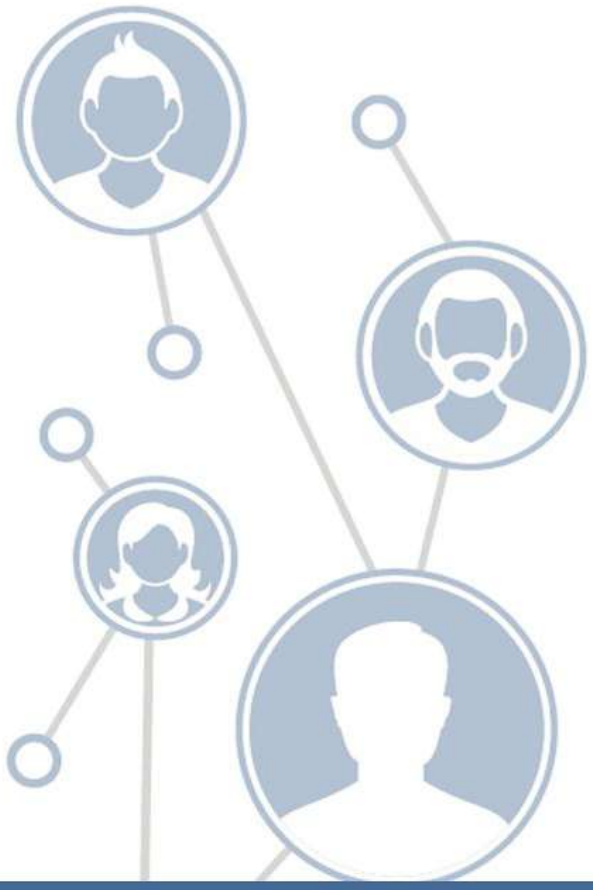
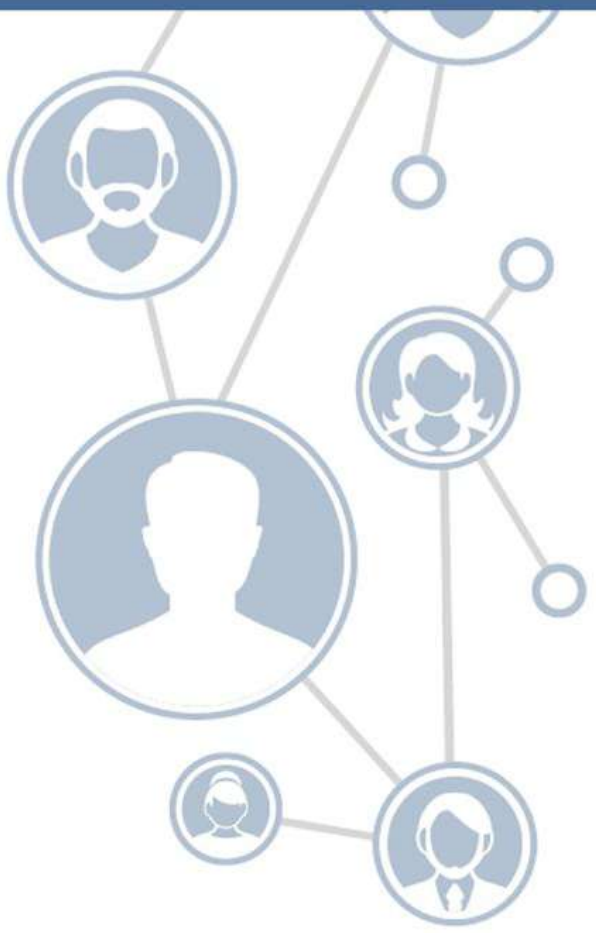


Catálogo de Módulos Interactivos



SMARTFENSE
HARDENING DE USUARIOS

Módulos Interactivos

Los módulos interactivos son contenidos de material de aprendizaje para usuarios que serán parte del programa de entrenamiento en su plataforma de SMARTFENSE. Éstos cuentan con calidad profesional y están pedagógicamente preparados para lograr cambios de hábitos permanentes en los usuarios.

Haga presente su área en la capacitación y concientización de su organización, demuestre su compromiso con la educación y con el personal propio.

Características

Interactivos

Especialistas en diseño pedagógico y diseñadores generan y actualizan material interactivo que permita a las personas asimilar de una forma fluida los buenos hábitos. Las personas le agradecerán por haberles permitido divertirse mientras aprenden y asimilan los conocimientos.

