**Incidentes de ciberseguridad**

# Política de gestión de incidentes [Ca‘Manolo](https://camanolo.es/)

| **ÍNDICE** |
| --- |
| [**Política de gestión de incidentes Ca‘Manolo 1**](#_n6arwwmay01c)  [**Introducción 4**](#_pek9b9153j2e)  [Activos 4](#_tevktkhh23q3)  [Contexto 6](#_pvbzp62k5jc5)  [Descripción del Alcance Físico 6](#_5t4j0w5fsr6l)  [Alcance 6](#_g2e9cm04wpn)  [**Objetivos 6**](#_rn2nmll62t44)  [Glosario 7](#_nha6vu7rwf68)  [**Política 8**](#_g4h0j4jy0c2k)  [**1. Responsabilidades y procedimientos 8**](#_g4h0j4jy0c2k)  [**Escalada 8**](#_cm8kgwqef4qj)  [Responsables 8](#_cgu96vfwca00)  [Tratamiento de incidencias 8](#_2dqbymtsz86t)  [Reporte de incidencias 8](#_cgu96vfwca00)  [Sanciones disciplinarias 9](#_cgu96vfwca00)  [2. Reporte de eventos y debilidades 9](#_c9wklmu5o8o8)  [Procedimientos a seguir 11](#_y815iy8ly7ze)  [Canales 11](#_thxl5l46yu4b)  [Responsables 12](#_xloe111z8bzt)  [Reporte 12](#_154gtzn8n7bu)  [Tratamiento 12](#_lhh4nqlvvzis)  [Mecanismos 12](#_arb7hqc36dpv)  [3. Evaluación y decisión de eventos 13](#_1iiwtyxrzd2j)  [Definición de escalas 13](#_9k4bulb29oq)  [Nivel de Prioridad 13](#_9k4bulb29oq)  [Impacto Actual 14](#_n346y137waoy)  [Impacto Futuro 14](#_2trjzfy9ajnj)  [Proceso de notificación a autoridades 16](#_qsknguat7sut)  [4. Respuesta a incidentes 16](#_14m6h8hvlrnw)  [Campos incluidos en la respuesta 16](#_kskicex8e2ta)  [Tipos de incidentes 17](#_kdjizg47b7i1)  [Responsable de la respuesta 17](#_bx25prm5q8do)  [Canales de comunicación 18](#_wywqdfez948y)  [Registro y seguimiento 18](#_pa3uve5ipovz)  [Tiempos de respuesta 18](#_ncsqfn4s7v3w)  [Análisis de incidente 18](#_4cd2aav8uzc9)  [Recursos para el análisis de incidentes 19](#_36cdewdwlh92)  [Detección 20](#_tkqz1gnhndta)  [Análisis 21](#_2j5tdkrcjahd)  [5. Aprendizaje y registros 22](#_y6mdwh2co7kk)  [Software de análisis de incidencias recomendados 22](#_tlmoweskk3ue)  [**Revisión, aprobación control de cambios 23**](#_dgu66db2rc1h)  [**Referentes 24**](#_h1i2zqu1af5u)  [**Plantillas 25**](#_t1kb7lv5p698)  [Registro de incidente 25](#_i0nhuwun0zf9)  [Control de cambios 26](#_fmcqp49gb9qk)  [Revisión 26](#_w9vqqusiuyvl) |
| Introducción |
| Este documento proporciona los lineamientos básicos para iniciar el plan de ejecución del Sistema de Gestión de Incidentes de Seguridad de la Información del Bar Restaurante Ca’Manolo. |
| Activos |
| **Hardware**    **Software**  **Humanos**   | **Nombre** | **Lugar de trabajo** | **Puesto** | | --- | --- | --- | | Manolo Pérez Gonzalez | Zona de restauración | Encargado de restauración | | PINO Manola Rodriguez | Sala administración | Encargado de operaciones administrativas y tecnológicas | | Manolín Perez Cruz | Zona de restauración | Ayudante de cocina | |
| Contexto |
| Ca'Manolo es un bar y restaurante que ha conquistado el corazón de sus  clientes gracias a su dedicación a proporcionar los mejores bocadillos y  pizzas como muestran en su página web.  PINO su sobrina abogada se dedica a mantener el negoció al día con los  impuestos y la contabilidad. |
| Descripción del Alcance Físico |
| El alcance físico de estas políticas abarca el área del servidor ubicado en el segundo piso del restaurante, específicamente en la sala de servidores. Esta sala alberga los servidores web y de bases de datos que contienen información vital para las operaciones del restaurante. Además, la sala de servidores también es utilizada por el administrador de documentos para el almacenamiento seguro de archivos y documentos relevantes. |
| Alcance |
| Este documento se aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas de información del restaurante.  Por parte de Ca’Manolo S.L, queremos enfatizar que no asumimos responsabilidad por los incidentes de seguridad provocados por el uso indebido de las tecnologías de la información por nuestros clientes en nuestras redes de acceso público. Con el fin de proteger sus datos, recomendamos encarecidamente el uso de software de seguridad adecuado. |
| Objetivos |
