Política de gestión de riesgos

Propietario: Especialista en Ciberseguridad

Fecha: 06-Dec-2023

Objetivo

Definir la metodología para evaluar y gestionar los riesgos de seguridad de la información de Connect con el fin de lograr los objetivos comerciales y de seguridad de la información de la empresa.

Alcance

El proceso de evaluación de riesgos se puede aplicar a todos los procesos comerciales, la información, los sistemas de información, las redes, los dispositivos y las instalaciones de procesamiento de información que son propiedad de o que son utilizados por solicitantes, empleados, contratistas, consultores, proveedores, socios de Connect, y otros usuarios afiliados a Connect, u otros que utilizan o acceden a las redes o sistemas de información de Connect.

Política

Connect garantizará que la gestión de riesgos desempeñe un papel integral en la gobernanza y la gestión de la organización a nivel estratégico y operativo. El objetivo de una política de gestión de riesgos está diseñado para garantizar que la empresa alcance sus objetivos de negocio y seguridad establecidos.

Estrategia para la gestión de riesgos

Connect, ha desarrollado procesos para identificar aquellos riesgos que obstaculizarían el logro de sus objetivos estratégicos y operativos. Connect garantizará, por lo tanto, que haya implementado los medios para identificar, analizar, controlar y supervisar los riesgos estratégicos y operativos que enfrenta

utilizando esta política de gestión de riesgos en función de las mejores prácticas.

El Especialista en Ciberseguridad se asegurará de que la estrategia y la política de gestión de riesgos se revisen regularmente y que:

- La política de gestión de riesgos se aplique a las áreas relevantes en Connect;
- La política de gestión de riesgos y su aplicación operativa se revisen anualmente;
- Los incumplimientos se comuniquen a los funcionarios y autoridades competentes de la empresa.

Aplicación práctica de la gestión de riesgos

Connect podrá emplear diversos formatos de informes de riesgos para identificar, clasificar y evaluar amenazas, tomando en cuenta factores como los proveedores involucrados, metodologías aplicadas y el alcance técnico de la evaluación. Siempre que sea posible, los riesgos se valorarán según su impacto y probabilidad de ocurrencia, siguiendo criterios definidos en esta política.

Con el objetivo de garantizar la protección continua de los activos y servicios críticos, Connect realizará:

- Evaluaciones formales de riesgos de TI
- Pruebas de penetración en redes y aplicaciones en producción
- Análisis de vulnerabilidades técnicas automatizados y manuales

Periodicidad de las pruebas técnicas: Estas pruebas se ejecutarán al menos dos veces por año (cada seis meses) y adicionalmente cuando se produzcan cambios significativos en los sistemas, infraestructura tecnológica o arquitectura de aplicaciones.

Los riesgos relacionados con la seguridad de la información serán evaluados durante diversas fases del ciclo de vida de diseño y desarrollo del software, especialmente en etapas clave como definición de requisitos, pruebas de aceptación y puesta en producción.

Categorías de riesgo

Algunos riesgos están bajo el control de Connect mientras que otros pueden ser de menor grado. Connect considerará los riesgos dentro de cada una de las siguientes categorías:

- Técnico Reputacional Contractual
- Económico/financiero Regulatorio/cumplimiento Fraude

Cada riesgo identificado se evaluará en cuanto a su probabilidad e impacto. La probabilidad se puede evaluar como poco probable, algo probable o muy probable. El impacto se puede evaluar cómo no impactante, algo impactante y muy impactante. La probabilidad y el impacto se considerarán juntos para formular una clasificación general de riesgo.

Criterios de riesgo

Los criterios para determinar el riesgo son la probabilidad y el impacto combinados de un evento que afecte negativamente la confidencialidad, disponibilidad, integridad o privacidad de los datos del cliente, la información de identificación personal o los sistemas críticos para el negocio.

Para todas las entradas de riesgo, como evaluaciones de riesgos, pruebas de penetración, análisis de vulnerabilidad, entre otros, la gerencia de Connect se reservará el derecho de modificar las clasificaciones de riesgo automatizadas o

proporcionadas por terceros en función de su evaluación de la naturaleza y criticidad del procesamiento del sistema, así como de la naturaleza, criticidad y explotabilidad de la vulnerabilidad identificada.

Respuesta y tratamiento de riesgos

Los riesgos se priorizarán y mapearán utilizando el enfoque contenido en esta política. Se deben emplear las siguientes respuestas al riesgo. Cuando Connect elija una respuesta al riesgo que no sea "Aceptar", desarrollará un Plan de Tratamiento de Riesgos.

