RESUMEN DE LAS MEDIDAS DE SEGURIDAD DE HP

Para garantizar la protección de los datos de los clientes, HP cumple con un riguroso conjunto de controles de seguridad de la información que incluyen políticas, prácticas, procedimientos y estructuras organizativas diseñadas para proteger la confidencialidad, la integridad y la disponibilidad de su información y la de sus clientes (incluidos la información personal, tal como se define en los Anexos de procesamiento de datos y clientes de HP). A continuación, se presenta una descripción general de las medidas técnicas y organizativas de seguridad implementadas por HP en toda la compañía.

1. Política de seguridad

   HP mantiene políticas, estándares y procedimientos aplicables a nivel mundial con el propósito de proteger los datos tanto de HP como de sus clientes. Los detalles de las políticas de seguridad de HP son confidenciales para resguardar la integridad de los datos y sistemas de HP. Sin embargo, a continuación se incluyen resúmenes de nuestras políticas clave.

2. Organización de seguridad de la información

   El programa de seguridad de la información de HP está diseñado para dirigir y mantener la estrategia y los controles de seguridad de la información de la organización. Este sistema garantiza el cumplimiento de las políticas y controles de seguridad de HP en toda la empresa, así como la conformidad con los requisitos de seguridad de sus clientes. Estructurado en consonancia con los marcos, las leyes y las normativas de ciberseguridad estándar de la industria, el Marco se somete a una revisión anual con el fin de adaptarse al panorama de amenazas en constante evolución que enfrenta HP.

3. Gestión de riesgos de ciberseguridad

   El programa de gestión de riesgos de ciberseguridad de HP tiene como objetivo preservar la confidencialidad, la integridad y la disponibilidad de sus activos de información. El programa proporciona un enfoque coherente para la identificación, evaluación, priorización, tratamiento, solución, seguimiento y reporte de los riesgos de ciberseguridad. HP define su apetito de riesgo como el nivel aceptable de exposición a pérdidas y su tolerancia al riesgo como el grado de variación respecto a este apetito. Los riesgos se evalúan mediante una metodología definida, lo que permite a HP mitigar los riesgos de seguridad de la información a un nivel aceptable. Este programa se alinea con el proceso de gestión de riesgos empresariales de HP.

4. Seguridad de RR. HH.

   La política de seguridad de Recursos Humanos de HP garantiza la seguridad de la información durante todo el ciclo laboral de los empleados mediante el establecimiento de procesos para el acceso a instalaciones, sistemas de información y otros activos. Esto incluye la obtención de reconocimientos por escrito a través de acuerdos de confidencialidad y no divulgación, así como la realización de procedimientos de verificación de antecedentes. Todos los aspirantes a empleo en HP deben completar una verificación de antecedentes conforme a las leyes, regulaciones y normas éticas pertinentes.

5. Gestión de activos

   HP cuenta con un proceso para identificar activos de información técnica, clasificar activos críticos y mantener procedimientos de manejo documentados para cada tipo de clasificación de información, incluidos aquellos que contienen información personal. Estos procedimientos cubren el almacenamiento, la transmisión, la comunicación, el acceso, el registro, la retención, la destrucción, la eliminación, la gestión de incidentes y la notificación de infracciones. Las políticas y estándares de seguridad de HP también exigen la eliminación segura de medios.

6. Seguridad de la información

   El programa de seguridad de datos de HP describe las prácticas de seguridad y los controles técnicos que se deben implementar para proteger la confidencialidad, autenticidad e integridad de los datos. Los requisitos legales, el valor, la criticidad y la sensibilidad a la divulgación o modificación no autorizada son algunos de los factores que determinan cómo se clasifica la información en virtud de la política de seguridad de datos de HP. Además de los procedimientos de manejo de datos, la política describe el cifrado, la eliminación, la recopilación y el procesamiento de datos, la retención, el respaldo y la prevención de pérdida de datos.

7. Control de acceso

   HP emplea el principio del mínimo privilegio para el control de acceso lógico, proporcionando acceso al usuario a través de ID de usuario y contraseñas únicas. La política de contraseña define los controles de complejidad, la solidez, la validez y los controles del historial de contraseñas. Los derechos de acceso se revisan periódicamente y se revocan tras la salida del personal. Se implementan procedimientos acordados para la creación y eliminación de cuentas de usuario con el propósito de otorgar y revocar el acceso a los sistemas del cliente durante las contrataciones.

8. Criptografía

   HP ha definido un conjunto de procesos sólidos para la criptografía con el fin de garantizar la confidencialidad, la integridad y la disponibilidad de los activos de información. Los protocolos aprobados requieren el cifrado de determinados activos, incluidos aquellos que contienen información personal. Nuestro programa de criptografía involucra el uso de técnicas matemáticas para asegurar la información y las comunicaciones, lo que garantiza que solo las partes autorizadas puedan acceder a los datos. Un componente fundamental del programa de seguridad de la información de HP es proteger los datos contra el acceso no autorizado y la manipulación.

9. Seguridad física y medioambiental

   Las instalaciones de HP están protegidas mediante diversos controles de acceso físicos y electrónicos, como guardias de seguridad, control de acceso electrónico y circuitos cerrados de televisión (CCTV). Las instalaciones también cuentan con el soporte de infraestructura necesario, que incluye controles de temperatura y sistemas de respaldo de energía, empleando sistemas de alimentación ininterrumpida o generadores diésel para garantizar el funcionamiento de los servicios críticos. Todo el personal de HP está registrado y debe portar las credenciales de identificación adecuadas.

