CYBER-SECURITY COMPLIANCE

Guía sobre el cumplimiento de regulaciones de seguridad con Panda Adaptive Defense

pandasecurity.com

panda

En los últimos años, han ido surgiendo diferentes **regulaciones y normativas gubernamentales**, y en algunos casos sectoriales, con el objetivo de asegurar que las empresas **almacenen y manipulen**, con la debida diligencia, la **información personal y sensible** de sus clientes.

1. ¿Qué regulaciones y normativas afectan a las empresas?

Algunas de estas normativas están adaptadas al tipo de sector donde las organizaciones desarrollan su actividad, siendo las siguientes algunas de las más destacadas:

General Data Protection Regulation (GDPR).

Regulación generalista, obligatoria para cualquier empresa que recopile datos de carácter personal de cualquier ciudadano de la Unión Europea.

Payment Card Industry Data Security Standard (PCI-DSS).

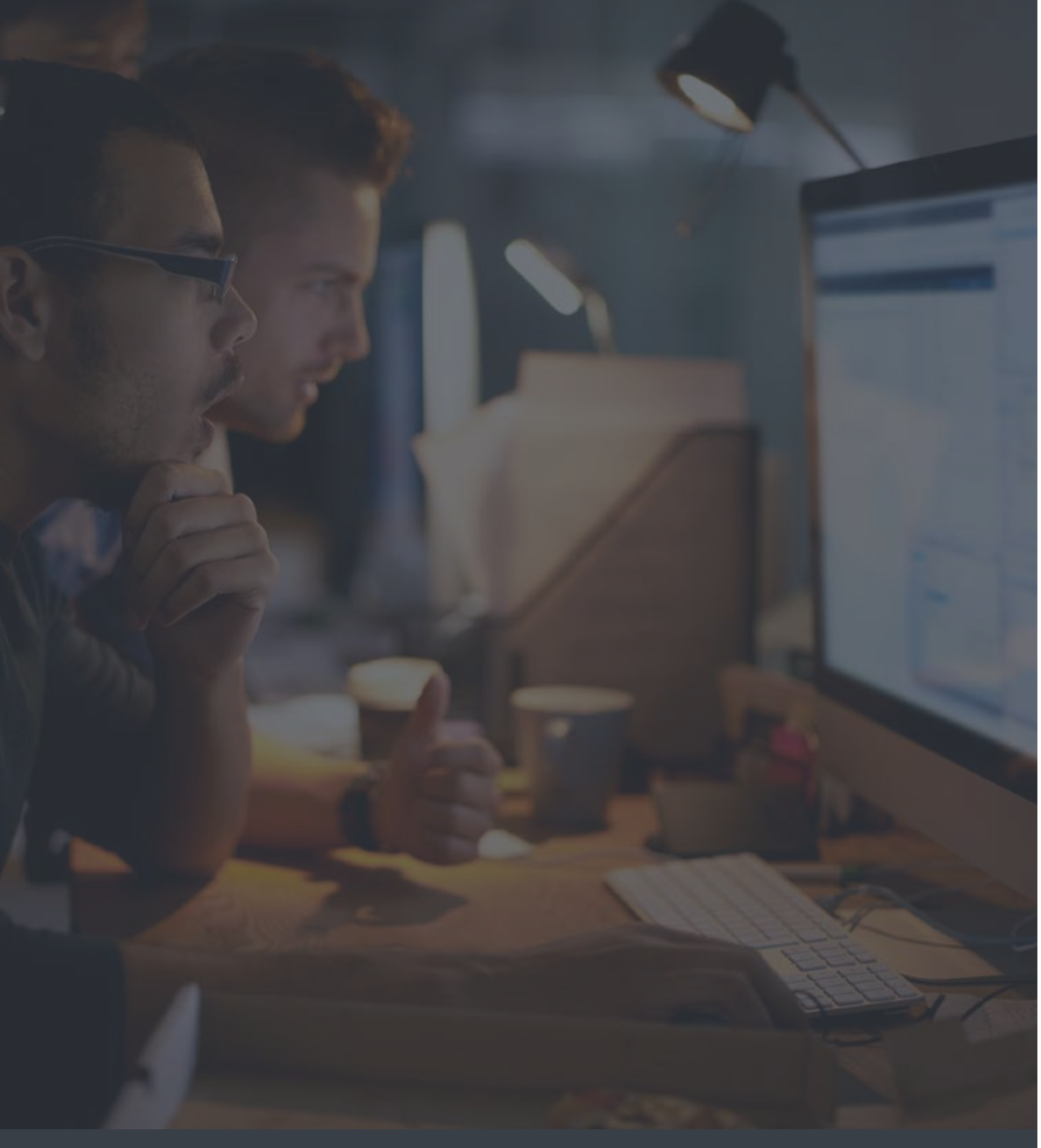
Aplica a comercios, e-commerce, entidades bancarias y colaboradoras que almacenan o tratan datos de tarjetas de pago.

Health Insurance Portability and Accountability Act (HIPAA).

Ley federal de EEUU que aplica al sector sanitario y organizaciones que almacenen u operen con información médica electrónica.

Sarbanes-Oxley (SOX)

Afecta a las empresas que cotizan en la bolsa de valores de Nueva York (EE.UU) y sus filiales, de fraudes contables. Aunque en casos específicos también afecta a empresas privadas.



