somos natura

Manual del proveedor

Evaluación de ciberseguridad

natura

Objetivos

La evaluación de seguridad tiene como finalidad:

- ***Asegurar*** *que los proveedores estén alineados con los estándares de Seguridad de la Información de Natura;*
- ***Evaluar*** *el nivel de madurez de los controles de seguridad implementados;*
- ***Identificar****, evaluar y mitigar riesgos que puedan impactar datos, sistemas y operaciones;*
- ***Promover*** *una relación transparente, colaborativa y orientada a la mejora continua.*

natura

natura AVON

Manual del proveedor de **seguridad cibernética**

En Natura, creemos que el cuidado de la seguridad digital y la continuidad de negocios es un compromiso compartido. Por ello, caminamos de la mano con nuestros socios para garantizar que todos estén en sintonía con nuestros estándares de ciberseguridad. Este material fue creado para guiarle en cada etapa de este proceso, de forma clara, segura y accesible.

Nuestro propósito

Nuestra Gestión de Riesgos con Terceros tiene un enfoque principal: asegurar que nuestros socios estén totalmente alineados con las prácticas de seguridad de Natura al prestar sus servicios. Es un proceso colaborativo que nos ayuda a comprender la madurez de sus controles de seguridad, identificando y mitigando juntos cualquier riesgo que pueda afectar los datos, sistemas y operaciones de Natura.

Alcance de la **evaluación**

El alcance incluye el análisis de los controles internos del proveedor y de los siguientes dominios de riesgo:

- ***Gobernanza*** *de Seguridad de la Información;*
- ***Privacidad*** *y Protección de Datos;*
- ***Identidad*** *y Accesos;*
- ***Desarrollo*** *Seguro;*
- ***Inteligencia*** *Artificial;*
- ***Monitoreo*** *y Respuesta a Incidentes;*
- ***Protección*** *de la Infraestructura y Cloud;*
- ***Riesgos*** *y Continuidad;*
- ***Capacitación*** *y Concientización;*
- ***Continuidad*** *de negocios y recuperación.*

El alcance es dinámico, ya que puede ajustarse durante la debida diligencia basándose en las respuestas proporcionadas en el cuestionario y está sujeto a la validación por parte del equipo de Seguridad de la Información de Natura.

Vista general del proceso de evaluación

natura

01. ***Clasificación** del Servicio (Tierización)*

En esta etapa, el responsable del proveedor en Natura envía información esencial para la clasificación del proveedor y del servicio prestado, considerando:

- **A** Tipo de datos involucrados (datos personales, sensibles o confidenciales);
- **B** Criticidad del servicio para el negocio;
- **C** Involucramiento con procesos estratégicos;
- **D** Desarrollo o mantenimiento del sistema;

El plazo para la realización de la tierización y el envío del cuestionario al proveedor es de hasta **3 días hábiles**.

02. ***Respuesta del cuestionario*** *y envío de evidencias*

Tras la tierización realizada internamente por Natura, el proveedor recibirá un cuestionario con preguntas sobre la seguridad de la información del proveedor.

El proveedor deberá:

Responder íntegramente al cuestionario de seguridad;

Garantizar la veracidad y claridad de la información;

Adjuntar evidencias obligatorias que comprueben los controles declarados.

Las respuestas afirmativas sin evidencias válidas serán consideradas como no conformes.

El plazo para la respuesta es de hasta 15 días, considerando hasta 3 interacciones de cobro, con plazos adicionales de 5 días cada una.

03. ***Análisis** técnico*

Natura realizará el análisis de las respuestas y evidencias con enfoque en:

- Gobernanza y conformidad;
- Controles técnicos y organizacionales de seguridad;
- Adherencia a las políticas y requisitos corporativos.

El plazo estándar de análisis es de **hasta 5 días hábiles**. Si hay necesidad de complementación, el SLA será pausado y reiniciado después de una nueva presentación.

