que opera ante incidentes de ciberseguridad de alto impacto, el cual alcanza a todas las partes interesadas, ya sea internas o externas, a fin de mantenerlas adecuadamente informadas.

- La entidad efectúa un proceso independiente de análisis forense para los ciberincidentes relevantes, que incluya al menos las etapas de identificación, recopilación, adquisición, examen y análisis de evidencias digitales, junto con la generación de documentación e informes de la investigación forense, interpretación de evidencia digital y las conclusiones del trabajo realizado; además de los requerimientos necesarios para custodiar adecuadamente las evidencias generadas.

- La entidad cuenta con una base de incidentes de ciberseguridad de los activos de información presentes en el ciberespacio suficientemente detallada que le permita perfeccionar la capacidad de respuesta de estos.

- La entidad considera la base de incidentes como un insumo para la realización de pruebas que permitan detectar las amenazas y vulnerabilidades que pudieran existir sobre su sistema de gestión de seguridad de la información y ciberseguridad.

- La entidad cuenta con una base de conocimientos y lecciones aprendidas, con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar; identificar posibles mejoras en los procesos; facilitar el intercambio de conocimientos; y disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.

- La entidad realiza autoevaluaciones en esta materia, al menos anualmente, para determinar el grado de cumplimiento con las políticas internas, normativa regulatoria y la adherencia a las mejores prácticas en ciberseguridad, de manera de determinar las vulnerabilidades de su infraestructura y tomar las acciones para su mitigación, así como para prever la adopción oportuna de medidas ante escenarios de amenazas de ciberseguridad.

5. Gestión de la infraestructura crítica de ciberseguridad del país

La entidad como componente de la industria financiera y del sistema de pagos, se convierte en un actor relevante de la infraestructura critica del país, la que de acuerdo con la definición establecida por la Política Nacional de Ciberseguridad “comprende las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado”.

En este sentido resulta importante que las entidades cuenten con políticas y procedimientos para la identificación de aquellos activos que componen la infraestructura critica de la industria financiera y del sistema de pagos, así como para el adecuado intercambio de información técnica de incidentes que afecten o pudieran afectar la ciberseguridad de la entidad, con otros integrantes que son parte de esta infraestructura crítica, cuidando siempre de cumplir con las exigencias legales de secreto y reserva legal, y de confidencialidad de la información personal de los clientes. Considerando lo anterior, a fin de detectar y gestionar las amenazas y vulnerabilidades que pudieran afectar el funcionamiento del sistema financiero, las distintas entidades deben procurar la realización de pruebas conjuntas de determinados escenarios de riesgo.

6. Vigencia

Las instrucciones establecidas en la presente Norma de Carácter General regirán a contar del 1 de diciembre de 2020.

Anexo: Definiciones de conceptos

- **Activo de información:** Componente, recurso o bien económico que sustenta uno o más procesos de negocio de una entidad. Los activos de las entidades varían de acuerdo con la naturaleza de la actividad desarrollada, los que pueden ser primarios como la información (física y lógica) y los procesos y actividades de negocio, o de soporte como *hardware*; *software*; redes de comunicación; personal; entre otros.

- **Amenaza:** Cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica en un sistema u otro tipo de activo, resultando en una pérdida de confidencialidad, integridad o disponibilidad de la información manejada o de la integridad o disponibilidad del propio sistema o activo.

- **Ciberespacio:** Entorno virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas *web*, foros, servicios de Internet y otras redes.

- **Ciberincidentes:** Acción desarrollada a través del uso de redes de computadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta.

- **Criterios de impacto del riesgo:** Se refiere al perjuicio o costos a la entidad causados por un evento de seguridad de la información, considerando aspectos tales como el nivel de clasificación del activo afectado; los incumplimientos de seguridad de la información (pérdida de confidencialidad, integridad y disponibilidad); o incumplimientos de requisitos legales, regulatorios o contractuales.

- **Criterios de valoración del riesgo:** Valor que tienen para la entidad, los activos de información, considerando aspectos tales como el valor estratégico del proceso de información del negocio; la criticidad de los activos; la importancia operacional del negocio en términos de su disponibilidad, confidencialidad e integridad; y el cumplimiento de requisitos legales y regulatorios.

- **Denegación de servicios (DoS):** Un ataque de denegación de servicio (*Denial of Service*) es aquel que tiene como objetivo degradar la calidad de servicio de un sistema o una red llegando a dejarlo en un estado no operativo o inaccesible.

- **Elevación de privilegios:** Acto de explotación de un error, fallo de diseño o configuración de una aplicación, dentro de un sistema operativo o aplicación, para conseguir acceso a recursos del sistema que normalmente están protegidos frente a una aplicación o usuario.

- ***Ethical hacking*:** Utilización de técnicas de ataque para encontrar fallas de seguridad, con el permiso de la organización que es objeto de estos ataques, con el propósito de mejorar la seguridad.

- **Información:** Cualquier forma de registro o dato físico, electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesado, distribuido y almacenado.

- **Incidente de seguridad de la información:** Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información de la entidad.

- **Manipulación de las comunicaciones:** Se basa principalmente en la captura de tráfico, inyección de paquetes, tramas, modificación de la información, entre otros.

- ***Pentesting*:** Acción constituida por un conjunto de pruebas que se basan en ataques hacia los sistemas informáticos con la intención de encontrar sus debilidades o vulnerabilidades.

- ***Security Operation Center* (SOC):** Área de seguridad informática, interna o externa, que es responsable de prevenir, monitorear y controlar la seguridad en las diferentes redes y en Internet, con el objetivo de contar con una capacidad de respuesta proactiva, efectiva y eficiente a incidentes de seguridad.

- **Sistema de Gestión de Seguridad de la Información:** Se refiere a la estructura organizacional, políticas, responsabilidades, procedimientos, recursos y procesos dispuestos por la entidad para establecer, implementar, operar, monitorear, revisar y mejorar la seguridad de la información.

- **Vector de ataque:** Ruta o camino que utiliza un atacante para tener acceso al activo objetivo de ataque, incluyendo las actividades y herramientas que el atacante emplea para materializar la amenaza.

- **Vulnerabilidad:** Cualquier debilidad de un activo o control que puede ser explotada por una o más amenazas.