La posibilidad de ser objeto de **ataques internos o externos** que comprometan los datos personales y sensibles de clientes y organizaciones, así como la obligatoriedad de **registrar cada acceso** y operación que se realiza sobre estos, obliga a que las organizaciones adopten fuertes **medidas de protección** de sus datos, y así evitar o minimizar, entre otras, las siguientes implicaciones:

- **Multas y sanciones** por su incumplimiento, que pueden ser muy significativas.
- **Costes** derivados de los análisis e investigaciones forenses en caso de fuga de datos.
- **Pérdida de confianza** por parte de clientes, colaboradores y empleados, como consecuencia de una brecha o exfiltración de datos personales.
- Además del impacto negativo en la **reputación** de la empresa, su **competitividad** y el **riesgo** que ello conlleva para su negocio.

2. ¿Cómo ayuda Panda Security en el cumplimiento de las regulaciones?

Estas regulaciones están diseñadas para garantizar la confidencialidad, integridad y seguridad de los datos personales o corporativos en los que se focalizan cada una de ellas. Para ello, todas ellas se centran en 3 áreas clave:

- **Seguridad** de los datos personales o corporativos que se crean, reciben, almacenan o transmiten.
- **Privacidad** de los datos personales, centrándose en los protocolos para acceder, transmitir y compartir estos datos.
- **Notificación de violaciones de datos** a las instituciones que velan por el cumplimiento de estas regulaciones, independientemente de cuando se produjo la violación, lo que obliga a la retención de logs para recuperación en caso de ser necesario.

El porfolio de soluciones de seguridad avanzada de Panda Security, Panda Adaptive Defense y Panda Adaptive Defense 360 y sus módulos adicionales Advanced Reporting Tool, Data Control y SIEMFeeder ayudan a las empresas en el cumplimiento de estas regulaciones, ya que se ofrece de base una monitorización continua de la actividad en el **endpoint**, entre otros de la actividad con ficheros creados, almacenados, operados y en tránsito en los puestos de trabajo y servidores protegidos. En concreto:

Panda Adaptive Defense y Panda Adaptive Defense 360

Son **soluciones de seguridad avanzada** para equipos, portátiles y servidores de empleados o colaboradores, cuyo objetivo es proteger contra cualquier tipo de amenaza: conocida, avanzada, zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless.

Todo esto es posible por su enfoque de seguridad único, cuyo pilar fundamental es el de asegurar que solo las aplicaciones que son confiables para Panda Security se ejecuten en los equipos y servidores, monitorizando y **supervisando continuamente la actividad** de cualquier aplicación y procesos que se ejecute.

Este **modelo de protección avanzada** cubre, con máxima eficiencia, todas las fases en la seguridad adaptativa que toda organización debe adoptar: desde la **Prevención y Detección** hasta la **Respuesta continua** a incidentes y amenazas y su **Remediación**. Ofrecer estas capacidades de forma transparente y sin inconvenientes en las organizaciones, es solo posible gracias a los servicios gestionados de clasificación del 100% de las aplicaciones y el servicio de **threat hunting e investigación de ciber-ataques** (THIS) que estas soluciones incluyen.

Para saber más acerca de **Panda Adaptive Defense Platform** y sus Servicios Gestionados, accede a: https://www.pandasecurity.com/intelligence-platform/

Panda Data Control[1]

Es un módulo adicional de **Panda Adaptive Defense y Panda Adaptive Defense 360**, ofrece herramientas de control y supervisión ante la pérdida o exfiltración de datos de carácter personal desestructurados que se encuentran en los puestos de trabajo y servidores, tanto dentro como fuera de la red corporativa, gracias a su **capacidad de descubrir datos de carácter personal o sensibles**. Además monitoriza en tiempo real las acciones realizadas y el comportamiento de los usuarios sobre estos datos.

Panda Data Control presenta la información descubierta, en tiempo real o pasada, en dashboards e informes pre-configurados, que pueden ser adaptados a las necesidades de cada organización, simplificando así las auditorías, la revisión de las políticas de acceso a los datos y la gobernanza de datos.

Advanced Reporting Tool (ART)

Es un módulo adicional de las soluciones de seguridad avanzadas de Panda Security, **almacena y correlaciona**, de forma desatendida, la información de la actividad en los puestos de trabajo y servidores junto con su contexto y datos enriquecidos generados por la Plataforma de Panda Adaptive Defense.

Esta plataforma de visualización y reporting es **100% cloud**, evitando inversiones adicionales en almacenamiento, mantenimiento y procesamiento. Además, los datos son retenidos hasta un año, permitiendo así acceder a la información retrospectivamente, y respondiendo a las disposiciones de las regulaciones que requieran poner en conocimiento de las autoridades el detalle de cualquier acceso o violación de datos en el pasado.

El módulo de SIEMFeeder

Permite a las organizaciones con un **SIEM on-premise**, alimentarlo en tiempo real con los eventos de los endpoints y enriquecidos por la plataforma de Panda Adaptive Defense. Los responsables de seguridad de las organizaciones establecerán las políticas de retención de logs necesarias para el cumplimiento de las regulaciones que les afectan.

