POLITICA GENERAL DE VINCI

SEGURIDAD DE LOS SISTEMAS DE INFORMACION

ABRIL 2019

EDITORIAL

Las amenazas contra nuestros sistemas de información son cada vez más sofisticadas y frecuentes, la lucha contra la ciberdelincuencia se ha convertido en una prioridad para nuestro Grupo.

La protección de los activos y de la información de VINCI es una cuestión estratégica por razones de competitividad, confianza y protección de datos. Con las tecnologías digitales ganando en todas nuestras líneas de negocio, nuestro Grupo ha tomado medidas para reforzar los mecanismos que utiliza para proteger sus datos, asegurar sus sistemas de información y mantener su rendimiento operativo.

Aunque los servicios financieros están especialmente expuestos a los riesgos cibernéticos, debido a las repercusiones potencialmente graves de los ataques a nuestros sistemas de pago seguros, todas las líneas de negocio del Grupo, transformadas por la revolución digital, están ahora afectadas. Por ello, cada empleado debe ser consciente de los ciberriesgos y prestar atención cuando observe algo inusual. Pero la ciberseguridad también requiere un enfoque global que incluya a todas las partes interesadas de nuestro ecosistema (proveedores, prestadores de servicios, socios, etc.).

Este documento describe la política general de ciberseguridad del Grupo. En él se especifica el marco político de VINCI en materia de ciberseguridad para todos los sistemas del Grupo y presenta las funciones y responsabilidades de todos los implicados.

Cuento con su compromiso para aplicar y hacer cumplir estas normas de seguridad para que podamos salvaguardar colectivamente el rendimiento operativo de VINCI de la mejor manera posible.

Christian Labeyrie
Vicepresidente Ejecutivo y Director Financiero de VINCI

POLÍTICA GENERAL DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DEL GRUPO VINCI - 15/04/2019 –
N° REVISION : 01
Ámbito de aplicación: Grupo VINCI
Contacto: Benoît Herment, responsable de seguridad de los sistemas de información, VINCI

PRÓLOGO

Para defendernos de una panoplia de ciberamenazas en constante evolución, es esencial reforzar significativamente la seguridad de nuestros sistemas de información.

Tras una visión general de los problemas y riesgos relacionados con la ciberseguridad, este documento pretende: establecen los principios y normas clave para garantizar la protección de nuestros datos y nuestros sistemas de información; definir cómo se organizan las capacidades de ciberseguridad dentro del Grupo, así como las funciones y responsabilidades de todas las partes implicadas.

Se aplica a todas las líneas de negocio, divisiones y entidades de VINCI en todo el mundo. Todos están obligados a aplicar esta política, teniendo en cuenta sus contextos y especificidades locales, especialmente a la luz de sus requisitos culturales, legislativos y reglamentarios.

La política general de ciberseguridad de VINCI es propuesta por los Responsables de Seguridad de la Información (CISO), validada por el Comité de Estrategia de Ciberseguridad y aprobada por el Comité Ejecutivo de VINCI.

Todas las líneas de negocio y entidades de VINCI son responsables colectivamente de la aplicación de medidas para proteger nuestros activos y datos. Los empleados del Grupo también están obligados, a su nivel, a adoptar comportamientos digitales responsables para hacer frente a las amenazas y vulnerabilidades. politique générale de sécurité des systèmes d'information de VINCI est propos.

Este documento se actualizará cuando y como sea necesario en respuesta a amenazas cambiantes.

NUEVOS SISTEMAS Y LOS RIESGOS QUE CONLLEVAN

La transformación digital de las líneas de negocio de VINCI promete numerosas oportunidades de desarrollo. Pero también presenta nuevos riesgos y amenazas - con la proliferación de canales de comunicación,la exposición del Grupo a los riesgos cibernéticos ha aumentado - y los reguladores ejercen una mayor presión.