Responsivos

Nuestros contenidos le permiten a sus usuarios poder tomar la capacitación desde cualquier dispositivo ya que respetamos el estándar HTML5. Sea innovador, sea proactivo, sea disruptivo y demuestre que seguridad de la información puede implicar muchas veces algo positivo.

Personalizables

Los módulos interactivos pueden ser modificados por usted mismo, pero también puede contar con nuestro acompañamiento si así lo desea. Esto le asegurará que nuestros contenidos se comportarán como usted lo espera.

Catálogo

Seguridad general

Contraseñas

Ingeniería Social

Riesgos en el uso de correo electrónico

Buenas costumbres en el uso de correo electrónico

Phishing

Descarga de archivos adjuntos

URLs Maliciosas

Ransomware

Redes Sociales seguras

Seguridad en la navegación web

Seguridad del navegador

Cómo proteger nuestra identidad digital

Aplicaciones móviles

Dispositivos móviles

Seguridad fuera de la oficina

Teletrabajo

Malware

Estación de trabajo y periféricos

Seguridad física

Confidencialidad

Política de uso aceptable

Derechos de autor y propiedad intelectual

Copia de seguridad

Comunicaciones

Reporte de incidentes

Manejo de información

Acceso

Seguridad general

Descripción

Introduce a sus usuarios en los conceptos básicos de Seguridad de la Información. Da a conocer el papel de ellos en la seguridad de la organización.

Cumplimiento

ISO 27002
7.2.2 Día de la seguridad de la información u otros días
7.2.2 Reporte de incidentes

Contraseñas

Descripción

Entrena a sus usuarios en los conceptos básicos y las buenas prácticas concernientes a las claves que manejan diariamente en su organización y vida personal.

Cumplimiento

ISO 27002
7.2.2 Password
9.2.4 Claves privadas secretas
9.2.4 Claves grupales conocidas en el grupo
9.3.1 Fortaleza de contraseñas
9.3.1 No compartir contraseñas

Ingeniería Social

Descripción

Concientiza a sus usuarios acerca de la existencia de esta disciplina y los instruye en la prevención y correcta reacción frente a los diversos tipos de ataque que un Ingeniero Social malintencionado puede realizar en su contra.

Cumplimiento

ISO 27002
16.1.2 Errores humanos

Riesgos en el uso de correo electrónico

Descripción

Introduce a sus usuarios en los riesgos a los cuales se exponen mediante la utilización del correo electrónico.

Cumplimiento

ISO 27002
13.2.1 Archivos adjuntos

Buenas costumbres en el uso de correo electrónico

Descripción

Enseña a sus usuarios las buenas costumbres a tener en cuenta para hacer un uso correcto, responsable y seguro del correo electrónico.

Cumplimiento

ISO 27002
13.2.1 Difamación, impersonalización, acoso, reenvío de cadenas, etc
13.2.1 Reenvío de email interno a terceros

Phishing

Descripción

Capacita a sus usuarios en la prevención de este tipo de trampas mediante su identificación y reporte. A su vez entrena a sus usuarios en la correcta reacción en caso de ser víctimas de este tipo de trampa.

Cumplimiento

ISO 27002
13.2.4 Notificación de divulgación o fugas de información

Descarga de archivos adjuntos

Descripción

Enseña a sus usuarios los riesgos de los archivos adjuntos de correos electrónicos y las buenas costumbres a seguir para prevenir convertirse en víctimas de ciberdelincuentes por este medio.

Cumplimiento

ISO 27002
13.2.1 Archivos adjuntos

URLs Maliciosas

Descripción

Capacita a sus usuarios en la identificación de URLs maliciosas y enseña cómo prevenir ser víctimas de los engaños

Cumplimiento

relacionados a este tipo de URLs.

Ransomware

Descripción

Explica a sus usuarios qué es el Ransomware y cómo prevenir una infección de este tipo haciendo foco en aquellas vías de infección que necesitan de la interacción del usuario final para efectivizarse.

Cumplimiento

ISO 27002
6.2.1 Malware
6.2.2 Malware
7.2.2 Malware
13.2.1 Malware

Redes Sociales seguras

Descripción

Concientiza a sus usuarios acerca de los riesgos de las Redes Sociales y muestra las directivas y buenas prácticas relacionadas al uso seguro y responsable de las mismas, tanto dentro como fuera de la organización.

Cumplimiento

ISO 27002
13.2.1 Difamación, acoso, impersonalización, reenvío de cadenas, etc.
13.2.3 Aprobación para utilizar redes sociales

Seguridad en la navegación web

Descripción

Enseña a sus usuarios las buenas costumbres a tener en cuenta mientras navegan por internet para enfrentar los riesgos a los cuales se exponen.

