Política de Administración de seguridad de la información
(para uso público y externo)

Referencia de control de documentos ISO 27001: 5.1
Número de versión: 1.0
Fecha de revisión: 31 de agosto de 2015

Objetivo

El propósito de esta política es definir controles para una administración o supervisión efectiva de todas las actividades de seguridad de la información realizadas por Pearson. Estas reglas se establecen para proteger a los usuarios*, a Pearson y a nuestros clientes. El uso inapropiado de los sistemas expone a Pearson y a los usuarios de Pearson a riesgos entre los que se incluyen ataques de malware, poner en peligro los servicios y los sistemas de redes, asuntos legales, y abusos de confianza para con nuestros aprendices y clientes.

Resumen

Nuestro objetivo es establecer una política que promueva y sea coherente con nuestros valores fundamentales: ser valientes, imaginativos, decentes y responsables con nuestros accionistas y los unos con los otros. La Oficina del Director de seguridad de la información (CISO, por sus siglas en inglés) tiene el compromiso de proteger a los usuarios* de Pearson, a sus socios comerciales, a sus clientes y a la compañía contra actividades ilegales o dañinas perpetradas por individuos ya sea a sabiendas o involuntariamente.

La seguridad efectiva es un esfuerzo de toda la compañía que incluye la participación y el apoyo de cada usuario y afiliada de Pearson que maneja información o sistemas de información. Es responsabilidad de cada usuario de tecnología de la información leer y comprender todas las políticas, y desarrollar sus actividades en consecuencia.

La estrategia de Administración de seguridad de la información de Pearson se basa en el Marco ISO 27001.

Alcance

Esta política se aplica a todos los usuarios y negocios de Pearson con el fin de proteger los sistemas, las solicitudes y la información de Pearson, inclusive a todos los servicios contratados o alojados.

Política

Programas de seguridad

a. **Programa de seguridad de la información:** Pearson implementará un programa de seguridad de la información completo por escrito que asegure los activos de información de Pearson de forma tal que se adecue al valor de cada activo según lo establecido por el análisis de impacto en el negocio, la evaluación de riesgos y las medidas de mitigación.

b. **Programa de privacidad de la información:** Pearson implementará un programa de privacidad de la información completo por escrito que proteja la información personal de identificación (PII, por sus siglas en inglés) de los clientes y los usuarios de Pearson contra la divulgación y el uso no autorizados.

c. **Dirección y soporte del programa de seguridad:** La administración de Pearson brindará una capacitación de concienciación sobre seguridad, una orientación clara y soporte gerencial visible para las iniciativas de seguridad.

d. **Recursos de seguridad de la información:** La administración de Pearson asignará un nivel de recursos y atención del personal para abordar la seguridad de los sistemas de información que sea acorde con el nivel de riesgo para la seguridad evaluado, la probabilidad de que suceda y su posible impacto.

e. **Requisitos contractuales, leyes y regulaciones:** Los requisitos de control para el programa de seguridad de la información de Pearson garantizarán el cumplimiento de todos los requisitos reglamentarios y estatutarios pertinentes. Los controles del programa también identificaran las deficiencias en el cumplimiento contractual y garantizarán las disposiciones y resoluciones pertinentes.

Requisitos de los procedimientos y Política

a. **Políticas de seguridad de los activos de información:** Se implementarán y harán cumplir las políticas para garantizar la seguridad, la confiabilidad, la integridad y la disponibilidad de los activos de información de Pearson.

b. **Procedimientos y procesos de seguridad de los activos de información:** Se implementarán y harán cumplir los procesos y procedimientos para garantizar el cumplimiento de las Políticas de seguridad de Pearson.

c. **Normas de seguridad de los activos de información:** Pearson desarrollará normas de seguridad de la información según sea necesario para respaldar la aplicación de las políticas de seguridad de la información.

Sanciones de la Política

a. Sanciones de la Política: Pearson implementará sanciones para encargarse de los usuarios que infrinjan las políticas.