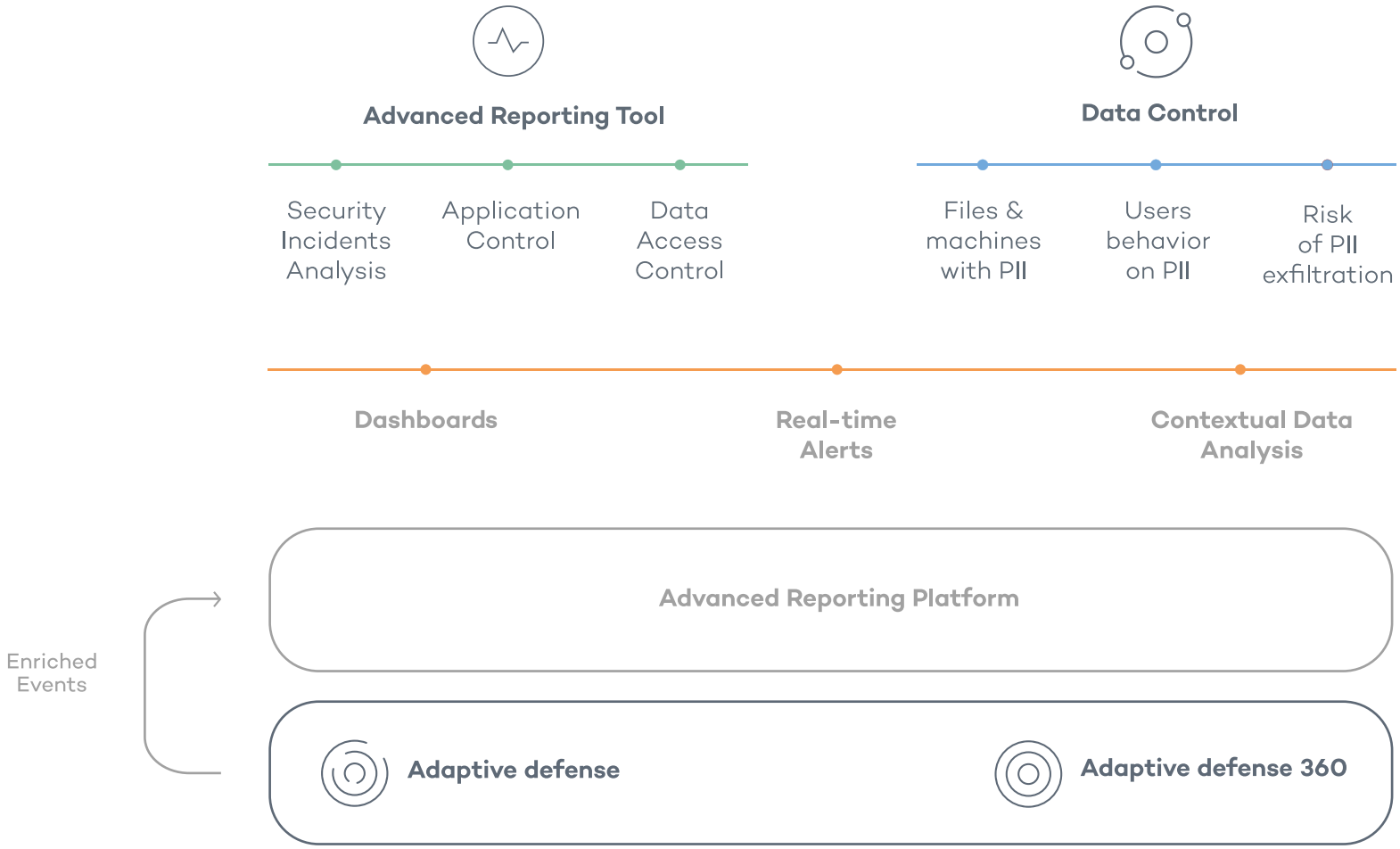
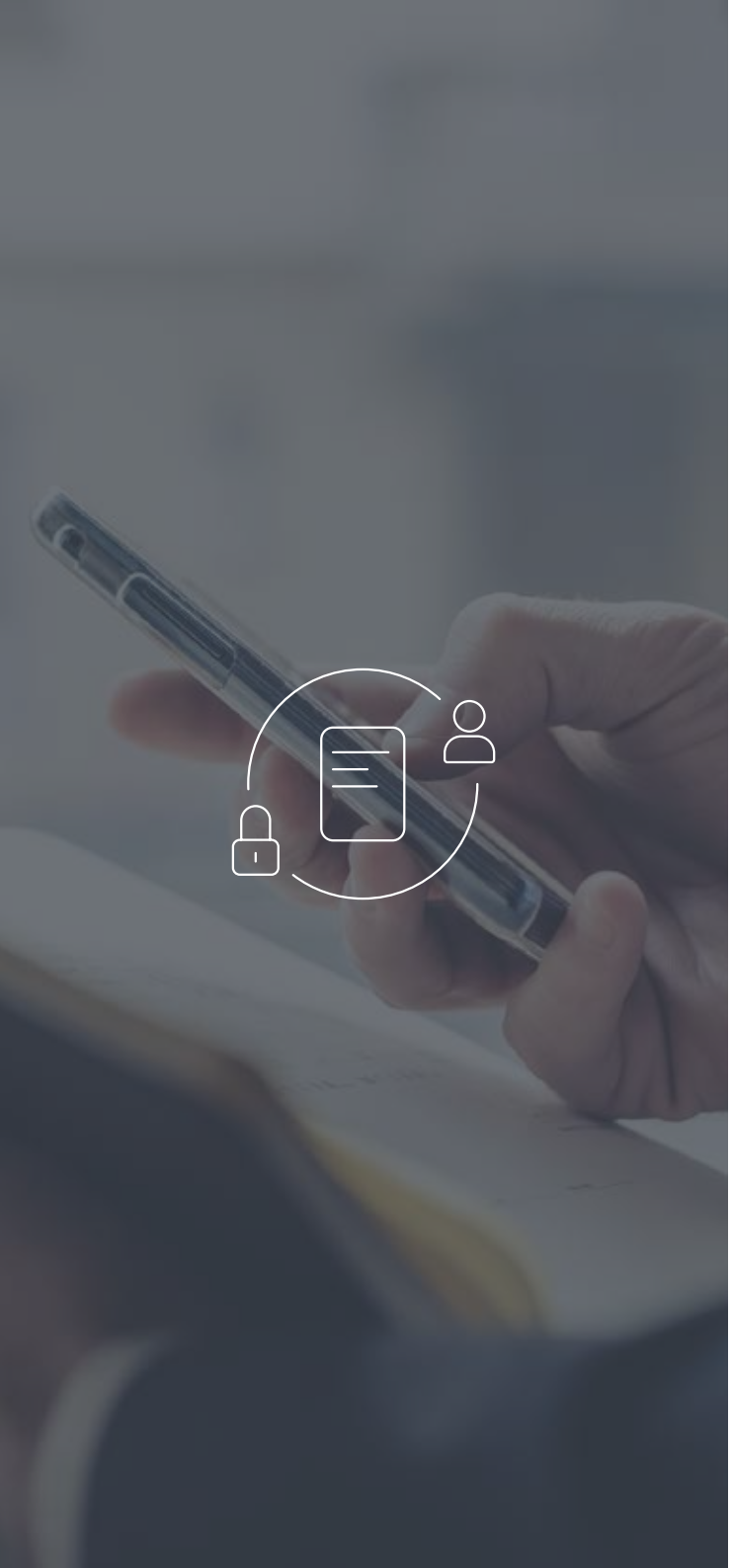