Cumplimiento

ISO 27002
13.2.1 Descarga de programas de internet

Seguridad del navegador

Descripción

Cumplimiento

Concientiza a sus usuarios acerca de la importancia de mantener seguro el navegador y explica cuál es la manera de lograrlo.

Cómo proteger nuestra identidad digital

Descripción

Concientiza a sus usuarios acerca de cómo exponen su privacidad en internet y enseña las pautas a tener en cuenta para proteger su identidad en este medio digital.

Cumplimiento

ISO 27002
13.2.3 Niveles de autenticación para redes accesibles públicamente

Aplicaciones móviles

Descripción

Capacita a sus usuarios en los riesgos relacionados a la instalación y uso de aplicaciones móviles o web, como así también en la importancia y correcto uso del cifrado en los dispositivos móviles.

Cumplimiento

ISO 27002
6.2.1 Restricción en la instalación de software
6.2.1 Cifrado
6.2.1 Uso de web services y aplicaciones web

Dispositivos móviles

Descripción

Enseña a sus usuarios las directivas para proteger los dispositivos móviles, tanto físicamente como contra acceso no autorizado. Además, capacita a los mismos en los riesgos de seguridad a los que se exponen cada vez que utilizan una conexión de internet ajena a su organización.

Cumplimiento

ISO 27002
6.2.1 Protección física
6.2.1 Restricciones de conexión
11.2.8 Bloquear dispositivos móviles

Seguridad fuera de la oficina

Descripción

Capacita a sus usuarios en el correcto uso y cuidado de sus dispositivos móviles fuera de la oficina.
Entrena además a los mismos en los riesgos y buenas prácticas relacionadas al cuidado de la seguridad de la información fuera de los límites de la organización.

Cumplimiento

ISO 27002
11.2.6 No dejar equipos desatendidos en lugares públicos
11.2.6 Evitar exposición electromagnética y otros daños
11.2.6 Robo, daño, eavesdropping
11.2.6 Cadena de custodia
13.2.1 Conversaciones confidenciales en lugares públicos

Teletrabajo

Descripción

Concientiza a sus usuarios en los aspectos más importantes de seguridad de la información que cobran relevancia al inicio, durante, y al final de su teletrabajo.

Cumplimiento

ISO 27002
6.2.2 Requisitos de seguridad de las comunicaciones
6.2.2 Escritorios virtuales
6.2.2 Licencias en el puesto de trabajo
6.2.2 Firewall
6.2.2 Mueble de almacenamiento
6.2.2 Monitoreo y auditoría
6.2.2 Finalización del teletrabajo y devolución de accesos y equipos

Malware

Descripción

Concientiza a sus usuarios sobre la existencia del Malware y los entrena en la prevención de la instalación de este tipo de software en los equipos de su organización u hogar. Brinda además los medios para que, en el caso de una

Cumplimiento

ISO 27002
6.2.1 Malware
6.2.2 Malware
7.2.2 Malware
13.2.1 Malware

eventual instalación, los usuarios sepan cómo reaccionar de manera correcta.

Estación de trabajo y periféricos

Descripción

Concientiza a sus usuarios acerca de los riesgos de seguridad de la información que conviven diariamente con ellos en su puesto de trabajo dentro de su organización. Capacita a los mismos para disminuir dichos riesgos y conocer las mejores prácticas para proteger la seguridad de la información en el día a día.

Cumplimiento

ISO 27002
7.2.2 Escritorio Limpio
11.2.8 Equipos desatendidos
11.2.8 Terminar sesión
11.2.8 Logoff
11.2.9 Guardar papeles en gabinetes con llave
11.2.9 Logoff
11.2.9 Uso autorizado de fotocopiadoras, escáneres y cámaras
11.2.9 Documentos impresos deben ser retirados inmediatamente de las impresoras

Seguridad física

Descripción

Concientiza a sus usuarios acerca de los riesgos físicos a los que se expone la información de su organización. Menciona las buenas prácticas que deben tener en cuenta diariamente para disminuir dichos riesgos y reaccionar frente a la eventual ocurrencia de alguno de ellos.