04. *Plan de acción*

Cuando sea aplicable, el proveedor recibirá:

- ***Resultado** de la evaluación y nota de conformidad;*
- ***Plan de acción** para la mitigación de riesgos identificados;*
- ***Plazos acordados** para la implementación de los controles pendientes.*

Criterios de Clasificación:

Categoría	Porcentaje de gaps	Status
A	0% - 19%	Aprobación directa
B	20% - 39%	Aprobación directa
C	40% - 55%	Aprobación por excepción
D	56% - 79%	Rechazo
E	80% - 100%	Rechazo

Los plazos para la implementación de los planes de acción siguen la criticidad de los riesgos:

Muy alto: hasta 2 meses
Alto: hasta 3 meses
Moderado: hasta 4 meses
Bajo: hasta 5 meses

05. ***Responsabilidades** del proveedor*

natura

El proveedor se compromete a:

- **Rellenar** el cuestionario de forma completa y veraz;
- **Suministrar** evidencias claras, organizadas y actualizadas;
- **Mantener** coherencia entre la información declarada y los documentos enviados;
- **Involucrar** áreas internas relevantes (TI, Seguridad, Jurídico, Privacidad);
- **Cumplir** los plazos establecidos;
- **Mantener** canales de comunicación activos durante todo el proceso.

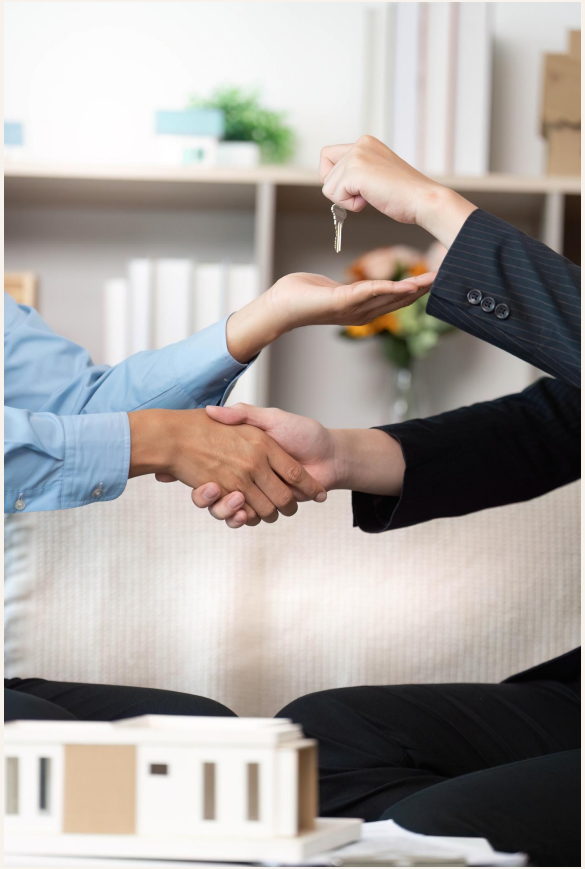
Las evidencias solicitadas pueden incluir, pero no se limitan a:

- **Políticas** y normas internas;
- **Matrices** de riesgo e informes de vulnerabilidad;
- **Procedimientos** de control de acceso;
- **Evidencias** de capacitaciones y concientización;
- **Documentação** de desenvolvimento seguro (DevSecOps);
- **Planes** de respuesta a incidentes y continuidad;
- **Informes** de DPIA y gobernanza de privacidad.

Las declaraciones sin comprobación documental serán tratadas como **ausencia de control.**

***Responsabilidad** compartida*

***La protección de la información y las operaciones** es una responsabilidad conjunta. La actuación colaborativa, transparente y continua entre Natura y sus proveedores es **esencial** para garantizar la seguridad, la continuidad de las operaciones y la conformidad legal.*



Seguridad es continuidad

El cumplimiento de estos requisitos fortalece la asociación, reduce los riesgos operativos y contribuye a la resiliencia y competitividad del proveedor en el mercado.

Soporte y comunicación

Las dudas relacionadas con el proceso de evaluación deben ser dirigidas al canal informado en la invitación de debida diligencia o a:

tprm_cyber@natura.net

natura


natura