Proceso de excepción

a. **Proceso documentado de excepción a la Política:** Pearson mantendrá un proceso documentado para supervisar y aprobar las excepciones a los procedimientos y las políticas de seguridad de la información.

b. **Excepciones a las políticas:** Los usuarios presentarán una solicitud por escrito para pedir excepciones a las políticas de seguridad de la información. Dichas excepciones se aprobarán de conformidad con el Proceso de excepción y se gestionarán para su cumplimiento.

c. **Revisión de las excepciones documentadas a la Política:** Todas las excepciones documentadas y aprobadas de la política de seguridad de Pearson incluirán una fecha específica en la cual la excepción caducará, y se aplicará la política. Mensualmente se revisará el estado de estas políticas para aplicar medidas correctivas y para asegurar su cumplimiento en la fecha especificada.

Distribución de la Política

a. **Distribución de documentación de la Política de seguridad:** La administración de Pearson publicará por escrito las políticas de seguridad de la información y las pondrá a disposición de todos los usuarios y las partes externas implicadas.

b. **Reconocimiento de las Políticas de seguridad:** Todos los usuarios de Pearson revisarán y reconocerán la aceptación y el cumplimiento de la Política de uso aceptable, y su gerente les suministrará todas las demás políticas relevantes para sus funciones laborales.

Revisión de la Política

a. **Revisión anual de la documentación de la Política de seguridad de la información:** Todas las políticas de seguridad de la información de Pearson se revisarán de forma anual.

Revisión del programa de seguridad

a. **Revisión anual del programa:** La administración revisará formalmente la efectividad del programa de seguridad de la información de Pearson como mínimo de forma anual por medio de las evaluaciones del alcance de riesgos.

b. **Informe a la Junta directiva sobre la estrategia anual de seguridad de la información:** El CISO preparará un informe sobre la estrategia anual para la Junta directiva, describiendo los medios por los cuales los esfuerzos internos de seguridad de la información soportan las directivas de estrategias comerciales, los objetivos comerciales actuales y los principales proyectos de la organización.

c. **Revisiones del control del sistema de información:** De manera periódica, se obtendrá una revisión independiente de la seguridad del sistema de información a fin de determinar tanto la idoneidad como el cumplimiento de los controles. Estas revisiones pueden estar a cargo de terceros externos cualificados, así como de la auditoría interna de Pearson.

Coordinación de la seguridad de la información

a. **Seguridad de la información centralizada:** Todas las políticas, los procedimientos y las actividades de seguridad de la información son guiadas y dirigidas bajo la autoridad del CISO.

b. **Coordinadores de la seguridad de la información:** Cada Línea de negocio será responsable de designar un coordinador o coordinadores en los niveles correspondientes dentro de la organización. Estos coordinadores se encargan de apoyar al CISO con la implementación, el mantenimiento y la elaboración de informes sobre los requisitos de seguridad de la información de toda la organización.

Asignación de responsabilidades en la seguridad de la información

a. **Definición de las funciones de seguridad específicas:** Pearson definirá las funciones de trabajo específicas necesarias para la implementación efectiva del programa de seguridad de la información de Pearson. Cada función incluirá una descripción específica de las tareas relacionadas con la seguridad de la información desempeñadas por cada miembro del equipo que lleve a cabo dichas funciones laborales.

b. **Responsabilidades departamentales:** Pearson definirá los requisitos de seguridad de la información específicos para cada departamento principal o función administrativa.

c. **Asignación clara de la responsabilidad para los controles internos:** La administración de Pearson asignará y documentará claramente la responsabilidad para cada control interno en Pearson. Esta responsabilidad incluirá la transparencia suficiente para que la administración se mantenga informada sobre la eficacia y la eficiencia de estos mismos controles internos.

Comunicación con las autoridades

a. **Comunicación con las agencias de orden público:** Todas las decisiones sobre la participación de las agencias de orden público en problemas o incidentes con la seguridad de la información estarán a cargo de un funcionario corporativo de Pearson en colaboración con el CISO, el Departamento Legal de Pearson y Comunicaciones Corporativas.