Figura 1. La Plataforma de **Panda Adaptive Defense** protege contra las ciber amenazas, monitorizando la actividad de las aplicaciones y procesos en los puestos de trabajo y servidores. **Advanced Reporting Tool** y **Panda Data Control** ofrecen información de valor en áreas como seguridad, optimización IT, control de la productividad y ayuda al cumplimiento de regulaciones, gracias a esa visibilidad.



3.A General Data Protection Regulation (GDPR)

¿Qué es?

Es el marco legal de protección de datos personales en toda la UE, cuyo objetivo es devolver el control a los ciudadanos sobre sus datos personales, imponiendo reglas estrictas sobre su ubicación, accesibilidad y tratamiento. La regulación entra en vigor en Mayo del 2018.

¿A quién afecta?

La GDPR impacta a todas las empresas, independientemente de a qué industria o región pertenezcan, incluso a aquellas fuera de la UE, que recopilan y almacenan datos de carácter personal de ciudadanos de la UE.

¿Qué efectos tiene para mi empresa?

Su incumplimiento acarrea severas multas, pudiendo llegar a los 20M€ o el 4% de la facturación anual y efectos reputacionales muy perjudiciales para las empresas.

¿Cómo ayuda Panda Security a las empresas en el cumplimiento de esta regulación?

A continuación indicamos los artículos de la regulación en los que Panda Adaptive Defense y sus módulos ayudan a las organizaciones en su cumplimiento.

Seguridad del tratamiento Artículo 32

Panda Adaptive Defense y Panda Adaptive Defense 360, protege contra cualquier tipo de amenaza: conocidas, avanzadas, zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless mediante un de enfoque de seguridad, basado en permitir solo la ejecución de las aplicaciones que son confiables para Panda Security y denegándoselo al resto, evitando así cualquier intento de violación de seguridad, incluido el robo o pérdida de información en los puestos y servidores protegidos.

Panda Data Control descubre y monitoriza en tiempo real los datos de carácter personal e información sensible en los puestos de trabajo y servidores. Proporciona herramientas que permiten identificar accesos no permitidos a los datos personales por parte de los empleados y colaboradores de la organización.

Notificación de violaciones de la seguridad de los datos personales a la autoridad de control. Artículo 33

Panda Adaptive Defense y Panda Adaptive Defense 360, ante una violación de seguridad o un proceso desconocido en los puestos y servidores, notifica inmediatamente a los administradores de seguridad, vía correo electrónico, detallando todas las acciones realizadas por la amenaza descubierta en la red corporativa.

Si la amenaza llegó a ejecutarse en algún momento en el parque, la consola de Panda Adaptive Defense mostrará el ciclo de vida del ataque, si ha accedido a ficheros de datos y que ha hecho con estos (exfitración, copia, etc). Esta información es fácilmente explotable a ficheros, accedida en **Advanced Reporting Tool**, e integrada en el SIEM corporativo gracias al módulo **SIEMFeeder**.

Los informes pre-configurados y personalizables de **Panda Data Control**, están enfocados a mostrar las aplicaciones, operaciones y ficheros relacionados con una posible exfiltración de datos de carácter personal como DNI, teléfono, domicilio, nombre, apellidos, etc. Esta información, es crítica a la hora de notificar una violación de seguridad.