| El presente documento establece las políticas de seguridad de la información para el restaurante Ca’Manolo. Su objetivo es garantizar la protección y confidencialidad de los datos críticos del negocio, así como prevenir cualquier acceso no autorizado, pérdida o alteración de la información almacenada.  Los objetivos de esta política son:   1. **Definir roles y responsabilidades claras:** Para evaluar los riesgos y garantizar la continuidad operativa y la disponibilidad del servicio. 2. **Gestionar eventos de seguridad eficientemente:** Identificar y tratar adecuadamente los incidentes, asegurando una respuesta ágil. 3. **Identificar y evaluar incidentes de seguridad:** Para proporcionar respuestas eficientes y adecuadas, minimizando impactos adversos. 4. **Aprender y prevenir futuros incidentes:** Mediante la implementación de salvaguardas adecuadas y la mejora continua. 5. **Monitorear y cuantificar incidentes:** A través de una base de conocimiento y registros actualizados, fortaleciendo la gestión de la seguridad. 6. **Establecer procedimientos formales:** Para el reporte y escalada de incidentes de seguridad, asegurando una respuesta coordinada. 7. **Identificar variables de riesgo potencial:** Permitiendo una evaluación efectiva del riesgo en los sistemas de información |
| Glosario |
| 1. **Phishing:** Técnica de ingeniería social utilizada para engañar a los usuarios y obtener información confidencial, como contraseñas o datos financieros, mediante correos electrónicos falsos o sitios web fraudulentos. 2. **Malware:** Software malicioso diseñado para infiltrarse o dañar un sistema informático sin el consentimiento del usuario. Ejemplos incluyen virus, gusanos, troyanos y ransomware. 3. **Ingeniería Social:** Práctica que implica manipular psicológicamente a individuos para obtener acceso no autorizado a sistemas o información confidencial, a menudo mediante la persuasión o el engaño. 4. **DDoS (Denegación de Servicio Distribuido):** Ataque cibernético que tiene como objetivo inundar un sistema, servidor o red con tráfico malicioso, lo que resulta en la interrupción del servicio para usuarios legítimos. 5. **Monitoreo:** Proceso de supervisar continuamente sistemas, redes o actividades para detectar y responder a posibles amenazas, anomalías o eventos sospechosos. 6. **Bases de Datos:** Conjunto estructurado de datos organizados de manera que permiten el almacenamiento, la gestión y la recuperación eficientes de información. En el contexto de seguridad de la información, las bases de datos pueden contener información vital para una organización y son un objetivo común para ataques de ciberseguridad |
| Política |
| Responsabilidades y procedimientos |
| Escalada |
| El personal designado para el escalamiento de la gestión de incidentes en orden descendiente es el siguiente: |
| 1. Líder del área de restauración. (Manolo) 2. Encargado de operaciones administrativas y tecnológicas. (Pino) 3. Auxiliar de operaciones administrativas y tecnológicas. 4. Auxiliar de restauración. |
| Responsables |
| Tratamiento de incidencias |
| El **encargado de la sección administrativa y tecnológica** será el responsable de la resolución, prevención y tratamiento de las incidencias. Podrá delegar sus funciones a un equipo especializado designado por incidencia. |
| Reporte de incidencias |
| Todos los integrantes de Ca’Manolo tienen el derecho y responsabilidad de reportar al encargado de tratar los incidentes de ciberseguridad detectados, acontecidos o previstos. |
| Sanciones disciplinarias |
| * Líder del área de restauración.   En el área de las las operaciones administrativas y tecnológicas se delega la potestad a tomar sanciones a:   * Encargado de operaciones administrativas y tecnológicas. |
| Reporte de eventos y debilidades |
| Un incidente de seguridad de la información es cualquier evento o situación que compromete la confidencialidad, integridad o disponibilidad de los datos o sistemas de información de una organización. Estos incidentes pueden ser provocados por una amplia gama de factores, que van desde acciones maliciosas como ataques cibernéticos y malware hasta errores humanos, desastres naturales o fallas en los sistemas tecnológicos.  La notificación en casos de incidentes de seguridad de la información permite a una organización informar a las partes afectadas, incluidos clientes, empleados y autoridades pertinentes, sobre el incidente ocurrido.  Algunas de las razones por las cuales la notificación es importante incluyen:   1. **Transparencia y confianza**: La notificación transparente demuestra el compromiso de la organización con la seguridad de la información y la protección de los datos de las partes afectadas. Esto ayuda a mantener la confianza de los clientes, empleados y otras partes interesadas. 