10. Gestión de operaciones

    HP ha establecido requisitos mínimos de endurecimiento para la infraestructura tecnológica, que abarcan estaciones de trabajo, servidores y equipos de red. Estos dispositivos emplean imágenes de sistemas operativos preendurecidos, cuyos requisitos varían según el sistema operativo y los controles implementados. Asimismo, HP ha implementado sistemas de detección y prevención de intrusiones en la red (NIDS/NIPS) que se supervisan y administran de manera continua, las 24 horas del día, los 7 días de la semana.

11. Seguridad de las comunicaciones

    La seguridad de las comunicaciones garantiza la protección de la información dentro de las redes corporativas. Esto incluye la instalación y administración de componentes de seguridad en la red (p. ej., firewalls), la segregación de redes, así como controles de filtrado web y gestión de correos electrónicos. Además, implica la supervisión y gestión de canales de comunicación para detectar y prevenir accesos no autorizados o infracciones de datos.

12. Seguridad de los sistemas

    La política de HP exige una metodología de desarrollo seguro para sistemas y software durante todo su ciclo de vida. El ciclo de vida del desarrollo de software abarca la iniciación, el desarrollo/adquisición, la implementación, las operaciones y la eliminación. Todos los componentes del sistema se evalúan en función de su impacto en la seguridad general. HP ha establecido controles para las transacciones de servicio de aplicaciones, que incluyen la validación de credenciales de usuario, firmas digitales, cifrado, protocolos de comunicación segura y el almacenamiento de los detalles de las transacciones dentro de la zona de seguridad de red adecuada. También se realizan regularmente análisis internos de vulnerabilidades.

13. Terceros y subcontratistas

    HP cuenta con procesos para seleccionar subcontratistas que cumplan con rigurosos requisitos de seguridad contractual. Para los proveedores pertinentes que manejan datos de HP o de los clientes, o que acceden a la red de HP, el equipo de ciberseguridad de HP lleva a cabo una evaluación de riesgos con el fin de verificar la existencia de un programa de seguridad de la información que incluya medidas de seguridad físicas, técnicas y administrativas. Esta evaluación es necesaria antes de que el proveedor pueda acceder a la información de HP.

14. Gestión de incidentes de seguridad de la información

    HP dispone de un proceso completo de gestión de incidentes cibernéticos que describe el propósito, el alcance, las funciones, las responsabilidades, el compromiso de gestión, la coordinación organizacional, los procedimientos de implementación y la verificación del cumplimiento. Este proceso se revisa y actualiza anualmente. El equipo de respuesta a incidentes cibernéticos, que incluye personal del equipo de ciberseguridad de HP capacitado en respuesta a incidentes y gestión de crisis, lleva a cabo revisiones regulares del proceso y de cualquier incidente o evento.

15. Gestión de la continuidad del negocio

    El programa global de continuidad de operaciones de HP garantiza la continuidad integral a través de procesos de planificación colaborativos, estandarizados y documentados. La empresa ejerce periódicamente sus planes de continuidad comercial para garantizar su efectividad, probando y actualizando todos los planes al menos una vez al año. Además, todo el personal involucrado en el plan de continuidad comercial recibe la capacitación adecuada.

16. Cumplimiento

    El cumplimiento da forma al enfoque de HP para cumplir con las expectativas legales, contractuales e internas de un programa de seguridad de la información eficaz. Las revisiones periódicas de seguridad de la información garantizan que los protocolos estén integrados en las operaciones de cada grupo empresarial. El proceso de revisión también mantiene los documentos actualizados para reflejar las obligaciones legales actuales a medida que evolucionan los requisitos.

17. Industria de tarjetas de pago

    El marco de la industria de tarjetas de pago (PCI) orienta el enfoque de HP para lograr el cumplimiento de PCI, definiendo las responsabilidades comerciales y los controles de seguridad conforme al estándar de seguridad de datos para la industria de tarjetas de pago (PCI DSS). Al instalar y mantener controles de seguridad de red, como firewalls, HP garantiza el cumplimiento de los requisitos de cumplimiento de PCI.

18. Seguridad de los productos de HP

    La seguridad de los productos de HP abarca prácticas esenciales para proteger los productos HP, como la firma de código, la gestión de vulnerabilidades de seguridad de los productos, la emisión de boletines de seguridad y la notificación de problemas de seguridad de productos. Estas medidas garantizan que los productos HP sigan siendo seguros y confiables para los usuarios. La seguridad de los productos es de suma importancia para HP, ya que ayuda a mantener la confianza de los clientes y a protegerse contra posibles amenazas.

19. Seguridad de los servicios de HP

    La seguridad de los servicios de HP comprende prácticas fundamentales para resguardar los servicios brindados a los clientes de HP. Esta política abarca diversas áreas de la seguridad de los servicios, incluidos entornos alojados en la infraestructura de HP, por terceros, por socios y por clientes. Estas medidas garantizan que los servicios de HP se mantengan seguros y confiables para los usuarios. Al implementar prácticas de seguridad sólidas, HP garantiza la seguridad e integridad de sus productos y servicios, fomentando un entorno seguro y confiable para todos los usuarios.