Pan American ENERGY

PREMIOS EIKON 2025

CIBERSEGURIDAD: UN COMPROMISO CON LA CONFIANZA Y LA REPUTACIÓN DE PAE

PAN AMERICAN ENERGY |
CAPÍTULO GENERAL

Categoría 02.7
Gobierno Corporativo y Compliance

ÁREA:

- **HR – Communication & Climate**
- **Cyber Security**

RESPONSABLES DEL PLAN DE COMUNICACIÓN:

- **Angel Facundo Vega.** *Governance & Risk & Controls Specialist*
- **Antonella Brusatin.** *Communication & Climate Specialist*
- **Agencia RAN Security**

CIBERSEGURIDAD:
UN COMPROMISO CON LA CONFIANZA Y LA REPUTACIÓN DE PAE.

con el objetivo de fortalecer el conocimiento y prevenir posibles amenazas digitales entre sus colaboradores, Pan American Energy (PAE) lanzó un plan de capacitación en ciberseguridad. A través de una campaña de concientización integral, se buscó educar a más de 4.900 colaboradores de la región en prácticas seguras de manejo de la información.

OBJETIVOS

1 - CONCIENTIZAR SOBRE RIESGOS
educar a los colaboradores sobre los riesgos cibernéticos.

2 - PROMOVER LA CULTURA ORGANIZACIONAL
proactiva en ciberseguridad.

3 - PROTEGER Y GESTIONAR
la reputación corporativa frente a incidentes de ciberseguridad.

4 - MEJORAR LA ACCESIBILIDAD
y comprensión del contenido de ciberseguridad entre sus equipos.

5 - REFORZAR EL CUMPLIMIENTO
normativo y las prácticas de gobierno corporativo.

ESTRATEGIA

> **La campaña se diseñó con una identidad visual que refleje desafío y entrenamiento utilizando elementos deportivos para motivar el aprendizaje.**
> Se implementaron contenidos dinámicos, lúdicos y accesibles para todos los colaboradores, sin barreras tecnológicas.
> **Las publicaciones fueron difundidas a través de múltiples canales: plataforma Smartfense, e-mails, Viva Engage, Microsoft Teams, y materiales visuales en la intranet y screensavers.**

RESULTADOS

17
campañas de sensibilización implementadas.

4.920
colaboradores formados en ciberseguridad.

19
contenidos compartidos incluyendo módulos interactivos, newsletters y charlas.

> **La optimización de la estrategia** permitió duplicar la participación en los cursos.

> **La campaña** fortaleció la cultura organizacional y la protección de los activos digitales y la reputación de

SOMOS PAE

Pan American Energy (PAE) es líder del desarrollo energético sustentable de la región. Es el principal productor, empleador e inversor privado de la industria con presencia en Argentina, Bolivia, Brasil, México, Paraguay y Uruguay. Tiene operaciones de upstream, midstream y downstream.

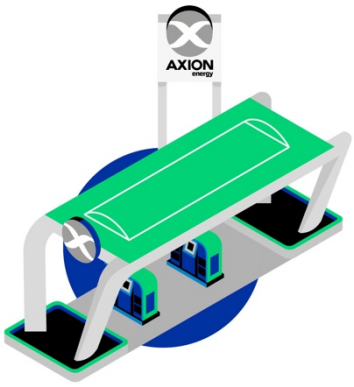
Desarrolla yacimientos de petróleo y gas, posee oleoductos, gasoductos, terminales de petróleo y productos derivados de hidrocarburos. Produce energía eléctrica y participa en el sector de energías renovables.

En el segmento del downstream, opera la refinería más moderna de Sudamérica, ubicada en Campana. Comercializa combustibles con ultra bajo contenido de azufre y lubricantes de máxima calidad, a través de la marca AXION energy. Abastece al público general y a las industrias.

PAE promueve programas que mejoran la calidad de vida de las comunidades cercanas a sus operaciones y la creación de vínculos sólidos y de largo plazo. Durante 2024, 390.000 personas fueron beneficiadas con sus más de 134 programas y actividades de sustentabilidad.

CONTEXTO:

GESTIÓN ESTRATÉGICA DE ISSUES INFORMÁTICOS



En un mundo digital en constante evolución, la información y los datos se han convertido en activos esenciales que definen el éxito y la competitividad de las empresas. En este contexto, **mantener seguro y protegido este activo se establece como un pilar fundamental** y crucial para mantener la confianza, garantizar la continuidad del negocio y evitar riesgos que puedan dañar la reputación corporativa.

Bajo esta premisa, la identificación y gestión proactiva de los issues relacionados a la informática es un ejercicio continuo para las compañías. Los posibles problemas tecnológicos o las brechas de seguridad informática pueden tener un impacto negativo en el desarrollo de sus negocios, afectando la confianza de los consumidores, socios y otras partes interesadas que dependen de la integridad y la estabilidad operativa de la empresa.

