OlimpIA | Sentry

Cómo crear una cultura de **ciberseguridad** en tu **empresa**

El 95% de los incidentes de ciberseguridad en 2024 involucraron algún tipo de error humano.

Fuente: *IBM X-Force Threat Intelligence Index 2025.*

Cuando pensamos en **ciberseguridad**, es común relacionarlo únicamente con amenazas externas o **ataques** sofisticados. Sin embargo, gran parte de la **protección digital** de una empresa depende de lo que sucede internamente: cómo se organizan los procesos, se toman las decisiones y se gestiona el **acceso a la información.**

Fomentar una verdadera **cultura de ciberseguridad** no es una tarea exclusiva del área de **tecnología**, sino un compromiso colectivo. Cada equipo, sin importar su función, puede aportar a la **protección** de la organización: desde cerrar accesos que ya no se utilizan, hasta reportar comportamientos **sospechosos**. Así, cada persona se convierte en un pilar fundamental para fortalecer la estrategia de **seguridad digital** de la empresa.

Este eBook está diseñado para ayudarte a integrar la **ciberseguridad** en la rutina diaria de tu negocio de manera práctica y efectiva. Y para acompañarte en ese camino, cuentas con OlimpIA Sentry, nuestro portafolio de soluciones diseñado para fortalecer la **protección** de tu empresa, facilitar la gestión de riesgos y promover una cultura digital **segura,** desde adentro hacia afuera.

¿Qué es cultura de ciberseguridad?

Es la manera en la cual una organización aborda los riesgos **cibernéticos** a través de la conciencia, capacitación y acciones de sus colaboradores.

En una organización con una cultura sólida de **ciberseguridad**, cada acción contribuye a proteger la información: compartir archivos de forma **segura**, gestionar accesos de manera responsable y reportar situaciones inusuales hacen parte del compromiso colectivo con la **ConfIAnza Digital.**

De este modo, la **seguridad** se integra naturalmente en las decisiones diarias, permitiendo que cada persona sepa cómo actuar y participe activamente en la solución. Así, la **ciberseguridad** se convierte en una práctica constante que respalda la continuidad y el crecimiento del negocio.

7 señales de que tu empresa necesita fortalecer su cultura de ciberseguridad

¡No siempre hay alertas evidentes! Sin embargo, reconocer las señales es el primer paso para construir una cultura más sólida. Te compartimos algunas situaciones que pueden ayudarte a identificar áreas de mejora dentro de tu empresa:

1

Uso compartido de contraseñas entre compañeros o equipos: aunque puede parecer una solución práctica el uso de credenciales genéricas, este hábito aumenta el riesgo de incidentes de seguridad, dificultando la identificación de accesos. Se sugiere que cada usuario tenga credenciales únicas y nombradas permitiendo una administración más segura y responsable.

2

Accesos a activos tras cambio de rol o salida de un colaborador: es importante revisar, validar y actualizar los permisos de acceso para garantizar que únicamente quienes son parte de la empresa puedan acceder a los sistemas e información.

3

Alertas ignoradas o no reportadas por considerarse un “tema de TI”: cuando los colaboradores no asumen un rol activo en la prevención, cualquier anomalía puede pasar desapercibida aumentando el riesgo. Es importante promover una cultura donde todos detecten y comuniquen a tiempo.

4

Decisiones operativas que no consideran riesgos de seguridad: prácticas como almacenar información sensible en plataformas no autorizadas y enviar datos sin cifrado, pueden comprometer la integridad y confidencialidad de la información. Generar espacios de capacitación con el área operativa y una definición clara de la política de seguridad de la información, apoya decisiones mayormente informadas.

5

Riesgo al centralizar la seguridad en un solo equipo:
delegar únicamente al equipo técnico la gestión de la seguridad limita la capacidad de respuesta e impide involucrar a otras áreas estratégicas de la empresa. Además, cuando quienes administran las plataformas son los mismos que realizan el monitoreo, se corre el riesgo de un conflicto de intereses, al actuar como juez y parte, lo que puede comprometer la objetividad en la identificación y gestión de incidentes.

6

Falta de seguimiento por parte de los líderes:
la participación de los líderes es fundamental para establecer la seguridad digital como una prioridad organizacional, garantizando recursos
y apoyo continuo para su gestión.

7

Uso predominante de herramientas tecnológicas:
apoyarse exclusivamente en soluciones tecnológicas, sin fomentar la formación y desarrollo del criterio de los colaboradores, puede generar una percepción errónea de seguridad. Si bien las herramientas automatizadas son esenciales, siempre debe existir un componente humano capaz de razonar y discernir sobre situaciones que la tecnología por sí sola podría no percibir, especialmente en aspectos de negocio o contexto operacional.