2. **Cumplimiento normativo:** En muchos casos, las leyes y regulaciones requieren que las organizaciones notifiquen a las partes afectadas sobre incidentes de seguridad de la información. Esto puede incluir leyes de protección de datos, regulaciones específicas de la industria o requisitos de divulgación obligatoria. 3. **Mitigación de riesgos:** La notificación oportuna puede ayudar a mitigar los riesgos adicionales al permitir que las partes afectadas tomen medidas para protegerse. Por ejemplo, si se produce una violación de datos que involucra contraseñas, la notificación puede alentar a los usuarios a cambiar sus contraseñas de inmediato. 4. **Responsabilidad y rendición de cuentas:** La notificación demuestra que la organización reconoce la gravedad del incidente y asume la responsabilidad de abordarlo. Esto puede ayudar a evitar acusaciones de ocultamiento o negligencia. 5. **Facilitación de la respuesta y recuperación:** La notificación puede ayudar a movilizar recursos internos y externos para responder al incidente y recuperarse de él de manera más efectiva. |
| Los siguientes ejemplos de incidentes de seguridad de la información ayudarán a contextualizar la variedad y la naturaleza de las amenazas cibernéticas que pueden afectar a las organizaciones y los individuos |
| 1. **Violación de datos:** Acceso no autorizado a información confidencial, como números de tarjetas de crédito, nombres de usuarios y contraseñas, información médica o información personal identificable (PII). 2. **Ataques de malware:** Infección de sistemas informáticos con software malicioso, como virus, gusanos, troyanos o ransomware, que pueden causar daños, robo de datos o interrupción del servicio. 3. **Phishing:** Intentos de engañar a los usuarios para que divulguen información confidencial, como contraseñas o información financiera, mediante el uso de correos electrónicos, mensajes de texto u otros medios de comunicación electrónica. 4. **Denegación de servicio (DDoS):** Ataques diseñados para inundar un sistema, servidor o red con tráfico malicioso, lo que resulta en la interrupción del servicio para usuarios legítimos. 5. **Intrusión de red:** Acceso no autorizado a sistemas informáticos o redes internas, a menudo mediante la explotación de vulnerabilidades de software o debilidades en la configuración de seguridad. 6. **Fugas de información:** Divulgación no autorizada de datos confidenciales o sensibles, ya sea accidentalmente o como resultado de acciones maliciosas. 7. **Ataques de ingeniería social:** Manipulación psicológica de individuos para obtener acceso no autorizado a sistemas o información confidencial, a menudo mediante la persuasión o el engaño. 8. **Vulnerabilidades de seguridad no corregidas:** Explotación de fallas de seguridad conocidas en software o sistemas que no han sido parcheadas o solucionadas. 9. **Acceso físico no autorizado:** Acceso no autorizado a instalaciones físicas donde se almacenan o procesan datos sensibles, como centros de datos o salas de servidores. 10. **Robo o pérdida de dispositivos:** Extravío o robo de dispositivos informáticos, como computadoras portátiles, teléfonos móviles o unidades USB, que contienen datos sensibles o confidenciales. |
| Procedimientos a seguir |
| Procedimiento básico para el reporte de debilidad o incidencia: |
| 1. **Identificación de eventos de seguridad:** Detectar cualquier anomalía o incidente en la seguridad de la información. 2. **Registro de eventos:** Documentar todos los eventos detectados, ya sea mediante un sistema automatizado o manual. 3. **Análisis de eventos:** Investigar cada evento para determinar su causa y potencial impacto. 4. **Notificación y escalado:** Notificar eventos significativos a las partes relevantes para su revisión y acción. 5. **Implementación de medidas correctivas:** Tomar medidas para abordar las debilidades de seguridad identificadas. 6. **Monitoreo y seguimiento:** Supervisar continuamente la efectividad de las medidas implementadas y detectar nuevas debilidades. 7. **Informe de debilidades:** Elaborar informes periódicos que detallen eventos y acciones tomadas para mejorar la seguridad. 8. **Capacitación del personal:** Proporcionar formación regular sobre seguridad de la información y procedimientos de reporte. 9. **Revisión y mejora continua:** Evaluar y actualizar el proceso de reporte de eventos para adaptarse a cambios y mejorar la seguridad de manera constante. |