Algunos de los problemas más comunes en este ámbito en Argentina y en el mundo son las **fallas en los sistemas,** las **filtraciones de datos** o incluso los **ataques cibernéticos.** Por ello, es imprescindible adelantarse para prevenir, identificar y abordar estos problemas antes de que se conviertan en crisis que puedan dañar la imagen la compañía. Para ello, es clave implementar soluciones tecnológicas robustas y estrategias de comunicación efectiva.

Es así que PAE identificó la necesidad de educar y formar a sus **colaboradores** sobre los **peligros cibernéticos** a los que están expuestos diariamente a la hora de realizar su trabajo. De hecho, este compromiso se encuentra incluido dentro de

la política de responsabilidad de la información de la compañía, que reconoce la importancia de generar **conciencia en ciberseguridad** entre todos los usuarios que utilizan los activos informáticos de la empresa. Este, junto con otras directrices de IT, está alineado con la Política de Seguridad de la Información de PAE, consolidándose como parte esencial de la estrategia organizacional.

EL CASO

En agosto de 2024 PAE lanzó un **plan de capacitación en ciberseguridad** con el objetivo de fortalecer el conocimiento y la prevención de amenazas digitales orientado a más de 4.900 colaboradores. El equipo desarrolló una campaña de concientización con una estrategia integral, asegurando la llegada a todos los públicos con contenido **relevante, accesible y dinámico.**

PÚBLICOS

Todos los colaboradores de PAE en la región (Argentina, Brasil y México).

OBJETIVOS

- **Concientizar y educar a los colaboradores sobre los riesgos cibernéticos.**
- **Promover una cultura organizacional proactiva en ciberseguridad.** Fomentar el aprendizaje continuo en la materia, dentro de la organización, asegurando que los colaboradores adopten hábitos y comportamientos que promuevan la seguridad en el manejo de la información y protección de activos digitales.
- **Proteger y gestionar la reputación corporativa frente a incidentes de ciberseguridad.** Asegurar que todos los colaboradores comprendan el impacto que los problemas de segu-

Un equipo informado en ciberseguridad reduce riesgos y fortalece las barreras de protección de los sistemas organizacionales, así como la privacidad individual de cada usuario, y la reputación de la empresa.

ridad informática pueden ocasionar en la imagen de la empresa, promoviendo una respuesta rápida y adecuada ante posibles brechas de seguridad.

- **Mejorar la accesibilidad y la comprensión del contenido de ciberseguridad.** Toda la comunicación, independientemente de las habilidades tecnológicas de cada colaborador, tiene que ser fácilmente comprensible y accesible para todos, garantizando que el mensaje llegue sin barreras.
- **Reforzar la comunicación interna.** Mantener un flujo constante y coherente de mensajes sobre ciberseguridad eduquen, concienticen y alineen a todos los empleados con los valores y objetivos de seguridad de la organización.
- **Fomentar el cumplimiento normativo y las prácticas de gobierno corporativo en ciberseguridad.** Asegurar que los colaboradores estén comprometidos con las políticas internas y normativas externas de ciberseguridad, promoviendo un ambiente de respeto a los estándares de seguridad, privacidad y regulación.

ESTRATEGIA Y ACCIONES

La campaña de **concientización en ciberseguridad** se desarrolló para reducir los riesgos asociados al factor humano, promoviendo hábitos seguros en el manejo de información y protegiendo los activos digitales y reputacionales de la organización. Para ello, se diseñó una identidad visual basada en el concepto de **desafío y entrenamiento,** incluyendo elementos deportivos característicos para enfatizar la idea de entrenamiento en ciberseguridad, bajo el naming **«CyberawarenessPAE».**

La compañía entiende que, para garantizar el éxito, es fundamental contar con profesionales expertos en la materia. Por eso, PAE llevó adelante esta capacitación en alianza con la **Agencia RAN Security,** su partner estratégico.

La estrategia de que el **contenido fuese dinámico y lúdico,** al plantearlo como un **desafío,** buscó generar un alto nivel de compromiso y aumentar la probabilidad de que los usuarios se sintieran motivados a interactuar. Además, al ser **accesible** todos podían participar más allá de sus habilidades o limitaciones tecnológicas. Este criterio permitió que las piezas de comunicación interna mejoraran la experiencia de los colaboradores. Los módulos de entrenamiento incluyeron además charlas de concientización de 60 minutos con especialistas de RAN Security, disponibles para todos aquellos que desearan aprovechar la oportunidad de capacitarse y profundizar en un tema clave para su desarrollo y la seguridad organizacional.

En cuanto a la implementación de la convocatoria, mensualmente se enviaron e-mails con notificaciones de los nuevos módulos cargados en la plataforma de capacitación **Smartfense.** También se utilizó como canal principal *Viva Engage* -la intranet de PAE- para reforzar la invitación a sumarse a aquella plataforma. Esta forma de comunicación

personalizada, a través de **posteos generados por referentes de ciberseguridad de la compañía,** aseguró que los mensajes sean aplicables a la realidad y tengan en cuenta los riesgos internos de la organización, facilitando que los colaboradores comprendan su importancia y le encuentren utilidad a los nuevos conocimientos en su día a día.