5 tendencias tecnológicas influyen en nuestros sistemas de información y en nuestra vida cotidiana

1 Computación en la nube

Si bien la nube ofrece un acceso universal a los servicios y aplicaciones de TI, también implica delegar la responsabilidad de la seguridad en los proveedores de servicios. Esto, a su vez impone nuevas responsabilidades a los equipos internos de seguridad.

2 Una mayor movilidad

La posibilidad de acceder a los sistemas de información desde cualquier red y puesto de trabajo ha generado nuevas prácticas como el trabajo remoto (ya sea desde casa, otro lugar o como nómada digital), así como una mayor libertad en la organización del trabajo.

3 Big data

Las tecnologías de Big Data mejoran el tiempo de procesamiento de grandes volúmenes de datos complejos. Dada la ampliación del abanico de fuentes de datos, el reto está en la clasificación de estos (privados, públicos, etc.), para aplicar las medidas de seguridad adecuadas. El Big Data también permite analizar el movimiento y el consumo de los datos, lo que permite anticipar mejor ciertos incidentes de seguridad.

4 Internet de las cosas (IoT)

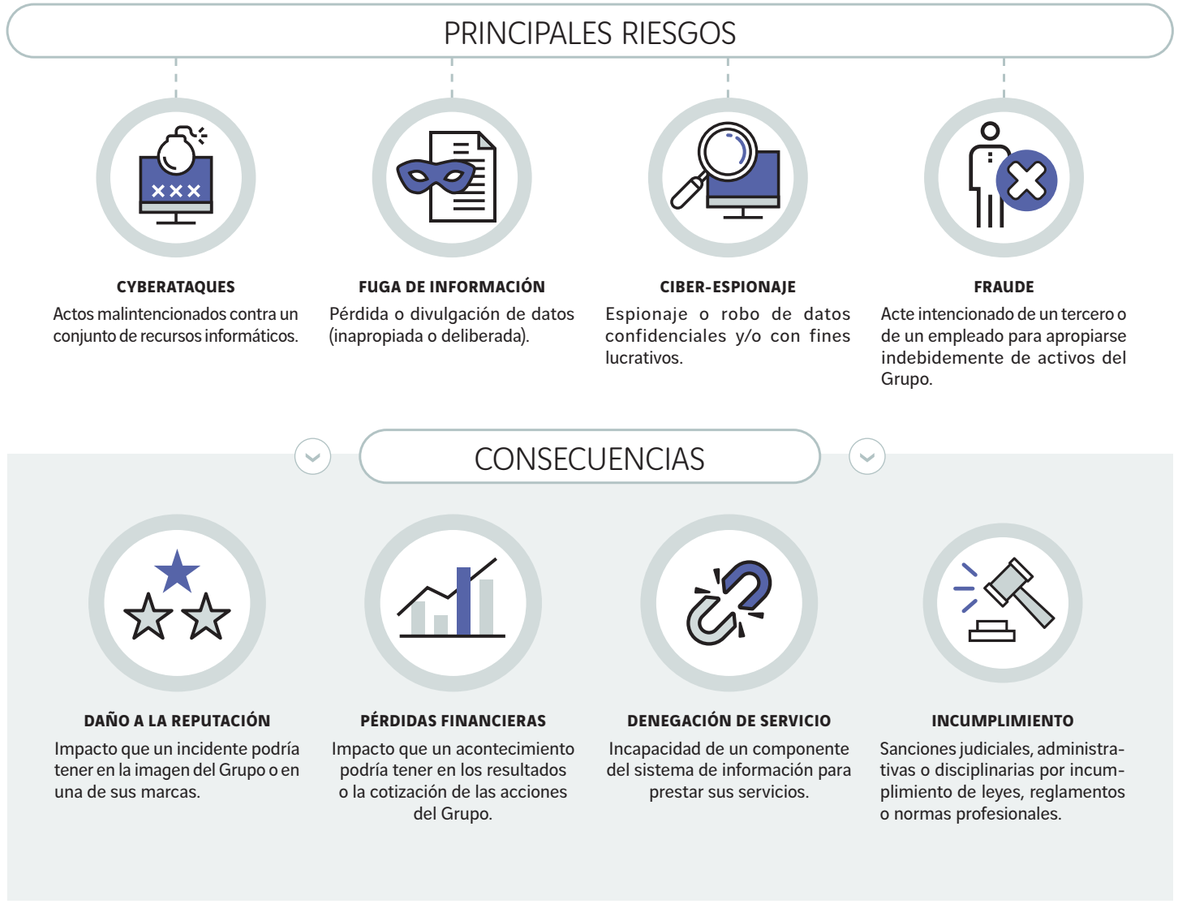
IoT permite el intercambio de datos entre sistemas informáticos no tradicionales en tiempo real y abre posibilidades muy prometedoras para el futuro. IoT presupone una disponibilidad constante de la red y plantea cuestiones cruciales en relación con la seguridad de los datos.