| Canales |
| Para facilitar el reporte de eventos y debilidades de seguridad de la información en Ca’Manolo se ofrecerá diferentes canales de reporte: |
| 1. **Línea directa o número de teléfono:** Proporcionar un número de teléfono directo o una línea de asistencia para que los empleados puedan llamar y reportar eventos de seguridad de manera inmediata. 2. **Buzón físico de sugerencias o quejas:** Donde los empleados puedan dejar notas anónimas sobre eventos de seguridad. 3. **Reuniones de equipo:** Con el objetivo de fomentar un ambiente de confianza en el que los empleados estén cómodos reportando eventos de seguridad durante reuniones de equipo regulares. 4. **Sistema de tickets o incidencias:** Donde los empleados puedan registrar eventos de seguridad y hacer un seguimiento del progreso de la resolución. |
| Responsables |
| Reporte Todos los empleados Ca’Manolo conocedores de cualquier debilidad y/o incidente de ciberseguridad. |
| Tratamiento |
| Equipo de incidencias con funciones delegadas del Encargado de la sección administrativa y tecnológica. |
| Mecanismos |
| 1. **Línea directa o número de teléfono:**    * Número de teléfono directo para reportar incidentes de seguridad: +34 696966969    * Se establecerá un sistema de respuesta automática para dirigir las llamadas entrantes al equipo de seguridad de la información. 2. **Buzón físico de sugerencias o quejas:**    * Ubicación del buzón físico: Recepción principal, junto a la puerta de entrada.    * Se proporcionarán formularios en papel para que los empleados puedan dejar notas anónimas sobre eventos de seguridad. Informe al final del documento. 3. **Reuniones de equipo:**    * Se llevarán a cabo reuniones de equipo semanales donde se dedicará un espacio para discutir temas relacionados con la seguridad de la información.    * Los empleados serán alentados a compartir cualquier preocupación o incidente de seguridad durante estas reuniones de manera abierta y confidencial. 4. **Sistema de tickets o incidencias:**    * Plataforma de gestión de incidencias: [JIRA Security Incident Management](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj3ptLu78iEAxV62QIHHXytAkUQFnoECBcQAQ&url=https%3A%2F%2Fwww.synapsa.tech%2Fuse-cases%2Fincident-response-automation-ira-2%2F&usg=AOvVaw3IaLyIGJgN2njik3xvt7az&opi=89978449)    * Los empleados podrán acceder a la plataforma utilizando sus credenciales de inicio de sesión habituales y registrar incidentes de seguridad de manera estructurada.    * Se proporcionará capacitación sobre cómo utilizar el sistema de tickets durante la inducción y de forma continua a lo largo del año. |
| 3. Evaluación y decisión de eventos |
| Definición de escalas |
| Nivel de Prioridad |
|  |
| Impacto Actual |
| Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado. |
| Impacto Futuro Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado. |
|  |
|  |
| Y los resultados obtenidos se deben comparar con la siguiente tabla para determinar la prioridad de atención. |
|  |
| Proceso de notificación a autoridades |
| Se notificará a las autoridades competentes cualquier incidente de ciberseguridad que esté sujeto **a leyes y regulaciones específicas**, incluyendo pero no limitado a leyes de protección de datos, regulaciones de la industria y requerimientos gubernamentales.  El encargado será el encargado del área administrativa y tecnológica. |
| 4. Respuesta a incidentes |
| Campos incluidos en la respuesta |
| Después de abordar y resolver el incidente, se debe estructurar el informe de la siguiente manera:   * **Resumen ejecutivo**: Se debe explicar de manera clara y concisa qué ha ocurrido, evitando el uso de terminología técnica. * Línea de tiempo del incidente: Detalla los eventos ocurridos paso a paso, basándose en la bitácora de incidentes. * **Datos del entorno:** Proporciona información relevante sobre el entorno afectado. * **Gestión del incidente**: Describe las acciones tomadas para responder al incidente. * **Análisis forense**: En caso de haberse realizado, se incluyen los resultados, pudiendo ir como anexo si es extenso. * **Análisis de malware**: Si se efectuó un análisis de malware, se detallan los resultados, también como anexo si es necesario. * **Impacto del incidente**: Se evalúa o estima el impacto del incidente, incluyendo datos perdidos, equipos afectados y daños ocasionados. * **Atribución:** Se indica, en la medida de lo posible, quién pudo ser el responsable del incidente. * **Recomendaciones de seguridad**: Se proponen medidas para prevenir la repetición del incidente. * **Lecciones aprendidas**: Se analiza lo que se hizo bien, lo que se hizo mal y las acciones que se deben tomar para mejorar en futuros incidentes. * **Anexo**: Se adjuntan evidencias relevantes, como registros o capturas de pantalla, que no se incluyeron en la gestión del incidente debido a su extensión. |
