SUCCESS

Security Democratized

Secure Universal Creative Cost-saving Efficient Standards for Small Businesses (Estándares seguros, universales, creativos, rentables y eficientes para las pequeñas empresas)

Divulgación ética: Los nombres de los autores y de la universidad se mantienen en anonimato según los requisitos de publicación de investigación. Planeamos y esperamos añadir esa información en la primera mitad de 2024.

Indice

Introducción

La implementación de estándares de seguridad puede ser compleja y costosa, por lo que representa un reto para las pequeñas empresas con recursos limitados. Este artículo aborda dichos retos mediante la investigación de la efectividad de los estándares de seguridad actuales y proponiendo un marco novedoso que se ajuste a las necesidades de las pequeñas y medianas empresas (PYMES). Presentamos el marco de Estándares de Seguridad para Pequeñas Empresas (SUCCESS, por sus siglas en inglés), desarrollado a través de metodologías de investigación rigurosas que comprenden encuestas, entrevistas y pruebas de campo con PYMES. SUCCES significa **S**ecure **U**niversal **C**reative **C**ost-saving **E**fficient **S**tandards for **S**mall Businesses (Estándares Seguros, Universales, Creativos, Rentables y Eficientes para las Pequeñas empresas).

Alcance

El marco de Estándares de Seguridad para Pequeñas Empresas (SUCCESS) está diseñado para ofrecer estándares de seguridad prácticos y optimizados adaptados específicamente al entorno operativo único y a las limitaciones en términos de recursos de las Pequeñas Y Medianas Empresas (PYMES). Este marco pretende abordar las complejidades y cargas financieras asociadas con los estándares de seguridad convencionales, permitiendo a las PYMES establecer y mantener prácticas de seguridad sólidas de manera efectiva.

Público objetivo

El público objetivo de los estándares dirigidos a pequeñas empresas comprende a sus propietarios, operadores y accionistas. Esto incluye emprendedores, gerentes y responsables de la toma de decisiones que supervisan las operaciones diarias y la dirección estratégica de estas empresas. Adicionalmente, se extiende a empleados que desempeñan un papel fundamental en la implementación y cumplimiento de las medidas de seguridad establecidas. Estos estándares están diseñados para satisfacer las necesidades específicas, los recursos y el alcance operativo de las pequeñas empresas, reconociendo sus distintas dificultades y limitaciones. Al dirigirse a este público, los estándares pretender brindar una orientación práctica y accesible para reforzar las medidas de seguridad y proteger la información de carácter confidencial en el contexto de las operaciones de las pequeñas empresas.

Visión general de SUCCESS

A continuación, presentamos la tabla de visión general de SUCCES en dos versiones distintas

A. Versión estándar, basada en investigación y encuestas
B. Edición para nuevos usuarios, en un lenguaje muy sencillo

Luego de diseñar la versión A y mejorar su lenguaje en pro de hacerlo más sencillo, continuamos recibiendo comentarios de que algunos propietarios de empresas podrían no cumplir con algunos requisitos. En lugar de continuar simplificándolo, creamos la versión B para nuevos usuarios o aquellos con poco o ningún conocimiento respecto a las tareas relacionadas con la seguridad.

La razón de que existan las versiones A y B es que, aunque algunos usuarios necesitan una versión muy sencilla, la versión principal aún puede servir a un experto en seguridad o auditor para ayudar y orientar a las pequeñas empresas.

Estándares SUCCESS - Versión principal

GOBERNANZA	La dirección debe apoyar la seguridad, incluyendo la asignación de presupuestos para tal fin
	Debe desarrollarse e implementarse una política de seguridad de la información
CONTROL DE ACCESO	Deben implementarse políticas de contraseñas seguras en conjunto con autenticación multifactor
	Se debe conceder el acceso con base en las funciones y responsabilidades para respetar el principio del mínimo privilegio
GESTIÓN DE ACTIVOS	Se debe recopilar y mantener un inventario de datos
	Los datos se deben clasificar en función de su sensibilidad
SEGURIDAD DE DATOS	Se deben encriptar los datos sensibles
	Se debe garantizar la prevención de filtraciones de datos
RECURSOS HUMANOS	Se debe realizar una verificación de antecedentes penales para todos los empleados y contratistas
	Se debe realizar una capacitación anual específica para cada puesto de trabajo que abarque dificultades de seguridad únicas
SEGURIDAD DEL SOFTWARE	La seguridad debe integrarse en cada etapa del ciclo de desarrollo de software
	Deben implementarse prácticas de programación seguras y revisiones de código
RESPUESTA A INCIDENTES	Desarrollar un plan integral de respuesta a incidentes y ponerlo a prueba
	Establecer funciones y protocolos claros para reportar y remitir a un nivel superior los incidentes de seguridad
GESTIÓN DE VULNERABILIDAD	Debe implementarse un proceso de gestión de parches para manejar los parches críticos
	Deben identificarse y tratarse los riesgos de vulnerabilidad
GESTIÓN DE RIESGOS	Deben identificarse y evaluarse los posibles riesgos para distintos activos
	Deben desarrollarse planes para mitigar estos riesgos
SEGURIDAD FÍSICA	Deben implementarse medidas de seguridad para restringir el acceso físico a las áreas críticas
	Se deben desarrollar políticas integrales de seguridad física para brindar orientación en cuanto a la protección del personal y los equipos
EQUIPO	Se debe designar como jefe de seguridad y cumplimiento a un empleado

Estándares SUCCESS - Versión Para nuevos usuarios

GOBERNANZA	La dirección debe apoyar la seguridad, incluyendo la asignación de presupuestos para tal fin
	Debe desarrollarse e implementarse una política de seguridad de la información
CONTROL DE ACCESO	Deben implementarse políticas de contraseñas seguras en conjunto con autenticación multifactor
	Se debe conceder el acceso con base en las funciones y responsabilidades para respetar el principio del mínimo privilegio
GESTIÓN DE ACTIVOS	Se debe recopilar y mantener un inventario de datos
	Los datos se deben clasificar en función de su sensibilidad
SEGURIDAD DE DATOS	Se deben encriptar los datos sensibles
	Se debe garantizar la prevención de filtraciones de datos
RECURSOS HUMANOS	Se debe realizar una verificación de antecedentes penales para todos los empleados y contratistas
	Se debe realizar una capacitación anual específica para cada puesto de trabajo que abarque dificultades de seguridad únicas
SEGURIDAD DEL SOFTWARE	La seguridad debe integrarse en cada etapa del ciclo de desarrollo de software
	Deben implementarse prácticas de programación seguras y revisiones de código
RESPUESTA A INCIDENTES	Desarrollar un plan integral de respuesta a incidentes y ponerlo a prueba
	Establecer funciones y protocolos claros para reportar y remitir a un nivel superior los incidentes de seguridad
GESTIÓN DE VULNERABILIDAD	Debe implementarse un proceso de gestión de parches para manejar los parches críticos
	Deben identificarse y tratarse los riesgos de vulnerabilidad
GESTIÓN DE RIESGOS	Deben identificarse y evaluarse los posibles riesgos para distintos activos
	Deben desarrollarse planes para mitigar estos riesgos
SEGURIDAD FÍSICA	Deben implementarse medidas de seguridad para restringir el acceso físico a las áreas críticas
	Se deben desarrollar políticas integrales de seguridad física para brindar orientación en cuanto a la protección del personal y los equipos
EQUIPO	Se debe designar como jefe de seguridad y cumplimiento a un empleado