Asimismo, se realizaron publicaciones cada 15 días en Viva Engage con recomendaciones para prevenir ataques informáticos. Está acción se complementa con el material publicado en **carteleras digitales, screensavers y banners de intranet.**

Para asegurar una participación efectiva y maximizar el impacto de la campaña, se optimizaron los formatos de comunicación y la extensión de los contenidos. También se perfeccionaron los correos de asignación y recordatorio, logrando duplicar la cantidad de usuarios que completaron el curso tras la implementación de estas mejoras.

Canales de comunicación:

- ***Smartfense:*** plataforma de capacitación con contenidos segmentados según el perfil del usuario (colaboradores, VP/Managers y contratistas).
- ***E-Mail:*** lanzamiento de Smartfense e invitaciones a charlas de concientización.
- ***Viva Engage:*** publicaciones quincenales con contenidos introductorios sobre ciberseguridad.
- ***Microsoft Teams:*** charlas de concientización de 60 minutos con especialistas.
- ***Intranet y Screensaver:*** banners en Intranet y Screensaver linkeados con QR al desafío en curso.

Además, los módulos incluyeron **14 desafíos** presentados bajo títulos inspirados en el entrenamiento físico como: **«En-**

trena tu privacidad en redes sociales», «Aprende a denunciar phishing», «Aumentá tu resistencia contra amenazas de conexiones inseguras y medios extraíbles», «Conocé los músculos que fortalecen tu seguridad digital», entre otros, los cuales abordaron temas cruciales de ciberseguridad que son altamente relevantes para los participantes a nivel laboral y personal.

Cada desafío no solo educó, sino que también incitó a la **acción inmediata.** Por ejemplo, en el vinculado a la privacidad en redes sociales, se les pidió a los empleados que ajusten la configuración de privacidad de sus propias cuentas, lo que hizo que la información no se quede solo en la teoría, sino que se lleve a la **práctica en su vida digital diaria.**

Asimismo, los desafíos permitieron medir el progreso de los colaboradores a lo largo del tiempo, lo cual resultó útil para identificar qué áreas necesitan mayor atención. Además, este fomentó la protección de los datos personales y la información confidencial de la compañía.

Por otro lado, el enfoque dinámico que se diseñó para los contenidos buscó aumentar la retención de la información y que el aprendizaje se lograra de manera participativa e intuitiva.

Anunciot publicado en Somos PAE

Vega, Angel Facundo
6 feb

Visto por 3196 ···

[CIBERSEGURIDAD] Desafío 13: Entrena tu privacidad en redes sociales

Así como fortaleces tu cuerpo en el gimnasio, también puedes reforzar la seguridad de tus cuentas en redes sociales con estos ejercicios:

🔒 Ajusta la configuración de privacidad

- **Controla quién ve tu información**: Configura tu privacidad para que solo tus contactos aprobados puedan ver tus publicaciones
- **Filtra quién te encuentra**: Restringe quién puede buscar tu perfil y enviarte solicitudes de amistad

🚫 Evita compartir infor... ver más

RESULTADOS

17 campañas

de sensibilización implementadas.

2 charlas

durante el Mes de la Ciberseguridad (noviembre)

4.920

colaboradores internos y externos formados en ciberseguridad.

30%

colaboradores, contratistas y VP/Managers completaron las actividades asignadas.

19 contenidos

compartidos, incluyendo vídeos, módulos interactivos, newsletters y charlas.

Según una encuesta realizada por la Agencia RAN, el tipo de pieza que mejor fue recibida fueron los videos y en segunda instancia los Newsletters. Este último pudo deberse a que no requiere el inicio de sesión en la plataforma externa Smartfense.

Por otro lado, en enero de 2024 se registró una baja de los participantes que completaban los cursos, lo que respondió al periodo de vacaciones, con lo cual, se implementaron mejoras en los contenidos y correos de asignación. Luego de esos cambios, se duplicó la cantidad de usuarios que completaron el curso con respecto al mes anterior (diciembre).

Los resultados reflejan un **enfoque efectivo en la protección de los datos,** lo que a su vez contribuye a salvaguardar la imagen, reputación y gestión de riesgos de PAE. Al mismo tiempo, estas acciones han fomentado una cultura corporativa más consciente de los peligros existentes en el mundo cibernético, fortaleciendo la capacidad de la empresa para prevenir incidentes y proteger su imagen ante posibles amenazas. Estos esfuerzos consolidan **una estrategia integral de la gestión de riesgos,** mejorando la confianza y estabilidad de la organización tanto interna como externamente.

Próximos pasos

A partir de enero de 2025, y en respuesta al feedback recibido, se optimizaron los entrenamientos reduciendo su duración para facilitar su finalización sin afectar la calidad del aprendizaje. Adicionalmente, se seguirá fortaleciendo la comunicación y personalización de los contenidos para incentivar la participación activa de todos los colaboradores.

La ciberseguridad es una responsabilidad compartida. El compromiso de PAE es seguir impulsando la formación y concientización en este tema clave para garantizar un entorno digital seguro.