| Tipos de incidentes |
| **Informe de Detección**  Se ha confirmado la detección de un incidente de seguridad en nuestra red. Hasta el momento, se ha observado un aumento inusual en el tráfico de red saliente desde varios sistemas internos hacia direcciones IP externas conocidas por alojar malware. Se estima que al menos cinco servidores están afectados, con potencial impacto en la integridad de los datos almacenados. Se está investigando la naturaleza exacta del incidente y se están tomando medidas inmediatas para contener la situación y minimizar el impacto en otros sistemas.  **Informe "de Batalla" (Actualización)**  El equipo de respuesta ante incidentes ha tomado medidas para aislar los servidores afectados y ha iniciado un análisis forense para determinar el alcance completo del incidente. Se han identificado archivos sospechosos en los servidores comprometidos, y se están tomando medidas para eliminar el malware y restaurar la integridad de los datos afectados. Se está trabajando en estrecha colaboración con el equipo de seguridad cibernética externo para recopilar más información y fortalecer las defensas contra futuros ataques.  **Informe de Crisis**  Se ha confirmado un incidente de seguridad significativo en nuestra red, con múltiples servidores comprometidos por malware. La integridad de los datos se ha visto comprometida, y se están tomando medidas inmediatas para contener la situación y minimizar el impacto en nuestras operaciones. Se está trabajando con expertos externos en seguridad cibernética para investigar la causa raíz del incidente y fortalecer nuestras defensas. La dirección y el equipo legal han sido informados y se mantendrán actualizados sobre los desarrollos. Es esencial que todos los empleados sigan los protocolos de seguridad establecidos y estén atentos a cualquier actividad sospechosa en nuestra red. |
| Responsable de la respuesta |
| El **encargado** del área administrativa y tecnológica será el responsable de elaborar en forma y tiempo la respuestas al incidente. Este podrá delegar las tareas a un equipo especializado pero ha de ser revisado y aprobado. |
| Canales de comunicación |
| Las comunicaciones de incidencias son multicanal y universales para evitar confusión a la hora de notificarlo. Por ello podemos tomar como referencia los [canales](#_thxl5l46yu4b) del punto 2. |
| Registro y seguimiento |
| Una vez escalado el incidente para su tratamiento ha de registrarse las acciones cometidas y el estado del mismo. Para ello se facilita [una plantilla](#_i0nhuwun0zf9) con los campos necesarios para un marco común. Uno de los campos es el estado del incidente, en caso de encontrarse resuelto se procederá a archivar este registro con una validez recomendada de 3 años para evidenciar el tratamiento del incidente en caso de reclamaciones legales.  En caso de mantenerse activa la incidencia, Ca’Manolo se compromete a acometer su solución dentro de los siguientes plazos. |
| Tiempos de respuesta |
| Para el caso de la atención de incidentes de seguridad se ha establecido unos tiempos máximos de atención de los mismos, con el fin de atender adecuadamente los incidentes de acuerdo a su criticidad e impacto |
|  |
| Análisis de incidente |
| Se enfocará en establecer un modelo que permita responder de manera efectiva a los incidentes de seguridad de la información. Esto implica no solo la capacidad de respuesta inmediata, sino también la detección, evaluación y gestión de vulnerabilidades para prevenir futuros incidentes.  El encargado de operaciones administrativas y tecnológicas de la planta de administración, o el equipo designado para esta tarea, debe asegurarse de contar con los recursos y herramientas necesarios para cubrir todas las fases del ciclo de vida de respuesta a incidentes. Esto incluye el desarrollo o validación de procedimientos existentes, así como la implementación de programas de capacitación para el personal involucrado.    El encargado de operaciones administrativas y tecnológicas debe ser notificado de la incidencia para que empieze con la elección de las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones, teniendo en cuenta los recursos con los que cuenta. |