- Mitigar: Connect puede tomar medidas o emplear estrategias para reducir el riesgo.
- Aceptar: Connect puede decidir aceptar y monitorear el riesgo en el momento actual. Esto puede ser necesario para algunos riesgos que surgen de eventos externos.
- Transferencia: Connect puede decidir pasar el riesgo a otra parte. Por ejemplo, pueden acordarse términos contractuales para garantizar que el riesgo no lo asuma Connect, o podría ser el seguro quien brinde la protección contra pérdidas financieras.
- Eliminación: el riesgo puede ser de tal manera que Connect decida dejar de realizar la actividad o cambiarla para que finalice el riesgo.

Procedimiento de gestión de riesgos

El procedimiento de gestión de riesgos cumplirá los siguientes criterios:

- Connect mantendrá un Registro de Riesgos y un Plan de Tratamiento.

- Los riesgos se clasificarán por "probabilidad" y "gravedad/impacto", como críticos, altos, medios, bajos o insignificantes.

- El riesgo general se determinará gracias a una combinación de probabilidad e impacto. Los riesgos pueden ser valorados para estimar las posibles pérdidas monetarias cuando sea práctico, o pueden considerarse en relación con un objetivo de control

- Connect responderá a los riesgos como prioridad. La prioridad de corrección tendrá en cuenta la probabilidad y el impacto del riesgo, el costo, el esfuerzo laboral y la disponibilidad de los recursos. Se pueden realizar varias correcciones simultáneamente.

- Se presentarán informes periódicos al equipo de liderazgo sénior de Connect para garantizar que los riesgos se mitiguen adecuadamente y de conformidad con las prioridades y los objetivos de la empresa.

Niveles de aceptación de riesgos

Función	**Responsabilidad**
Presidente	Es el responsable último de aceptar o tratar riesgos que tienen un **impacto estratégico, financiero o reputacional significativo** para toda la organización. Esto incluye riesgos que podrían afectar la viabilidad del negocio, la confianza de los inversores o la imagen pública de Connect. Su decisión se basa en una visión global y en la alineación con los objetivos a largo plazo.
Director de IT	Es el responsable de la aceptación o el tratamiento de riesgos directamente relacionados con la infraestructura tecnológica y la gestión de datos. Esto incluye vulnerabilidades en la red o la infraestructura, y el cumplimiento de normativas de protección de datos. Sus decisiones buscan proteger los activos digitales y asegurar la continuidad operativa de los servicios tecnológicos.
Director de Ingeniería	Se encarga de la aceptación o el tratamiento de riesgos asociados al diseño, desarrollo e implementación de productos y soluciones técnicas. Esto abarca riesgos relacionados con la calidad del código, la arquitectura de las aplicaciones, la escalabilidad de los sistemas, los defectos de software, y la viabilidad técnica de los proyectos. Su enfoque está en asegurar la robustez y funcionalidad.
Director de Producto	Es responsable de la aceptación o el tratamiento de riesgos vinculados directamente con la estrategia, el desarrollo y el ciclo de vida de los productos. Esto incluye riesgos relacionados con la adecuación del producto, la experiencia del usuario, la competitividad, los plazos de

	lanzamiento y la adopción por parte de los clientes. Sus decisiones buscan garantizar que el producto cumpla con los objetivos de negocio y satisfaga las necesidades del mercado.
Especialista en Ciberseguridad	Responsable de velar que se cumpla todas las políticas, puede aprobar la evitación, corrección, transferencia o aceptación de cualquier riesgo citado en el Registro de Riesgos. Esta persona será responsable de comunicar los riesgos a la alta gerencia y a la Junta Directiva y de adoptar tratamientos de riesgo de acuerdo con la dirección ejecutiva.

Modificación y cancelación de esta Política

Connect se reserva el derecho de modificar, enmendar o cancelar esta política en cualquier momento.

Excepciones

Las solicitudes de excepción a esta Política deben enviarse a Director de IT / Especialista en Ciberseguridad para su aprobación.

Infracciones y cumplimiento

Cualquier infracción conocida de esta política debe reportarse al Director de IT / Especialista en Ciberseguridad. Las infracciones de esta política pueden dar lugar a la retirada o suspensión inmediata de los privilegios del sistema y la red o medidas disciplinarias de acuerdo con los procedimientos de la empresa, incluido el despido.

