**Incidentes de ciberseguridad**

# Plan de concienciación

| Índice [**Plan de concienciación 1**](#_n6arwwmay01c)  [**Índice 2**](#_y8n9kv7nwfxx)  [**Introducción 3**](#_mdo7l8shan09)  [Justificación 3](#_6bxn3dfmn300)  [**Objetivos 3**](#_b7a4c3esy9mi)  [Alineación con la política 4](#_3dkaja35ve6t)  [**Alcance 4**](#_vxtgbxpjg8cd)  [Lista de empleados 4](#_c9mv5syyp8b4)  [Puestos implicados 5](#_zcgepudswx12)  [Autorización de las sesiones formativas 5](#_p03rkiu8as30)  [Revisión del plan 5](#_mxqyxqkm66qy)  [Fomento de la conciencia en seguridad 6](#_pcl8qckgfv1p)  [Gestión del contenido y las acciones formativas 6](#_igpe9jkmpjym)  [Seguimiento del cumplimiento de las recomendaciones 6](#_lk6u5ob2e8jt)  [Metas 6](#_z1r3l135j681)  [Personal en su conjunto 6](#_4m20l0o8f0wi)  [Cargos críticos 6](#_twauuksdasoz)  [Audiencia objetivo 7](#_yblea1ne0qxr)  [Temática 7](#_j4e35pnk87ck)  [Actividades 7](#_j4e35pnk87ck)  [Presentación: Ciberseguridad estafa de CEO 7](#_ed8posur8g6v)  [Charla: Reportes de incidentes a autoridades 8](#_oyosg1dxgmyn)  [Materiales y recursos 9](#_9ofdv1nk6r7i)  [Presentación: Ciberseguridad estafa de CEO 9](#_5i9jt3ah128i)  [Charla: Reportes de incidentes a autoridades 9](#_sulkz8ooo221)  [**Evaluación, Mejora y Seguimiento 9**](#_ucg7sushotxw)  [**Anexos 10**](#_2a9siz3v6nft)  [Anexo 1 - Registro de resultado de auditorías 10](#_karag3vaqo74)  [Anexo 2 - Tabla de seguimiento del usuario 10](#_qeq8amg0888d)  [Anexo 3 - Fondos de pantalla 11](#_lxar54ew6iha) |
| --- |
| Introducción |
| El Plan de Sensibilización para el reconocimiento del **fraude del CEO** de la compañía Ca’Manolo presentará las siguientes acciones para sensibilizar a todos los empleados y capacitar a puestos directivos para prevenir, identificar y actuar ante el **intento de estafa**. |
| Justificación |
| En vista a las nuevas herramientas de replicación de imagen y voz potenciadas por inteligencia artificial, se ha decidido plantear y difundir la situación en Ca’Manolo. |
| Objetivos |
| El siguiente plan busca promover la cultura de la seguridad de la información, recorrer los ataques más comunes en las islas y explicar los nuevos riesgos asociados a la estafa del CEO.  Todo ello con los objetivos de:   1. **Concienciar al personal** sobre los riesgos asociados con la ingeniería social y la manipulación de la inteligencia artificial para llevar a cabo estafas como la del CEO. 2. **Capacitar a los empleados de mayor riesgo** para identificar señales de alerta y técnicas utilizadas en este tipo de estafas, como solicitudes de transferencias de dinero urgentes o comunicaciones no verificadas. 3. **Fomentar una cultura de seguridad** cibernética que promueva la colaboración y la comunicación transparente ante cualquier sospecha de actividad fraudulenta. 4. **Proporcionar recursos y procedimientos para reportar** incidentes de seguridad de manera rápida y eficiente. |
| Alineación con la política |
| El plan de sensibilización para el reconocimiento del **fraude del CEO** se alinea con la política de seguridad de Ca’Manolo en la medida que permite garantizar que cada uno de los procesos, políticas, metas y actividades se cumplan de acuerdo a lo preestablecido por la ley. |
| Alcance |
| La formación contempla la variedad de los puntos de partida formativo de todos los trabajadores de Ca’Manolo así pues, se darán las nociones de carácter general sobre la protección ante estafas, ejemplos adecuados a la empresa y al menos una demostración práctica del fraude del CEO.  Además, los puestos de mayor riesgo recibirán una capacitación relacionada con **la formalización y responsabilidades de notificación a las autoridades.**   * El encargado del área administrativa y tecnológica. * CTO y encargado del área de restauración.  Lista de empleados Los contenidos aprendidos en la sensibilización no dependen de las actividades ni del área física de la empresa sino de la política de la gestión de la información del propio trabajador.  Por lo tanto, será responsable de aplicar la perspectiva centrada en la seguridad de la información de acuerdo con su formación, ya sea que esté realizando su actividad laboral o fuera de ella, independientemente del tiempo y lugar.  Dada la estrecha relación del fraude con los dispositivos de comunicación electrónicos se contemplarán los riesgos inherentes y residuales de las redes, dispositivos y medios de comunicación dentro de Ca’Manolo.  Redes    Servidores |
| Dispositivos |
|  |
| Puestos implicados |
| Autorización de las sesiones formativas |
| CTO |
| Revisión del plan |
| Encargado el área tecnológica y administrativa |
| Fomento de la conciencia en seguridad |
| Cargos criticos:   * CTO * Encargado el área tecnológica y administrativa |
| Gestión del contenido y las acciones formativas |
| Consultor en seguridad de la información de [**Black9**](https://www.black9.es/) |
| Seguimiento del cumplimiento de las recomendaciones |
| Plan de auditorías de [**Black9**](https://www.black9.es/). |
| Metas |