Evaluación de impacto relativa a la protección de datos Artículo 35

Panda Data Control permite conocer la cantidad, tipología, volumen y uso de datos personales en los puestos de trabajo y servidores, de tal manera que se pueda realizar una evaluación de impacto y de riesgo en el tratamiento de la información. Los informes y paneles de los apartados anteriores, también aplican a este artículo.

Funciones del delegado de protección de datos (DPO) Artículo 39

Panda Data Control proporciona informes y paneles predefinidos y configurables según las necesidades requeridas por el DPO, ayudando a este último, al desempeño de sus funciones y a la evaluación del impacto relativo a la protección de datos.

3.B Payment Card Industry Data Security Standard (PCI DSS)

¿Qué es?

PCI DSS es el estándar mundial de seguridad de datos de la industria de tarjetas de pago, creado para ayudar a las empresas a procesar los pagos de forma segura, reducir el fraude y proteger los datos confidenciales de los titulares de tarjetas.

¿A quién afecta?

Esta regulación afecta tanto a usuarios, como a bancos e intermediarios financieros, que almacenen, transmitan o procesen datos del titular de la tarjeta, generalmente en el sector retail (plataformas eCommerce y negocios de venta al público).

¿Qué efectos tiene para mi empresa?

Su incumplimiento implica multas de hasta $500.00 por incidente, pudiendo ser acumulables.

¿Cómo ayuda Panda Security a las empresas en el cumplimiento de esta regulación?

Panda Security ayuda en el cumplimiento de PCI DSS a través de las buenas prácticas expuestas a continuación:

Implementar y Mantener unos sistemas y una red corporativa seguros

Panda Adaptive Defense y Panda Adaptive Defense 360, son soluciones de protección avanzadas que protegen contra cualquier tipo de amenaza: conocidas, avanzadas, zero-day, ransomware y ataques de seguridad fileless (en memoria) y malwareless.

Panda Adaptive Defense 360, incluye firewall personal, IPS/IDS, anti-spam, anti-spam en correo, filtrado y categorización en navegación web y control de dispositivos, entre otras técnicas de seguridad preventiva que ayudan a reducir la superficie de exposición a ataques.

Proteger los datos del titular de la tarjeta

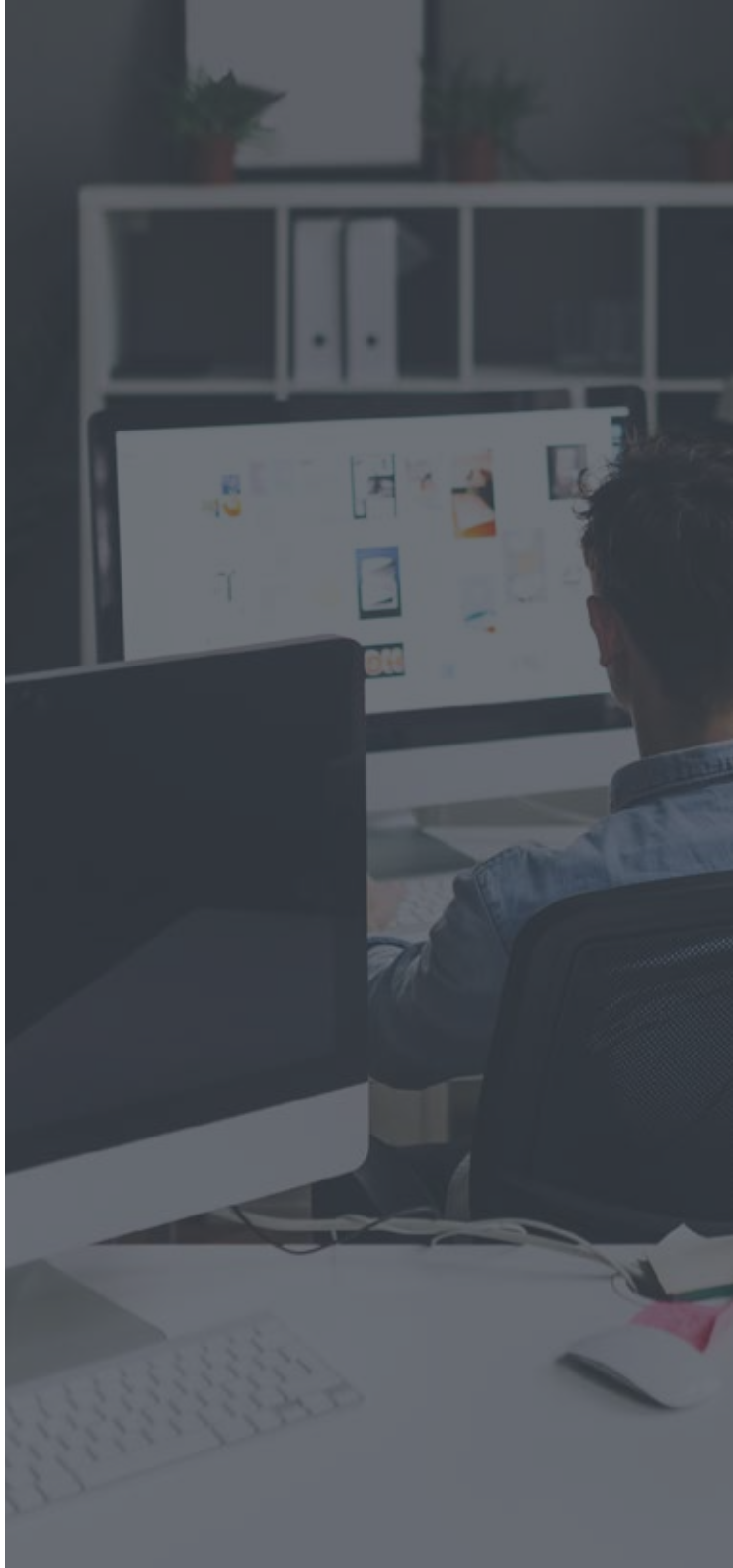
Panda Data Control descubre la ubicación de datos relativos a tarjetas de pago y cuentas bancarias en ficheros desestructurados en los puestos de trabajo y servidores, monitorizando en todo momento, las operaciones que se hacen sobre estos ficheros. Esta información es clave para definir e implementar **medidas en el control de acceso** y operación sobre los datos de carácter personal objeto de esta regulación: Identificadores del titular, tarjeta de crédito y cuenta bancaria.