Cumplimiento

ISO 27002
6.2.2 Requisitos de seguridad física
8.2.3 Registros de personas autorizadas
8.2.3 Almacenamiento de activos de IT de acuerdo a las especificaciones del proveedor
11.1.2 Usar identificadores
11.1.2 Avisar si alguien no tiene identificadores
11.1.3 Información sobre las instalaciones no deben ser accesibles públicamente
11.2.5 Todo egreso de activos de la organización debe quedar registrado
16.1.2 Brechas de seguridad física

Confidencialidad

Descripción

Pone en conocimiento de sus usuarios todos los aspectos de relevancia relacionados con el Acuerdo de Confidencialidad de su organización.

Cumplimiento

ISO 27002
7.1.2 Acuerdo de confidencialidad
7.1.2 Manejo de información de la empresa y de terceros
8.1.4 Retornar activos
8.1.4 Borrado seguro de información
13.2.4 Acuerdos de confidencialidad y NDA: duración de los acuerdos
13.2.4 Propietarios de información
13.2.4 Retorno o destrucción de la información ante cesación

Política de uso aceptable

Descripción

Pone en conocimiento de sus usuarios todos los aspectos de relevancia relacionados con la Política de Uso Aceptable de su organización.

Cumplimiento

ISO 27002
7.1.2 Qué pasa si el empleado viola los términos y condiciones
7.1.2 Qué pasa luego de que el empleado deja la organización
7.1.2 Uso del equipamiento
8.1.3 Responsabilidad de los usuarios
8.1.4 Retornar activos
12.6.2 Restricción en la instalación de software y actualizaciones
13.2.1 Difamación, acoso, impersonalización, reenvío de cadenas, etc
13.2.4 Sanciones
13.2.4 Monitoreo de usuarios
13.2.4 Notificación de divulgación o fugas de información
16.1.2 No cumplimiento de políticas y guías

Derechos de autor y propiedad intelectual

Descripción

Pone en conocimiento de sus usuarios todos los aspectos de relevancia relacionados con los Derechos de Autor y Propiedad Intelectual que se cumplen en su organización.

Cumplimiento

ISO 27002
7.1.2 Derechos de autor
13.2.4 Propiedad intelectual

Copia de seguridad

Descripción

Capacita a sus usuarios sobre la importancia de las copias de seguridad y la manera correcta de manipular las mismas dentro de su organización.

Cumplimiento

ISO 27002
6.2.1 Backups
6.2.2 Backups
8.2.3 Protección de copias de información
8.2.3 Marcado de copias

Comunicaciones

Descripción

Entrena a sus usuarios para que conozcan qué es la información confidencial y cómo ésta se expone a diversos riesgos cuando se transmite en el contexto de una comunicación. Da pautas y buenas prácticas a los mismos para poder prevenir estos riesgos y velar por la confidencialidad en sus comunicaciones y poder realizar éstas en forma responsable y confiable.

Cumplimiento

ISO 27002
13.2.1 Cifrado de comunicaciones
13.2.1 Información confidencial
13.2.1 Mensajes dejados en máquinas contestadoras
13.2.1 Fax
13.2.3 Mensajería electrónica: acceso no autorizado, modificación, DOS
13.2.3 Confiabilidad y disponibilidad del servicio
13.2.3 Firmas digitales y otros métodos legales
13.2.3 Aprobación para usar mensajería instantánea, redes sociales y compartir archivos

Reporte de incidentes

Descripción

Concientiza a sus usuarios sobre la necesidad de reportar cualquier incidente de seguridad de la información que puedan detectar. Brinda los medios para realizar dichos reportes y ejemplos de diversos casos en los que sus reportes podrían ser de gran utilidad para la organización.

Cumplimiento

ISO 27002
7.2.1 Reporte de incidentes anónimo
7.2.2 Reporte de Incidentes
16.1.2 Controles inefectivos
16.1.2 Cambios no controlados de sistemas
16.1.2 Mecanismos y canales
16.1.2 Brecha de confidencialidad, integridad y disponibilidad
16.1.2 Malfuncionamiento de software y hardware
16.1.3 Mal uso potencial de sistemas
16.1.3 Mecanismos y canales

Manejo de información

Descripción

Enseña a sus usuarios las buenas prácticas y directivas a tener en cuenta a la hora de manejar los activos de información de su organización.

Cumplimiento

ISO 27002
8.2.2 Procedimiento de etiquetado de información
8.2.3 Permisos de acceso

Accesos

Descripción

Capacita a sus usuarios en los riesgos relacionados a la autenticación y las buenas prácticas y directivas para que los accesos en su organización sean responsables y sin repudio.

Cumplimiento

ISO 27002
6.2.1 Autenticación
9.3.1 SSO
9.2.1 Usuarios únicos
16.1.2 Violaciones de acceso