5 Inteligencia artificial (IA)

Las nuevas tecnologías de inteligencia artificial (IA) están destinadas a acelerar y automatizar aún más el tratamiento de la información. En este sentido, la IA desempeña un papel en la propagación de programas maliciosos, pero también puede ayudar a proteger los sistemas de información mejorando la capacidad de respuesta ante incidentes de seguridad.

Principales riesgos

El enfoque de ciberseguridad se esfuerza por mitigar las consecuencias de los cuatro riesgos principales:



El incumplimiento de las obligaciones (legales, reglamentarias, profesionales, contractuales) derivado de una fuga de datos o de un fallo en el sistema de información, también constituye un riesgo en sí mismo.

Cualquier disfunción de los sistemas de información podría tener consecuencias importantes para las actividades del Grupo, como el cese de determinados servicios, pérdidas financieras, sanciones administrativas, sanciones civiles o penales o daños a la imagen del Grupo.

Gestionar la seguridad implica por tanto conjurar con éxito las amenazas, minimizar los riesgos para nuestros sistemas de información y limitar el impacto de estas amenazas en nuestra actividad.

Los niveles de seguridad y protección son proporcionales a los retos a los que se enfrenta cada empresa y se adaptan a cada sistema de información; evolucionan para responder a una ciberdelincuencia estructurada y creciente.

LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN VINCI: 10 PRINCIPIOS CLAVE

El enfoque de VINCI en materia de ciberseguridad se basa en los 10 principios que se presentan a continuación. Cada principio va acompañado de una serie de normas que se aplican a todas las entidades del Grupo.

01.

El Comité Ejecutivo de VINCI es el patrocinador del enfoque en ciberseguridad

El Comité Ejecutivo valida los planes de acción propuestos por el Responsable de Sistemas de Información del Grupo (CIO) sobre la base de un examen de los niveles de seguridad existentes y en función del grado de aceptabilidad de los riesgos para nuestras actividades. El Responsable de Seguridad de Información de VINCI (CISO) dirige los planes de acción en materia de ciberseguridad. El Responsable de Sistemas de Información de VINCI informa de los progresos al Comité Ejecutivo.

- El Comité Ejecutivo asigna un presupuesto específico a la ciberseguridad.
- El Responsable de Sistemas de Información informa periódicamente al Comité Ejecutivo sobre la evolución de las amenazas y los progresos del plan de acción.

02.

Las acciones de ciberseguridad están coordinadas por una Comunidad de todo el Grupo

Una comunidad formada por CISOs de todas las líneas de negocio, divisiones y entidades de VINCI llevan a cabo acciones relacionadas con la seguridad de los sistemas de información. Está gestionada y dirigida por el CISO de VINCI.

- Los debates entre los CISOs deben ser confidenciales dentro de esta comunidad.
- Los CISOs del Grupo informan sistemáticamente al CISO de VINCI de cualquier incidente de seguridad. Los incidentes también se ponen en conocimiento de los demás CISOs.
- Los CISOs trabajan por el interés común del Grupo y comparten sus reacciones. Sus acciones deben comunicarse al CISO de VINCI y contribuir a mejorar la madurez global del Grupo en este ámbito.