Mantener un programa de gestión de vulnerabilidades

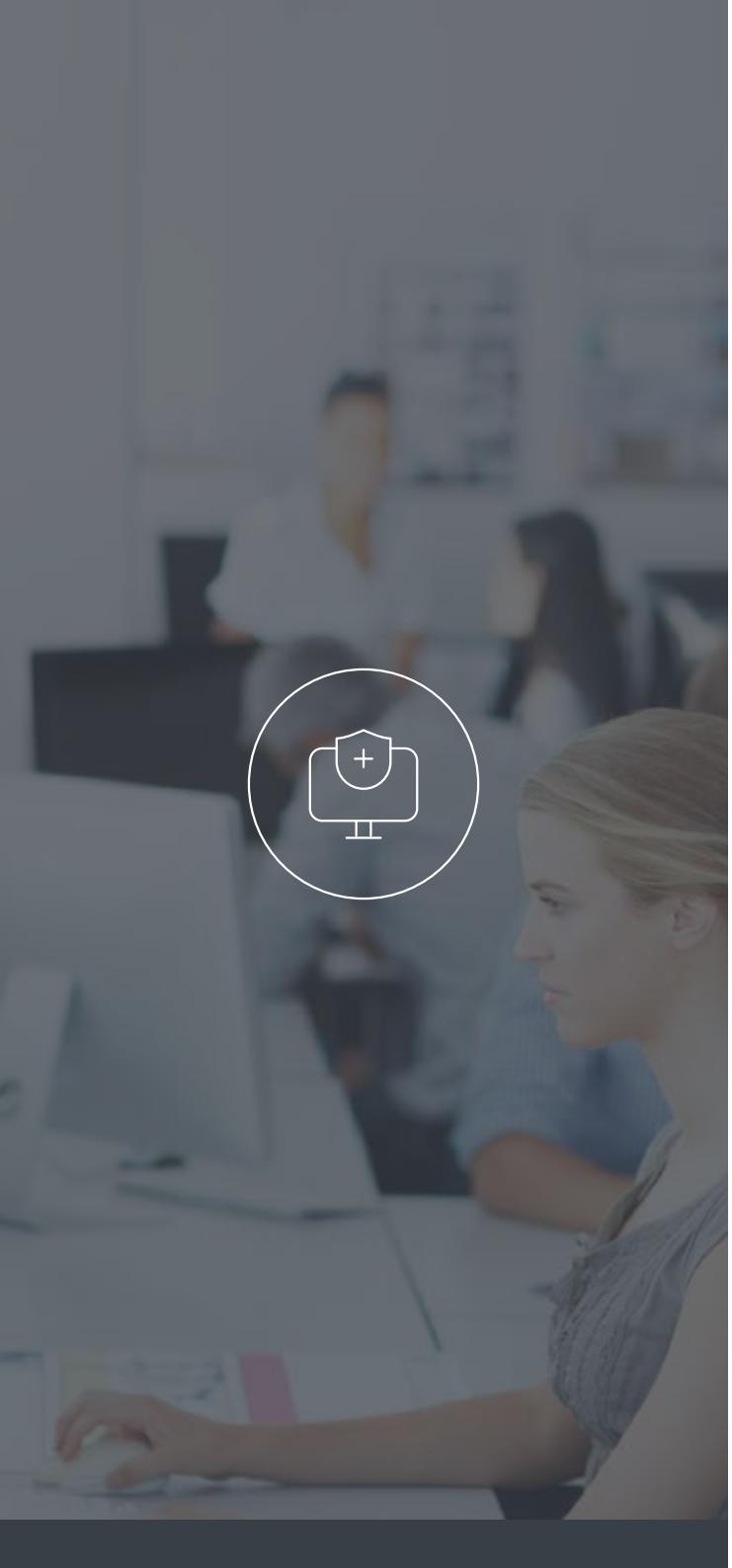
Gracias a la monitorización continua de Panda Adaptive Defense y Panda Adaptive Defense 360, su módulo opcional **Advanced Reporting Tool** incluye informes sobre las aplicaciones vulnerables instaladas y las aplicaciones vulnerables ejecutadas en los puestos de trabajo y servidores. Esta información ayuda a los equipos de IT y seguridad en su tarea de gestión de vulnerabilidades.

