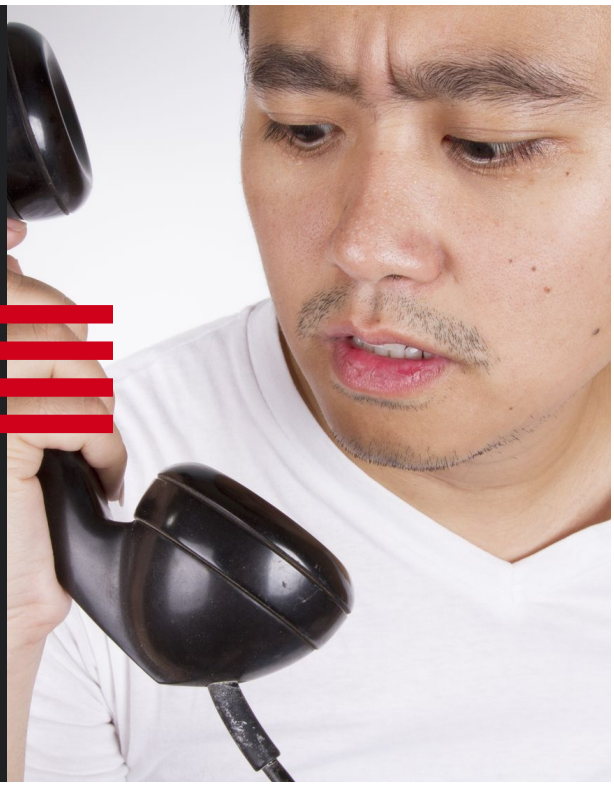
ASLO
INFORMATION TECHNOLOGIES

Estrategia Business Intelligence para la Seguridad Telefónica.

ALCANCES

EXPERTOS EN CIBERSEGURIDAD TELEFÓNICA.

www.aslo.us



SITUACIÓN ACTUAL.

La extorsión virtual, las amenazas a ejecutivos y empleados de cualquier nivel, los intentos de fraude por Ingeniería Social, los ataques a la disponibilidad de los conmutadores y Centros de Contacto, la recepción interminable de llamadas falsas y de origen dudoso, la clonación y el hackeo de las redes telefónicas con fines de robo de información y de llamadas de alto costo; todos estos son problemas que son visualizados, atendidos y mitigados a través de una estrategia de Seguridad Telefónica.

Cualquier empresa está en riesgo, en particular las empresas con instalaciones estratégicas y operaciones de alto perfil. En este sentido, el riesgo puede materializarse de distintas formas y afectar en diversos niveles, desde la vulnerabilidad de procesos internos con fines de fraude, hasta la suplantación de la identidad telefónica de la empresa o la interrupción de operaciones con el objetivo de saturar las líneas telefónicas y liberarlas a cambio de un pago.

Las empresas observan y atienden la seguridad integral desde distintos enfoques dependiendo de su estructura orgánica y del giro principal de negocio, sin embargo, la definición de un objetivo estratégico en común entre las áreas encargadas de la seguridad y el área de finanzas es clave para reducir al mínimo la posibilidad de impacto por amenazas a la seguridad telefónica. De esta forma, el área de TI contará con las prioridades y directrices necesarias para planificar y ejecutar la puesta en producción de los sistemas requeridos.

SOLUCIONES.

Nuestro sistema de Business Intelligence para la Seguridad Telefónica permite a la empresa entender y medir el riesgo de los activos de la empresa y del personal, establecer un programa de concientización, establecer mejores prácticas de seguridad y finalmente, implementar tecnología que automatice el proceso de análisis y mitigación de amenazas telefónicas en tiempo real.

AUDITORIA DE RIESGO

La auditoría de Riesgo Telefónico se lleva a cabo durante un periodo que no excede los 45 días (dependiendo de los alcances y el tamaño de la infraestructura) durante los cuales nuestros expertos colaboran de manera remota con los responsables de Tecnologías de Información, Ciberseguridad, Seguridad Patrimonial, Recursos Humanos y Prevención de Fraude y Aseguramiento de Ingreso para identificar áreas de oportunidad para una efectiva identificación, manejo y mitigación de riesgos en las herramientas de comunicación telefónica y para sentar las bases para una implementación exitosa de nueva tecnología.

CULTURA DE SEGURIDAD

Nuestro grupo de expertos implementa y ejecuta un plan de concientización sobre temas de Ciberseguridad y mejores prácticas en el uso de los teléfonos y los dispositivos móviles cuyo contenido es alineado con los objetivos del negocio. Los asistentes a las sesiones ya sea de manera presencial o en linea, obtienen información real y contundente sobre los posibles escenarios negativos en los que pueden incurrir cuando se ignoran las recomendaciones, tanto en el ámbito personal, como dentro de sus responsabilidades laborales.

SERVICIOS Y TECNOLOGÍA

Nuestros servicio de Voice Security habilita a la empresa para mitigar la recepción de llamadas con fines ajenos a la actividad normal de la organización. Esto incluye el denominado SPAM telefónico el cual se divide en distintas categorías de riesgo de acuerdo con el impacto que pudiera tener sobre la organización (extorsión, fraude o suplantación de identidad, confidencialidad, productividad).