| Recursos para el análisis de incidentes |
| Para la correcta gestión de incidentes hará de contarse con los siguientes recursos: |
| 1. **Puertos:** Información detallada sobre los puertos abiertos y servicios en ejecución en los sistemas afectados, lo que ayuda a identificar posibles vectores de ataque y comportamiento anómalo. 2. **Inventario de activos:** Una lista completa de todos los dispositivos y recursos de red, incluidos servidores, equipos de red, dispositivos IoT, etc., para comprender el alcance del incidente y sus posibles impactos. 3. **Diagrama de red:** Un esquema visual que representa la topología de la red, la conectividad entre los dispositivos y los flujos de datos, lo que facilita la comprensión del entorno de red y la identificación de posibles puntos de entrada o propagación de amenazas. 4. **Servidores:** Información detallada sobre los servidores afectados, incluidos sistemas operativos, roles y servicios instalados, configuraciones de seguridad y registros de actividad, para comprender cómo se vieron comprometidos y qué datos pueden estar en riesgo. 5. **Aplicaciones:** Detalles sobre las aplicaciones instaladas y en funcionamiento en los sistemas afectados, incluidas versiones, configuraciones y posibles vulnerabilidades conocidas, para determinar si el incidente está relacionado con una aplicación específica o una brecha en su seguridad. 6. **Registro de actualizaciones:** Un registro de todas las actualizaciones de software aplicadas a los sistemas afectados, incluidos parches de seguridad, actualizaciones de software y cambios de configuración, para evaluar si el incidente podría haberse explotado debido a una vulnerabilidad no parcheada. 7. **Direcciones IP:** Información sobre las direcciones IP asignadas a los dispositivos afectados, junto con registros de tráfico de red y registros de eventos, para rastrear el origen y la propagación de un ataque y para identificar posibles direcciones IP de atacantes. 8. **Análisis del comportamiento de red estándar**: teniendo en cuenta puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones. |
| Detección |
| Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido generalmente algunos de estos elementos son:   * **Actividades de inicio de sesión sospechosas**: Intentos repetidos de inicio de sesión fallidos o desde ubicaciones inusuales. * **Anomalías en el tráfico de red**: Picos de actividad, conexiones a direcciones desconocidas. * **Cambios no autorizados en archivos de sistem**a: Alteraciones en archivos críticos del sistema operativo. * **Aumento en la actividad de correo no deseado**: Correos electrónicos sospechosos o de phishing. * **Errores inesperados en aplicaciones o sistemas:** Mensajes de error, bloqueos frecuentes de aplicaciones. * **Modificaciones no autorizadas en la configuración del sistema.** * **Informes de anomalías del personal de TI:** Observaciones o informes de comportamientos anómalos en los sistemas. * **Alertas en sistemas de seguridad**: Notificaciones generadas por sistemas de seguridad sobre actividades sospechosas o potencialmente maliciosas. * **Caídas de servidores**: Interrupción repentina del servicio de un servidor, lo que podría indicar un ataque o un fallo de seguridad. * **Reportes de usuarios:** Informes presentados por los usuarios sobre comportamientos inusuales o problemas de seguridad percibidos en el sistema. * **Informes de antivirus:** Alertas o informes generados por software antivirus sobre la detección de amenazas o actividades maliciosas en el sistema. * **Comportamientos no habituales**: lentitud inesperada, consumo excesivo de recursos, etc |
| La identificación y gestión de elementos que alertan sobre un incidente nos proveen información que puede alertarnos sobre la futura ocurrencia del mismo y preparar procedimientos para minimizar su impacto. Algunos de estos elementos pueden ser:   * Logs de servidores * Logs de aplicaciones * Logs de herramientas de seguridad * Cualquier otra herramienta que permita la identificación de un incidente de seguridad. |
| Análisis |