03.

Se aplica el principio de subsidiariedad

Las medidas de seguridad comunes y obligatorias se determinan a nivel de Grupo. Cada división/entidad está obligada a aplicarlas y, posteriormente, puede establecer medidas adicionales a su propio nivel. De acuerdo con la organización del Grupo, y en consonancia con la estrategia de seguridad, todas las entidades de VINCI son responsables de aplicar las medidas de seguridad.

- Los CISOs participan en la definición de las normas comunes y obligatorias.
- Velan por el cumplimiento de las normas en su entidad e informan al CISO de VINCI.

04.

Cada entidad debe estar preparada para una crisis de ciberseguridad

Para garantizar que cada entidad pueda reaccionar adecuadamente en caso de incidente, los responsables de la seguridad de la información deben identificar las amenazas que les son propias y establecer procedimientos de gestión de crisis.

- Cada entidad determina las personas de contacto en caso de incidente de seguridad.
- Deben definir y poner a prueba su procedimiento de gestión de crisis al menos una vez al año.

05.

La política de SSI se adapta al nivel de riesgo

El Comité Ejecutivo valida los planes de acción propuestos por el Responsable de Sistemas de Información del Grupo (CIO) tras examinar los niveles de seguridad existentes y en función del nivel de riesgo aceptable para nuestras actividades. Responsable de Seguridad de Información de VINCI (CISO) es responsable de supervisar los planes de acción de ciberseguridad. El CIO de VINCI informa al Comité Ejecutivo de los progresos realizados en relación con estos planes.

- Los CISOs deben validar la coherencia de los grandes riesgos definidos por VINCI para su perímetro.
- Cada entidad debe enumerar sus sistemas críticos y mantener actualizado este inventario.

06.

Los usuarios son la primera línea de defensa

Es compromiso de todos los usuarios comportarse de forma responsable y adecuada para protegerse de los siguientes riesgos.

- La misión de la comunidad de CISOs es concienciar a los usuarios sobre los problemas de seguridad y presentarles procedimientos, herramientas y mejores prácticas.
- Los empleados deben familiarizarse con la «Guía de usuarios de los sistemas de información del Grupo VINCI» y asistir a las sesiones de sensibilización sobre ciberseguridad. Se comprometen a respetar las buenas prácticas de uso de los sistemas de información recomendadas por la comunidad de CISOs.

07.

Medidas de seguridad diseñadas para ser lo menos invasivas posible para los usuarios

En lo posible, las medidas de seguridad deben ser sencillas y comprensibles para todos. Deben tener en cuenta sistemáticamente las necesidades inherentes a cada empresa y no perturbar significativamente la experiencia del usuario.

08.

La mejora de los niveles de seguridad está garantizada por controles periódicos rôles

Comme toute activité, la démarche d'amélioration de la sécurité des systèmes d'information consiste aussi à définir et à exécuter des contrôles ainsi qu'à rendre compte de leurs résultats.

- El diseño del sistema no sólo debe prever estos controles, sino también facilitarlos.

09.

La seguridad de la SI cumple la ley y las normativas

Cada división es responsable de garantizar que el plan de acción tenga en cuenta y cumpla las leyes y normativas vigentes.

10.

El enfoque de la ciberseguridad se revisa periódicamente

La ciberseguridad forma parte de un proceso de mejora continua. En este contexto, el enfoque asociado debe supervisarse y reevaluarse periódicamente.

GOBERNANZA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE VINCI

Partes implicadas y sus responsabilidades

Comité Ejecutivo de VINCI

El Comité Ejecutivo valida la política y la estrategia de seguridad de los sistemas de información de VINCI. Supervisa el progreso del despliegue de la política de ciberseguridad y de los controles asociados.

Responsable de Sistemas de Información de VINCI

El Responsable de Sistemas de Información de VINCI informa periódicamente al Comité Ejecutivo de los cambios en las amenazas y de los avances en el plan de acción. Preside el Comité Estratégico de Ciberseguridad de VINCI.