Nuestro sistema BI para la seguridad telefónica protege a la organización ante ataques de denegación de servicio que tienen como finalidad bloquear sus líneas telefónicas para liberarlas a cambio de un pago y ante posibles hackeos que resulten en un abuso indiscriminado de sus troncales telefónicas generando pérdidas de miles de dólares en pocas horas.

De manera inherente, la adopción de nuestro sistema provee métricas que permitirán optimizar la infraestructura y establecer políticas para prevenir el abuso interno de manera transparente y sin entorpecer las operaciones normales del personal.

Nuestra tecnología se integra con la infraestructura telefónica de los clientes situándose en el punto medio entre el proveedor de servicio telefónico y el punto de ingreso a los sistemas de la empresa. De esta manera, asumimos el control sobre las llamadas telefónicas a través de políticas que, alineadas con los objetivos del negocio y con sus lineamientos de operación, analizamos en tiempo real autorizando, monitoreando, midiendo, y en su caso, bloqueando o redireccionando el tráfico que no cumpla con los criterios de aceptación definidos. Además, observando y respondiendo de manera proactiva a cualquier actividad que salga de los rangos normales de operación generando notificaciones electrónicas a nuestro Centro de Operaciones y al personal clave dentro de la organización.

AUDITORÍA DE RIESGO

De manera particular, los resultados de la Auditoría reflejan las oportunidades de mejora y reforzamiento para implementar la estrategia de seguridad telefónica en la organización.

TECNOLOGÍAS DE INFORMACIÓN

El estado de la configuración de seguridad del conmutador, teléfonos y otras funcionalidades avanzadas de telefonía, así como el estado de la configuración de seguridad de la red de datos sobre la que opera la red de colaboración y telefonía.

CIBERSEGURIDAD

El alcance de las políticas de seguridad informática y de información sobre los sistemas de colaboración; el estado de cumplimiento sobre el tratamiento de datos personales, particularmente durante el uso de los sistemas telefónicos y de colaboración y el estado de la configuración de la infraestructura de Ciberseguridad en lo que respecta a la protección de los protocolos y activos que conforman la red de colaboración. El estado de las políticas de administración, control y aseguramiento de dispositivos móviles.

SEGURIDAD PATRIMONIAL

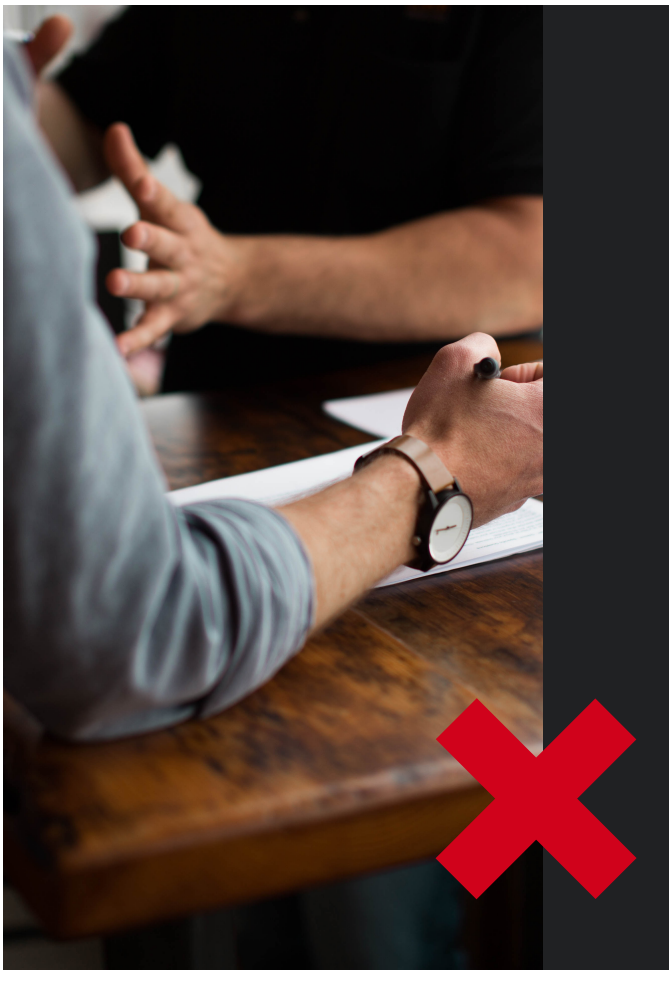
El alcance de la política de Continuidad de Negocio en lo que respecta a la disponibilidad y resiliencia de sus sistemas de comunicación; el grado de preparación de personal en posiciones clave de recepción de llamadas, el alcance de sus procedimientos de recuperación y manejo de crisis durante un evento de ataque cibernético, protesta social o algún otro evento que vulnere la continuidad de las comunicaciones en la empresa.

RECURSOS HUMANOS

La estrategia de formación y educación continua para el personal en general sobre la cultura de la Ciberseguridad en medios electrónicos, teléfonos empresariales, dispositivos móviles y programas de comunicación corporativa respecto a la naturaleza cambiante de estas amenazas.

PREVENCIÓN DE FRAUDE

El estado de los protocolos de identificación y autenticación de usuarios con el objetivo de reducir al mínimo intentos de suplantación de identidad en los centros de atención internos y externos; El estado de las políticas de identificación de actividades alejadas de la ética de la empresa usando los sistemas de comunicación como herramienta para la identificación y prevención.



EXPERTOS EN CIBERSEGURIDAD TELEFÓNICA.

www.aslo.us