Estándares de Ciberseguridad para Proveedores

Sección A –Todos los proveedores

Se espera que TODOS los proveedores cumplan con los estándares de ciberseguridad definidos a continuación.

1. Los proveedores deben ser capaces de demostrar que están sensibilizados con los asuntos de ciberseguridad dentro de su organización. Esto incluye, entre otros:
   I. Pruebas de la adopción de un estándar de ciberseguridad reconocido (por ejemplo, los que se incluyen en Cyber Essentials).
   II. Formación de los empleados en materia de ciberseguridad, incluido un programa continuo de mejora.
   III. Copias de seguridad sólidas; políticas de respuesta ante incidentes; planes de recuperación en caso de desastres, etc.

2. El phishing y malware puede proceder de proveedores en riesgo. Por lo tanto, los proveedores deben demostrar que cuentan con sistemas de ciberseguridad sólidos. Entre ellos:
   I. Sistemas de correo electrónico que utilicen la autenticación multifactor u otras medidas de protección, por ejemplo, DMARC.
   II. Procesos instaurados para garantizar una notificación activa y temprana en caso de que el proveedor detecte que sus sistemas están en riesgo o han sufrido phishing.

3. En caso de phishing o malware, procedentes del proveedor y detectados por INEOS Inovyn, debe existir una ruta clara de derivación al proveedor.

4. El fraude financiero suele intentarse mediante correos electrónicos interceptados que solicitan al destinatario la modificación de sus datos bancarios. Como parte de la Política antifraude de INEOS Inovyn, los proveedores deben contar con un proceso claramente establecido mediante el cual notifiquen a INEOS Inovyn los cambios legítimos, con contactos designados a los que INEOS Inovyn pueda recurrir para hacer comprobaciones independientes a fin de confirmar la validez.

5. Los proveedores que almacenen datos relacionados con INEOS Inovyn deben garantizar que dicho almacenamiento cumple con los requisitos legales en materia de protección de datos de cada país, incluido:
   I. Cumplimiento del Reglamento general sobre protección de datos (RGPD) o equivalente.
   II. Cifrado completo de los datos de INEOS Inovyn almacenados en dispositivos portátiles, como los ordenadores portátiles.

6. Obligación de uso de mecanismos adecuados y seguros para transferir software o datos como parte del trabajo del proveedor, por ejemplo:
    I. Un sitio seguro de SharePoint en el host de INEOS Inovyn.
    II. Un sitio seguro de transferencia de archivos proporcionado por el proveedor acreditado por INEOS Inovyn.

7. Los dispositivos de transferencia masiva, como las unidades/dispositivos USB, solo deben emplearse cuando no existan otros mecanismos prácticos y deben, en todos los casos, cumplir con las políticas y comprobaciones de INEOS Inovyn en el momento de usarse.

Sección B –Proveedores de sistemas y recursos que trabajan en los sistemas de INEOS Inovyn

Además de la sección A, TODOS los proveedores de sistemas, equipamiento y recursos que trabajen en sistemas de INEOS Inovyn deben garantizar que se cumplan los siguientes requisitos adicionales.

8. Los sistemas suministrados y cualquier equipamiento remarcado deben utilizar plataformas respaldadas por el proveedor con una vida útil estimada de 5 años. Se incluyen aspectos como:
    I. Sistemas operativos (SO).
    II. Firmware;
    III. Dependencia de los componentes, exploradores web y aplicaciones de terceros.

9. Los sistemas proporcionados deben poderse **actualizar para hacer frente a futuras vulnerabilidades**, por ejemplo:
    I. Aplicación periódica de parches del sistema operativo.
    II. Aplicación de actualizaciones de versiones del sistema operativo.
    III. El proveedor debe exponer su procedimiento de comprobación y aprobación de parches, por ejemplo, la duración de la fase de aprobación del proveedor y consideraciones especiales para parches especialmente importantes.

10. Los sistemas suministrados deben tener capacidad de ciberprotección, con medidas como:
    I. Protección antivirus básica.
    II. Protección mediante la inclusión en lista blanca de aplicaciones.
    III. Protección avanzada contra malware.
    IV. Protección de la red mediante dispositivos de firewall.
    V. El proveedor no debe haberse identificado por el gobierno como inherentemente inseguro en el plano cibernético y, por lo tanto, sujeto a restricciones.

11. Si a un proveedor se le otorga acceso remoto a los sistemas de INEOS Inovyn, dicho acceso solo deberá utilizarse para el fin previsto y únicamente a los sistemas identificados en el ámbito del servicio, el acuerdo de nivel de servicio, etcétera:

I. dicho trabajo debe acordarse con INEOS Inovyn antes de que se realice y debe estar sujeto a una revisión periódica (anual, como mínimo).

12. En caso de que se otorgue acceso remoto a cualquier parte de los sistemas INEOS Inovyn, pueden ser necesarios requisitos adicionales, como:
    I. Únicamente personas designadas, con posible comprobación de antecedentes, prueba de formación, sustitutos designados, etcétera;
    II. Autenticación de dos factores realizada por INEOS Inovyn.

13. En caso de que los proveedores proporcionen recursos en lugar de sistemas a INEOS Inovyn, se espera que todos los recursos funcionen conforme a las directrices de INEOS Inovyn en materia de ciberseguridad, tanto en nuestras instalaciones como en otro lugar siempre que se realice un trabajo relacionado con INEOS Inovyn. Dichas directrices normalmente se comunicarían como parte del proceso de incorporación a INEOS Inovyn.

FIN DEL DOCUMENTO

V1. Agosto de 2020