Responsables de Sistemas de Información en las líneas de negocio

Los Responsable de Sistemas de Información de todo el Grupo aplican medidas de ciberseguridad y asignan los presupuestos necesarios. Garantizan que la estrategia de ciberseguridad se integre en la estrategia global de sistemas de información de su línea de negocio.

Responsables de Seguridad de la Información (CISO) de VINCI

El CISO de VINCI elabora la estrategia de ciberseguridad junto con los CISOs de las líneas de negocio y la presenta al Responsable de Sistemas de Información de VINCI.

Coordina el plan de acción de VINCI y garantiza su aplicación en las líneas de negocio. Comunica el nivel de riesgo de ciberseguridad. Coordina la red de CISOs en las líneas de negocio y difunde las normas y buenas prácticas del Grupo.

CISOs en las líneas de negocio

El CISO de cada línea de negocio es responsable de adaptar y aplicar la política de ciberseguridad de VINCI dentro de su área de responsabilidad. Debe tener en cuenta las amenazas y especificidades locales con el fin de establecer una política de ciberseguridad adaptada a las necesidades de la línea de negocio.

Participa en el programa de transformación de la ciberseguridad de VINCI y es supervisar el plan de acción local. Informa de los incidentes de ciberseguridad e indicadores clave al CISO de VINCI.

Otras partes implicadas

La ciberseguridad es una preocupación clave para VINCI. El Grupo se organiza con vistas a colaboración y participación en las medidas necesarias para alcanzar los objetivos de ciberseguridad:

- El Departamento de Auditoría supervisa las medidas de ciberseguridad.
- El Responsable de Protección de Datos (RPD) define las medidas relativas a la privacidad.
- El Departamento Jurídico y el Departamento de Compras de TI definen las cláusulas de ciberseguridad en los contratos.
- El Departamento de Seguridad garantiza la seguridad física de personas y activos.
- El Departamento de Recursos Humanos despliega programas de concienciación y formación a todos los usuarios.
- El Departamento de Comunicación desempeña un papel clave en la comunicación de crisis relacionadas con la ciberseguridad.
- Los jefes de proyecto evalúan el impacto de la ciberseguridad en la empresa.
- Las autoridades externas (AEPD, CCN-CERT, etc.) prestan asistencia y apoyo en caso de incidentes de ciberseguridad.

Organos de ciberseguridad de VINCI y sus funciones

Comité de Estrategia de Ciberseguridad de VINCI

El Comité de Estrategia de Ciberseguridad de VINCI, presidido por el Responsable de Sistemas Información de VINCI y coordinado por el CISO de VINCI, se reúne cada seis meses. Su función consiste en:

- validar la estrategia de ciberseguridad de VINCI y asignar los recursos y presupuestos necesarios para aplicarla;
- recibir y analizar información sobre incidentes de ciberseguridad dentro del Grupo y gestionar las crisis importantes;
- examinar los principales indicadores de resultados en materia de ciberseguridad.

Miembros: El Responsable de Sistemas Información de VINCI, el experto en ciberseguridad del Comité Ejecutivo, el CISO de VINCI, el Responsable de Auditoría de VINCI y el Responsable de Seguridad de la Información de VINCI.

Comité Directivo de Ciberseguridad de VINCI

El Comité Directivo de Ciberseguridad de VINCI, presidido por el CISO de VINCI, se reúne todos los meses.

Sus responsabilidades incluyen:

- elaborar la estrategia global de ciberseguridad de VINCI y someterla a validación;
- dirigir el programa de transformación de la ciberseguridad de VINCI e implementar proyectos en las líneas de negocio;
- elaborar indicadores clave de rendimiento en materia de ciberseguridad.

Miembros : CISO de VINCI, CISOs de las líneas de negocio.