Implementar medidas de control de acceso sólidas

Panda Data Control monitoriza todos los accesos y operaciones que se realizan sobre ficheros con datos relativos a tarjetas de pago y cuentas bancarias. Esta información se presenta en **paneles de control e informes pre-configurados** que pueden ser adaptados a las exigencias de cada organización.



panda



3.C Health Insurance Portability and Accountability Act (HIPAA)

¿Qué es?

Esta Ley Federal de los EE.UU. establece una serie de normas para salvaguardar la información personal sanitaria electrónica (ePHI[2]) almacenada, accedida, o compartida por empresas del sector sanitario u organizaciones afines, como aseguradoras que tratan datos médicos.

Las organizaciones que no operan en el mercado de EE.UU, no se verán afectados por las obligaciones de HIPAA, sin embargo, las disposiciones de la legislación europea son similares, siendo las de la HIPAA criterios válidos de aplicación general.

¿A quién afecta?

Esta regulación afecta al sector sanitario y a cualquier organización afín, como aseguradoras médicas que almacenen u operen con información personal de salud electrónica.

¿Qué efectos tiene para mi empresa?

Su incumplimiento puede acarrear grandes multas de hasta $1,5 millones al año y, en casos extremos, incluso la pérdida de licencias médicas y entrada en prisión.

¿Cómo ayuda Panda Security a las empresas en el cumplimiento de esta regulación?

Panda Security ayuda en el cumplimiento de HIPAA a través de las buenas prácticas expuestas a continuación:

Panda Adaptive Defense y Panda Adaptive Defense 360

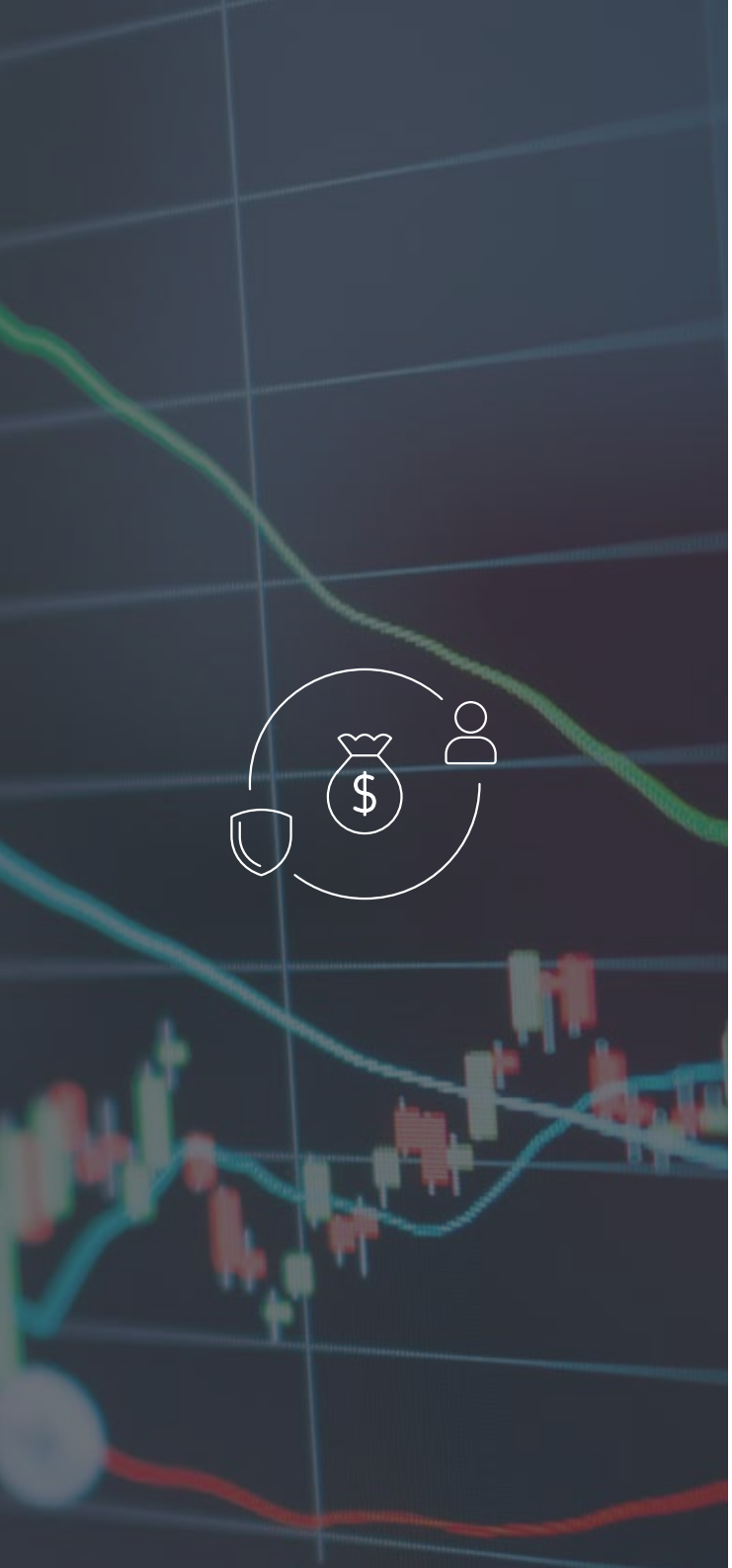
- Garantiza la **seguridad** de toda la información de salud protegida electrónicamente que se **crea, recibe, mantiene o transmite** en los puestos de trabajo y servidores protegidos, protegiendo contra cualquier tipo de amenaza, conocida o desconocida. Sección 164.306
- Habilita la **implementación de procedimientos de revisión periódica** de la actividad de los sistemas, informes de acceso e informes de seguimiento de incidentes de seguridad. Sección 164.306
- Protege, detecta e informa de **software malicioso** en el parque. Secciones 164.308 (a) (5) (ii) (B)
- Previene y mitiga **incidentes de seguridad con software malicioso** conocidos y desconocidos; reduciéndolos drásticamente, prácticamente a cero. En el caso en que llegarán a ejecutarse, la capacidad de detección mediante la monitorización del comportamiento de estos los **identifica y bloquea**, minimizado sus efectos. Secciones 164.308(a)(6)(ii)
- Permite **documentar incidentes de seguridad y sus resultados**, gracias a la monitorización continua de la actividad de las aplicaciones y procesos en los puestos de trabajo, portátiles y servidores, propio de las **soluciones de seguridad EDR** (Endpoint Detection & Response). Sección 164.312 (b)
- Ofrece **información detallada** de las acciones realizadas por el atacante durante el incidente de seguridad tanto en la consola, como en las notificaciones por correo electrónico, permitiendo así a la organización responder al requerimiento de **notificar con el máximo detalle** por quién, cómo y cuándo se ha accedido a la **información personal sanitaria**. 45 CFR 164.404 (b)