| En el proceso de análisis de incidentes, es crucial priorizar la seguridad de la información y considerar diversos componentes para una gestión efectiva. Se sugiere tener en cuenta lo siguiente:   1. **Entendimiento de la red y sistemas:** Los administradores de TI deben estar completamente familiarizados con el comportamiento típico de la infraestructura.. 2. **Centralización de la información relevante** 3. **Correlación de eventos:** La correlación de eventos es esencial para detectar patrones de comportamiento anormal y entenderlo para tomar medidas efectivas y eficientes. 4. **Utilización de una base de conocimiento actualizada:** Establecer ycoordinar al equipo para la recopilación eficiente de datos que ayuden a poner fin a la debilidad y/o incidencia. 5. **Realizar pruebas:** Una vez conformado el equipo se toman medidas y analizan los resultados. Se documentará cada intento independientemente de los resultados. En caso de resultados inesperados se volverá al anterior paso. |
| 5. Aprendizaje y registros |
| 1. **Registro de Conocimiento del Incidente:**    * Se establecerá un registro centralizado y [estandarizado](#_pa3uve5ipovz) para documentar todos los detalles relevantes de cada incidente de ciberseguridad.    * El responsable de mantener este registro será en caso de que lo hubiere, el Equipo de Respuesta a Incidentes (IRT), designado por el encargado del sector administrativo y tecnológico. 2. **Responsabilidades:**    * El Equipo de Respuesta a Incidentes (IRT), si lo hubiere, será responsable de registrar todos los incidentes de ciberseguridad.    * El encargado del sector administrativo y tecnológico será el responsable de mantener y actualizar el registro de incidentes. 3. **Preservación de Evidencias:**    * El procedimiento incluirá la creación de una cadena de custodia hacia el equipo de respuestas a incidentes para garantizar la integridad de las evidencias recopiladas.    * Se utilizarán [herramientas y técnicas adecuadas](#_ujinxxg0y4p4) para recopilar, almacenar y proteger las evidencias digitales de manera forense. |
| Software de análisis de incidencias recomendados |
| La unidad de operaciones administrativas y tecnológicas, debe contar con:   * **Analizadores de protocolos**: Para monitorear y detectar actividades sospechosas en la red. * **Software para recolección de evidencia**: Facilita la recopilación y preservación de evidencia digital relevante. * **Kit de respuesta a incidentes**: Conjunto de herramientas y procedimientos para una respuesta rápida y efectiva. * **Software de análisis forense**: Permite examinar sistemas e identificar la causa y el alcance de los incidentes. * **Medios de almacenamiento:** Para preservar la integridad de la evidencia digital.   Software recomendado:   * **Wireshark**: Analiza el tráfico de red en tiempo real. * [Wazuh](https://wazuh.com/): Herramienta para detectar y analizar amenazas y responder a ellas antes de que afecten a las operaciones. * [Snort](https://www.snort.org/): Herramienta de análisis de intrusiones. * [FTK Imager](https://www.exterro.com/digital-forensics-software/ftk-imager): Facilita la adquisición y análisis de imágenes de discos duros.   Integrar estos elementos fortalecerá la capacidad de la unidad para gestionar incidentes de seguridad de la información. |
| Revisión, aprobación control de cambios |
| El proceso de revisión y actualización de las políticas de seguridad de la información del restaurante se llevará a cabo de manera regular y sistemática para garantizar su relevancia y eficacia en todo momento. Con una ventana de tiempo **máxima anual**.  Este proceso se realizará de la siguiente manera:   1. **Programación de Revisiones Periódicas:** Se establecerá un calendario de revisiones periódicas, que se llevarán a cabo al menos una vez al año. Durante estas revisiones, se evaluará la efectividad de las políticas existentes y se identificarán posibles áreas de mejora. 2. **Participación de Partes Interesadas:** Se involucrará a todas las partes interesadas relevantes en el proceso de revisión, incluidos los gerentes de departamento, el personal de TI y cualquier otra persona que tenga un papel clave en la seguridad de la información del restaurante. 3. **Evaluación de Incidentes de Seguridad:** Se tendrán en cuenta los incidentes de seguridad pasados ​​y las vulnerabilidades identificadas para mejorar las políticas de seguridad y prevenir futuros incidentes. 