Seguridad de la información en la Gestión de proyectos

a. **Arquitectura de seguridad de los sistemas de información guidada por la Política:** A fin de garantizar que las metas y los objetivos comerciales se traduzcan correctamente a sistemas de la información, así como a los controles empleados en estos mismos sistemas de información, Pearson aplicará un enfoque de arquitectura de seguridad de los sistemas de información guiado por la política que esté coordinado y administrado por el CISO e integrado al proceso de gestión de riesgos de la seguridad de la información.

b. **Identificación de los requisitos de seguridad:** Antes de que se adquiera o desarrolle un nuevo sistema de información, la administración del departamento usuario involucrado, trabajando junto con el CISO, especificará y documentará de forma clara los requisitos de seguridad pertinentes.

c. **Análisis de impacto en la seguridad de la información:** Cuando se vaya a colocar información sensible en sistemas informáticos adquiridos recientemente, se realizará una evaluación de riesgos del posible impacto relacionado con la seguridad. El CISO revisará los resultados de esta evaluación de riesgos antes de que se compren y desplieguen los sistemas.

Normas y políticas adicionales de Pearson

Las políticas adicionales de Pearson que todos los usuarios deben conocer y respetar se encuentran disponibles en el sitio de Seguridad de la Información Global del CISO.

Sanciones
Pearson empleará métodos lógicos y técnicos para supervisar y auditar en busca de violaciones de las políticas de seguridad de la información y de los controles internos. Los usuarios que violen esta política pueden ser sometidos a acciones disciplinarias que incluyen hasta el cese de la relación laboral. Los individuos, que no sean empleados, que se determine que hayan violado esta política quedarán sujetos a la revocación de su acceso y a la rescisión de su contrato.

Responsabilidad

Pearson
Pearson aplicará las mejores prácticas razonables para hacer cumplir las disposiciones de esta política para la protección de la Confidencialidad, la Integridad y la Disponibilidad de los activos de la compañía.

Director regional/comercial de seguridad de la información
El Director regional/comercial de seguridad de la información es el responsable directo de impulsar el cumplimiento de la Política de seguridad de Pearson y de brindar asesoramiento sobre las mejores prácticas comerciales.

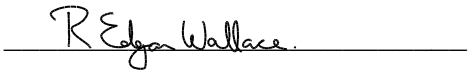
Administración de negocios
Todos los gerentes son directamente responsables de implementar todas las políticas y los controles de Pearson dentro de sus áreas de negocios y de hacer que su personal cumpla con dichas políticas y controles.

Personal
Actuará de manera tal que cumpla con, y apoye, esta política tanto en su contenido como en espíritu, e informará a un supervisor o representante de Recursos Humanos cualquier violación de la política.

Proceso de excepción
Cualquier excepción a la aplicación de esta política, o declaraciones políticas individuales dentro de esta, o a cualquier política de respaldo, requiere una aprobación previa por escrito por parte de la Oficina del CISO. La Gerencia ejecutiva de la organización solicitante debe evaluar y aprobar todas las solicitudes de excepción, con el claro enunciado de su aceptación de cualquier riesgo remanente producto de la excepción.

Aprobación del documento y propiedad
El Director principal de seguridad de la información es el propietario de este documento y es responsable de asegurar que se revise de forma anual. Esta política fue aprobada por la Junta directiva de seguridad ejecutiva de Pearson, y se emite como una versión contralada bajo la autoridad del Director principal de seguridad de la información.

Director principal de seguridad de la información aprobación: Rod Wallace



Fecha de

Historial de modificación

Versión:	Fecha de emisión:	Notas:
1.0	31 de agosto de 2015	Versión original

Definiciones

*"Usuario": usuario hace referencia a cualquier empleado, contratista, consultor, trabajador temporal y otras personas que tengan acceso a la red o los sistemas de Pearson.