Si varios de estos comportamientos están presentes en tu **empresa** pueden indicar la necesidad de fortalecer la cultura de **ciberseguridad.** Tomar medidas oportunas contribuye a mitigar **riesgos** operativos y prevenir que posibles vulnerabilidades evolucionen hacia exposiciones críticas.

OlimpIA

Te puede interesar:

IA, ciberseguridad e identidad digital: La tríada que está redefiniendo la ConfIAnza digital

Prácticas que construyen una cultura de ciberseguridad efectiva

Una de las formas más efectivas de fortalecer la cultura de ciberseguridad es por medio de la formación de los colaboradores acerca de la responsabilidad individual. Aquí te contamos algunas tácticas que pueden ayudarte en este camino:

Educación y capacitación continua: es importante que de manera periódica se generen espacios de formación en ciberseguridad, con el fin de generar mejores prácticas en pro de la seguridad de la información. Estos deben realizarse acorde con las responsabilidades de cada área.

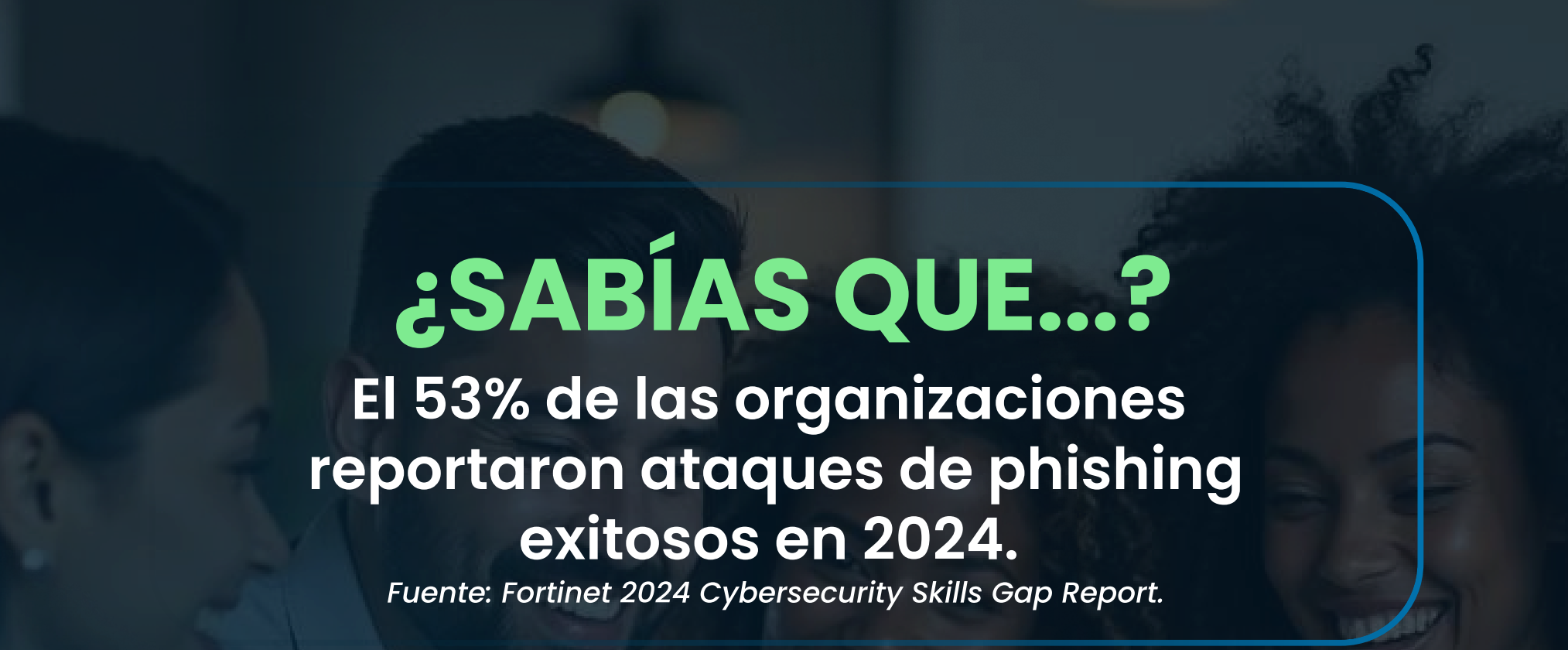
Contenido breve, recurrente y accesible: comparte con los colaboradores cápsulas de video o mensajes enfocados en la cultura de la seguridad digital, permitiendo reforzar conceptos sin interrumpir la productividad.