4. **Actualización de Normativas y Estándares:** Se revisarán las normativas y estándares de seguridad de la información pertinentes, tanto a nivel local como nacional e internacional, para asegurarse de que las políticas del restaurante estén alineadas con las mejores prácticas de la industria. 5. **Documentación de Revisiones:** Se documentarán todas las revisiones realizadas, incluidos los cambios implementados y las razones detrás de ellos. Esta documentación servirá como registro histórico y proporcionará transparencia sobre el proceso de revisión. 6. **Comunicación y Capacitación:** Después de cada revisión, se comunicarán los cambios realizados a todo el personal relevante y se proporcionará la capacitación necesaria para asegurar su comprensión y cumplimiento. |
| Referentes |
| La Política de Gestión de Incidentes de Ciberseguridad del restaurante Ca’Manolo se basa en una serie de referentes y estándares reconocidos a nivel nacional e internacional. A continuación, se enumeran algunos de los documentos y normativas relevantes: |
| 1. **ISO/IEC 27001:** Esta norma internacional establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Proporciona un marco integral para la gestión de la seguridad de la información, incluida la gestión de incidentes de ciberseguridad. 2. **Reglamento General de Protección de Datos (GDPR):** Esta regulación de la Unión Europea establece las normas para la protección de datos personales y la privacidad de los individuos. Contiene disposiciones relacionadas con la notificación y gestión de incidentes de seguridad de datos. 3. **Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD):** La legislación española en materia de protección de datos, que complementa el GDPR y establece requisitos adicionales para la gestión de incidentes de seguridad de datos en el ámbito nacional. 4. **INCIBE (Instituto Nacional de Ciberseguridad):** Este organismo público español proporciona recursos, guías y herramientas para la gestión de incidentes de ciberseguridad, así como asesoramiento en materia de seguridad de la información. 5. **Guía CCN-STIC 817:** Publicada por el Centro Criptológico Nacional (CCN), esta guía ofrece pautas y recomendaciones para la gestión de incidentes de ciberseguridad en organizaciones públicas y privadas en España. 6. **NIS Directive (Directiva sobre la seguridad de las redes y los sistemas de información):** Esta directiva de la Unión Europea establece requisitos para garantizar un nivel común de seguridad cibernética en toda la UE, incluida la notificación de incidentes de seguridad de redes y sistemas de información. |

# Plantillas

## Registro de incidente

|  | **Descripción** |
| --- | --- |
| Fecha y hora del incidente | Registro de la fecha y hora exactas en que se produjo el incidente. |
| Tipo de incidente | Clasificación del incidente según su naturaleza (por ejemplo, malware, ataque de denegación de servicio). |
| Descripción del incidente | Detalles sobre lo ocurrido, incluyendo el impacto y las áreas afectadas. |
| Origen del incidente | Indicación de la fuente o causa del incidente (por ejemplo, ataque externo, error humano). |
| Recursos afectados | Lista de los sistemas, aplicaciones o datos afectados por el incidente. |
| Medidas tomadas | Acciones realizadas para contener el incidente, minimizar el daño y restaurar la operatividad. |
| Responsable del incidente | Persona o equipo encargado de la gestión y respuesta al incidente. |
| Información de contacto | Datos de contacto de los responsables del incidente para consultas y seguimiento. |
| Impacto del incidente | Evaluación del impacto del incidente en términos de pérdidas financieras, reputacionales u operativas. |
| Lecciones aprendidas | Análisis retrospectivo del incidente y recomendaciones para prevenir futuros incidentes similares. |
| Estado del incidente | Estado actual del incidente (por ejemplo, en curso, resuelto, en investigación). |
| Información adicional | Cualquier otra información relevante relacionada con el incidente. |

## Control de cambios

| **Fecha de cambio** | **Versión** | **Descripción de Cambio** |
| --- | --- | --- |
| 26/02/2024 | 1.0 | Creación del documento. |

## Revisión

| **Fecha de aprobación** | **Versión** | **Elaborado por** | **Revisado por** | **Cargo de Revisor** |
| --- | --- | --- | --- | --- |
| 26/02/2024 | 1.0 | Francisco Iván Ramírez Ortega | Pino Manola Rodriguez | Encargado de operaciones administrativas y tecnológicas |