Pivot Club de Ciberseguridad

Cada tres meses se reúne el Pivot Club de Ciberseguridad coordinado por los CISOs de VINCI. Sus principales objetivos son:

- proporcionar información sobre el programa de transformación de la ciberseguridad de VINCI y recabar opiniones sobre el terreno;
- calificar y registrar formalmente la retroalimentación y comunicar acerca de las mejores prácticas de la industria y las aplicadas dentro del Grupo;
- realizar un seguimiento tecnológico y normativo.

Miembros: El CISO de VINCI, los CISOs de las líneas de negocio, expertos en seguridad, expertos en ciberseguridad y seguridad informática, responsables de redes y sistemas y personal de las líneas de negocio, en función del orden del día.

Papel del Comité Directivo de Sistemas de Información

El Comité Directivo de Sistemas de Información, presidido por el Responsable de Sistemas de Información de VINCI, garantiza que la estrategia global de ciberseguridad esté plenamente en consonancia con la estrategia global de sistemas de información. Se asegura que la estrategia de ciberseguridad sea aplicada eficazmente por las líneas de negocio.

Miembros: El Responsable de Sistemas de Información de VINCI, los Responsables de Sistemas de Información en la línea de negocio.

Comités de ciberseguridad en las líneas de negocio

Cada línea de negocio puede crear tantos comités como necesite en función de su contexto y organización.

Se recomiendan los dos comités siguientes para cada línea de negocio:

Comité directivo de ciberseguridad de las líneas de negocio

Debe crearse un comité directivo de ciberseguridad para cada línea de negocio, presidido por su CISO y que se reúna cada seis meses.

Sus responsabilidades incluyen:

- validar el seguimiento del plan de acción de la línea de negocio y definir y supervisar los recursos y presupuestos relacionados;
- informar sobre los incidentes de ciberseguridad y las crisis graves.

Comité operativo de ciberseguridad de las líneas de negocio

Debe crearse un comité operativo de ciberseguridad para cada línea de negocio, presidido por su CISO y que se reúna periódicamente. Garantiza la aplicación

MARCO DE REFERENCIA DE VINCI PARA LA CIBERSEGURIDAD

La política de ciberseguridad se basa en un conjunto de documentos estándar, que van de lo general a lo específico, y que se enumeran a continuación:

Políticas

Definen formalmente los principales objetivos de la ciberseguridad y la gobernanza correspondiente.

Este conjunto de documentos incluye :

- La política general de ciberseguridad de VINCI (este documento);
- las políticas de ciberseguridad de las líneas de negocio;
- la Guía para usuarios de sistemas de información del Grupo VINCI.

Directivas

Aclaran las normas de seguridad obligatorias para cada ámbito del sistema de información.

Estándares

Incluyen las normas técnicas y una presentación de las herramientas obligatorias en los sistemas de información del Grupo.

Buenas prácticas

Son recopilaciones de un conjunto de comportamientos y normas ya aplicados en el Grupo y que han dado resultados satisfactorios.

Procedimientos

Detallan los pasos y las precauciones que hay que tomar o las metodologías que hay que seguir a la hora de aplicar medidas de seguridad. A menudo, estos procedimientos deben adaptarse al contexto tecnológico del sistema de información.

Estos procedimientos incluyen, entre otros:

- Procedimientos para todo el Grupo (p.e.: el procedimiento a seguir en caso de fuga de datos personales);
- procedimientos para cada función designada (p.e.: gestores de proyectos informáticos, desarrolladores, administradores de sistemas);
- procedimientos para cada tecnología (p.e.: sistema operativo, servidores, cortafuegos).

Estos documentos están a disposición de todas las partes interesadas en la intranet de VINCI.

LOS VERDADEROS
ÉXITOS
SON LOS
QUE SE
COMPARTEN

Traducción julio 2024 - Edición de noviembre 2018 – Fotografía: Luc Benevello – Diseño: wwwgcommeuneidee.com

VINCI
1, cours Ferdinand-de-Lesseps
92851 Rueil-Malmaison Cedex
Tél. : + 33 1 47 16 35 00
www.vinci.com