Integrar métricas del negocio: para que la ciberseguridad sea vista como una prioridad estratégica, es fundamental vincularla con indicadores clave del negocio. La conexión entre los datos y los objetivos estratégicos permite a los equipos tomar decisiones informadas que promuevan prácticas seguras.

Definición de políticas y procedimientos: estas directrices definen el comportamiento del uso seguro de la información, así como los pasos a seguir ante posibles incidentes. Contar con protocolos promueve la coherencia en el actuar, y a su vez facilita la respuesta eficaz ante amenazas, minimizando riesgos operativos.

Evaluación mediante simulaciones controladas: las pruebas de Ingeniería Social permiten medir el nivel de conciencia y preparación del equipo humano frente a amenazas digitales. A través de campañas simuladas de phishing enviadas por correo electrónico, se evalúa la capacidad del personal para detectar, interpretar y responder de manera adecuada.

Estas simulaciones generan aprendizajes valiosos y fomentan una cultura más alerta, consciente y preparada frente a los riesgos reales del entorno digital.



¿SABÍAS QUE...?

El 53% de las organizaciones reportaron ataques de phishing exitosos en 2024.

Fuente: Fortinet 2024 Cybersecurity Skills Gap Report.

Soluciones avanzadas para anticipar, responder y fortalecer la seguridad digital

En OlimpIA entendemos que la ciberseguridad ya no puede limitarse a proteger perímetros estáticos: debe evolucionar constantemente para adaptarse a los cambios del negocio, las tecnologías emergentes y las amenazas cada vez más sofisticadas. Bajo esa visión evolucionamos nuestro CSIRT OlimpIA Sentry, un modelo integral que combina automatización, análisis avanzado e inteligencia contextual para transformar la protección digital en un motor de continuidad, eficiencia y ConfIAnza Digital.

A través de este enfoque, las organizaciones logran anticiparse a posibles ataques, mejoran su capacidad de respuesta y mantienen el control sobre su superficie de exposición en todo momento.

Los **pilares estratégicos** de nuestra propuesta son:

MDR
(Managed Detection and Response):

Monitoreo, detección y respuesta gestionada 24/7, sobre toda la infraestructura tecnológica del cliente. Este servicio combina analítica avanzada, inteligencia de amenazas y automatización para identificar, contener y mitigar incidentes de seguridad de forma rápida, priorizando los eventos realmente críticos y reduciendo tiempos de exposición.

Cyber Threat Intelligence (CTI):

Obtención y análisis de inteligencia de amenazas para anticipar riesgos emergentes que puedan impactar a la organización o sus terceros. Monitoreamos constantemente filtraciones de datos, campañas de phishing, dominios falsos y riesgos de marca, con el fin de entregar alertas tempranas y recomendaciones accionables para proteger la reputación y los activos críticos de la empresa.

Cacería de amenazas (Treath Hunting):

Servicios especializados de búsqueda proactiva de amenazas, orientados a detectar actores maliciosos que podrían evadir controles tradicionales. A través de simulaciones controladas, análisis forense y técnicas de ofensiva ética, identificamos brechas potenciales, optimizamos las defensas y mejoramos la capacidad de resiliencia ante futuros incidentes.

Con este portafolio, desde nuestro CSIRT **OlimpIA Sentry** acompañamos a nuestros clientes no solo a protegerse, sino a generar un verdadero diferenciador competitivo, afianzando la **ConfIAnza** Digital como base para su crecimiento y sostenibilidad.

DATO CURIOSO...

El 59% de los ataques exitosos en 2024 se originaron por errores de configuración o políticas mal aplicadas.

Fuente: Unit 42 Cloud Threat Report, Palo Alto Networks.

En **ciberseguridad,** la verdadera ventaja no proviene solo de la tecnología, sino de cómo se integra en la operación diaria de los colaboradores, por ello, es fundamental aprender a anticiparse, adaptarse y actuar **con precisión.**

OlimpIA | Sentry

En **OlimpIA**, transformamos la **protección** digital en una decisión estratégica que impulsa la continuidad del negocio, fortalece la **ConfIAnza Digital** y convierte cada interacción en una oportunidad para construir un entorno más seguro e **inteligente.**

Conoce más sobre OlimpIA | Sentry