Advanced Reporting Tool y SIEMFeeder

- Ayuda en la **gestión de vulnerabilidades**, ofreciendo información de las aplicaciones vulnerables instaladas y ejecutadas. Sección 164.308(a)(1)(ii)(B)
- Registra, con una retención de 1 año, los **intentos de inicio de sesión** en los equipos y servidores protegidos para así reportar anomalías. 45 CFR 164.308 (a) (6) (ii)

Panda Data Control

- Identifica el **incidente de seguridad** en el que datos de tipo personal están involucrados, indicando el fichero, su ubicación, etc. De esta forma, es posible **identificar los ataques a ficheros** con datos personales sanitarios y notificar del incidente debidamente. Sección 164.404(b).
- Permite identificar los **accesos** por empleados y colaboradores sin autorización a este tipo de información y notificar de la irregularidad de forma pertinente. Sección 164.404(b).



3.D Sarbanes-Oxley (SOX)

¿Qué es?

Esta Ley federal de la EE.UU tiene como objetivo evitar fraudes y riesgo de bancarrota, protegiendo al inversor de empresas que cotizan en bolsa. La Ley requiere que las organizaciones afectadas implementen controles internos y se protejan ante la revelación de datos confidenciales y la alteración de estos con objeto fraudulento.

La ley, que se promulgó en el año 2.002, nace como reacción al caso Enron Creditors Recovery Corporation, cuyo fraude contable llevó a esta compañía estadounidense, líder mundial eléctrica, de gas natural, papelera y de comunicaciones a la bancarrota en el 2.001 y que afectó duramente a sus empleados y accionistas.

¿A quién afecta?

SOX afecta a empresas que cotizan en bolsa NYSE (Bolsa de Nueva York), así como a sus filiales. También hay una serie de disposiciones de la Ley que se aplican a las empresas privadas, por ejemplo, la destrucción voluntaria de pruebas para impedir una investigación federal.

¿Qué efectos tiene para mi empresa?

En caso de incumplimiento la empresa responsable se enfrentaría a multas que ascienden hasta los $5 millones, o incluso penas de hasta 20 años de cárcel.

¿Cómo ayuda Panda Security a las empresas en el cumplimiento de esta regulación?

Panda Security ayuda en el cumplimiento de SOX a través de las secciones expuestas a continuación:

Sección 404 - Evaluación de la gestión de los controles internos

Panda Adaptive Defense y **Panda Adaptive Defense 360** permiten identificar los puestos de trabajo y servidores que o bien, no están siendo protegidos o bien, tienen algún problema operativo que puede provocar malfuncionamientos de la protección. De esta forma la organización puede establecer controles periódicos de estos estados para mitigar su riesgo.

Sección 409 - Revelación de cambios en condiciones financieras u operativas

A nivel de seguridad, **Panda Adaptive Defense 360, Advanced Reporting Tool** y **Panda Data Control,** notifican en tiempo real sobre los incidentes de seguridad cuya ejecución se haya bloqueado y en el caso de que el atacante hubiera podido realizar alguna acción, como ganar persistencia, acceder a ficheros, movimientos laterales, etc, los detallará minuciosamente, permitiendo a la organización responder al requerimiento de notificar con el máximo detalle sobre por quién, cómo y cuándo se ha accedido a la información en los puestos y servidores.

Sección 802: Penas criminales para el que altere documentos

Panda Data Control monitoriza las operaciones de creación, modificación, apertura, borrado, renombrado, copiado y pegado que los usuarios realizan sobre los ficheros con datos personales, permitiendo identificar acciones de alteración de ficheros, así como quién, cuándo y desde dónde se realizaron.

---

1. Comercializado en los siguientes países: España, Suecia, UK, Francia y Alemania.

2. Existen 18 tipos de información de ePHI, incluidos nombres de pacientes, direcciones, números de Seguridad Social, correos electrónicos, huellas dactilares o imágenes fotográficas. Cualquier registro médico actual o pasado está sujeto al mismo grado de protección

panda

Adaptive Defense 360

Más Información en:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

panda