Historial de versiones

Versión	Fecha	Descripción	Autor	Aprobado por
1	15-Jun-2023	Creación de documentos	Raanvalen Ramos Especialista en Ciberseguridad	Jorge Marín Directo de IT
1.1	12-Nov-2024	• Cambio de formato • Ajustes en los niveles de aceptación del riesgo	Raanvalen Ramos Especialista en Ciberseguridad	Jorge Marín Directo de IT
2	16-JUN-2025	• Ajustes en los niveles de aceptación	Raanvalen Ramos Especialista en Ciberseguridad	Jorge Marín Directo de IT

Anexo A: Matriz de evaluación de riesgos y clave de descripción

Escala de puntuación de probabilidad

Puntaje	Etiqueta	Descripción
1	Muy improbable	Un evento de amenaza es tan improbable que se puede suponer que es posible que no se experimente su ocurrencia. Una fuente de amenaza no está motivada o no tiene capacidad, o existen controles para prevenir o impedir significativamente la explotación de la vulnerabilidad.
2	Improbable	Un evento de amenaza es poco probable, pero existe una pequeña posibilidad de que se experimente su ocurrencia. Una fuente de amenaza carece de motivación o capacidad suficiente, o existen controles establecidos para prevenir o impedir que se explote la vulnerabilidad.
3	Algo probable	Es probable que se produzca un evento de amenaza y se puede suponer que se puede experimentar su ocurrencia. Una fuente de amenaza está motivada o plantea la capacidad, pero existen controles que pueden reducir significativamente o impedir la explotación exitosa de la vulnerabilidad.
4	Probable	Es probable que se produzca un evento de amenaza y se puede suponer que se experimentará su ocurrencia. Una fuente de amenaza está altamente motivada o presenta capacidad y recursos suficientes, pero existen algunos controles que pueden reducir o impedir la explotación exitosa de la vulnerabilidad.
5	Muy probable	Un evento de amenaza es muy probable y se puede suponer que se experimentará su ocurrencia. Una fuente de amenaza está altamente motivada o presenta capacidad o recursos suficientes, pero no existen controles o los controles existentes son ineficaces y no previenen ni impiden la explotación exitosa de la vulnerabilidad.

Escala de puntuación de impacto

Puntaje	Etiqueta	Descripción
1	Impacto muy bajo	Se podría esperar que un evento de amenaza casi no tenga efectos adversos en las operaciones organizacionales, las capacidades de la misión, los activos, los individuos, los clientes u otras organizaciones.
2	Bajo impacto	Se podría esperar que un evento de amenaza tenga un efecto adverso limitado, es decir: degradación de la capacidad de la misión, pero aún se pueden realizar funciones primarias; daños menores; pérdida financiera menor; o el rango de efectos se limita a algunos recursos cibernéticos pero no a recursos críticos.
3	Impacto medio	Se podría esperar que un evento de amenaza tenga un efecto adverso grave, es decir: una degradación significativa de la capacidad de la misión, pero las funciones primarias aún se pueden realizar a una capacidad reducida; daños menores; pérdida financiera menor; o la gama de efectos es significativa para algunos recursos cibernéticos y algunos recursos críticos.
4	Alto impacto	Se podría esperar que un evento de amenaza tenga un efecto adverso grave o catastrófico, es decir: degradación grave o pérdida de la capacidad de la misión y que no se puedan realizar una o más funciones primarias; daños importantes; pérdida financiera importante; o la gama de efectos es extensiva a la mayoría de los recursos cibernéticos y a la mayoría de los recursos críticos.
5	Impacto muy alto	Se podría esperar que un evento de amenaza tenga múltiples efectos adversos graves o catastróficos en las operaciones, activos, individuos u otras organizaciones de la organización. La gama de efectos es amplia y afecta a casi todos los recursos cibernéticos.

Grupos de puntuación

Rango	Grupo	Descripción
1 – 4	Bajo	Se podría esperar que un evento de amenaza tenga un efecto adverso limitado en las operaciones organizacionales, las capacidades de la misión, los activos, los individuos, los clientes u otras organizaciones.
5 – 14	Medio	Se podría esperar que un evento de amenaza tenga un efecto adverso grave en las operaciones organizacionales, las capacidades de la misión, los activos, los individuos, los clientes u otras organizaciones.
15 – 25	Alto	Se podría esperar que un evento de amenaza tenga un efecto adverso severo en las operaciones organizacionales, las capacidades de la misión, los activos, los individuos, los clientes u otras organizaciones.