| Con la intención de evaluar la eficacia de este plan de formación se han identificado algunos puntos a alcanzar. Personal en su conjunto  * Establecer el formato y los datos relevantes, procedimientos y encargados al reportar los incidentes. * Identificar los datos y acciones críticas buscadas por el atacante. * Establecer los medios y procedimientos de comunicación seguros para compartir información empresarial. * Lograr resultados aceptables dentro de la legalidad en una futura auditoría de ciberseguridad. * Concienciar sobre el grado de sofisticación de las nuevas amenazas potenciadas por la inteligencia artificial.  Cargos críticos  * Contextualizar el riesgo a asumir según la capacidad económica, formativa y tecnológica de la compañía. * Responsabilizar de las acciones actualmente asumibles por la empresa en materia de cumplimiento normativo. * Concienciar sobre la necesidad de incorporar solamente infraestructura segura a la empresa y de la necesidad de sanearla si procediera. * Adecuar el formato del reporte a autoridades competentes y aclarar los casos de obligada notificación. |
| Audiencia objetivo |
| Empleados con habilidades digitales, familiarizados con el uso de tecnologías informáticas y herramientas digitales, independientemente de su nivel de experiencia en áreas específicas de formación. |
| Temática |
| Las actividades programadas atenderán a la necesidad de concienciar a los integrantes de Ca’Manolo de los riesgos emergentes de la inteligencia artificial aplicada a la replicación de voz y video relacionadas con la estafa del CEO. |
| Actividades |
| Presentación: Ciberseguridad estafa de CEO |
| * Tipo de actividad → Presentación * Título → Estafa del CEO, mentiras en la cara. * Descripción → Identificar estafas y aprender a cómo protegerte de ellas. * Lugar: Bar Ca’Manolo * Contenido →   + Presentación. Quiénes somos.   + Contextualizar, información de base.   + Video ejemplo casos cercanos. **→** [**Estilo**](https://www.youtube.com/watch?v=gTY2Rr0d01A)   + Prueba de las herramientas ([Replicación de voz](https://elevenlabs.io/blog/voice-conversion/), [Replicación de cara](https://www.youtube.com/watch?v=rTOiRH1UQOc)).   + Responsabilidades legales. Qué puede ocurrir.   + Datos y acciones críticos. Qué buscan los criminales.   + Medios seguros.   + Reporte. Quién nos puede ayudar.   + Recursos. Dónde seguir formándote. * Resultados esperados → Concienciación de los riesgos, repercusiones e identificación de la estafa del CEO.   Duración: ~ 60 min |
| Charla: Reportes de incidentes a autoridades |
| * Tipo de actividad → Charla y diálogo. * Título → Lo sientes, pero ahora qué. * Descripción →   + Charla para definir casos de notificación obligada a las autoridades.   + Diálogo para contextualizar el riesgo y responsabilidades asumibles. * Lugar: Oficinas Black**9** * Contenido →   + Presentación del análisis de las obligaciones normativas del sector de la empresa.   + Datos de las pérdidas y riesgos tras diferentes ataques.   + Diálogo para contextualizar la situación económica, formativa, de infraestructura y antecedentes.   + Formalización de los datos necesarios para elaboración de análisis extras a futuro.   + Entrega de los recursos con     - Información ejecutiva y técnicas de referencia para consolidar los expuestos.     - la estructura de un reporte para las autoridades competentes.     - Las definiciones de los casos de notificación obligada a las autoridades.   + Datar la fecha para la auditoría.   + **Brindis** * Resultados esperados → Definición de los recursos y pasos a tomar por la empresa para la notificación a las autoridades en tiempo y lugar.   Duración: 30 - 15 - 30 min |
| Materiales y recursos |
| Presentación: Ciberseguridad estafa de CEO |
| * 2 bebidas /asistente * 3 aperitivos / asistente * Conexión a internet * Altavoces * Cableado para proyección. |
| Charla: Reportes de incidentes a autoridades |
| * 2 bebidas / ejecutivo * 3 aperitivos / ejecutivo * Conexión a internet estable * Altavoces * Cableado para proyección. |
|  |
| Evaluación, Mejora y Seguimiento |
| Se planificará [auditorías externas periódicas](#_karag3vaqo74), fijando fechas para una reunión con el representante de Ca’Manolo para analizar las vulnerabilidades identificadas, su evolución y, en base a los resultados obtenidos, las medidas recomendadas. Para este propósito, será beneficioso crear [perfiles para los empleados](#_qeq8amg0888d), estableciendo objetivos en función de sus respuestas ante ciberataques |
| Además, se implementará un sistema de recompensas centrado en el desarrollo del personal, con el fin de proporcionar un refuerzo positivo. |
| También se incluirá un [paquete de fondos de pantalla](#_lxar54ew6iha) minimalistas que contengan mensajes informativos sobre ciberseguridad. |
| Este plan de sensibilización tiene como propósito acompañar al encargado de fomentar la ciberseguridad en la empresa. Los resultados una vez realizada la formación dependen del conjunto de los integrantes de Ca’Manolo.  La formación son las herramientas, Ca’Manolo los artesanos. |

| Anexos |
| --- |
| Anexo 1 - Registro de resultado de auditorías |
|  |
| Anexo 2 - Tabla de seguimiento del usuario |
|  |
| Anexo 3 - Fondos de pantalla |
|  |
|  |