**Incidentes de ciberseguridad**

# Plan director empresa

ÍNDICE

[Plan director empresa 1](#_n6arwwmay01c)

[Aprobación y entrada en vigor 3](#_pg5wj9ktykm9)

[Introducción 4](#_wmztr9s0m23)

[Análisis inicial 5](#_yy8e5ziyvpb6)

[Alcance 5](#_74sgvi4y8x0j)

[Gestión de activos 5](#_gqn9rhewnl4t)

[Objetivo 6](#_jk07bb6txvi8)

[Auditorías de seguridad 6](#_yt7woqhv6azk)

[Auditoría de sistemas 6](#_hes8m57tfh8)

[Auditoría de procesos y usuarios 8](#_mjtp08b1lfx1)

[Políticas debidamente implementadas 8](#_a0fda71jrydo)

[Políticas no implementadas 9](#_t99f76ajf2k4)

[Análisis de riesgos 9](#_ltlj523q0df1)

[Riesgos Inherentes 11](#_rja6lkcovguh)

[Nivel de riesgo aceptable 12](#_bs1jlab6qfq8)

[Definición de proyectos e iniciativas 13](#_y8xf5181ljmc)

[Formación y concienciación 14](#_j7s5n479y1bw)

[Procedimiento de Gestión de Incidentes 15](#_1zseexfhk7g7)

[Responsabilidades en la Gestión de Incidentes: 15](#_x3rkni6p3dnb)

[Procedimientos en la gestión de incidentes 15](#_lrk2uz2h835)

[Reporte de eventos 16](#_odgp1l8fp8n)

[Clasificación / Taxonomía de los Ciberincidentes 18](#_8b7h5xbf9ne5)

[Clasificación y priorización 18](#_ko5oxeks898y)

[Implementación del Plan Director de Seguridad 19](#_wpta22chgwr7)

[Obligaciones del personal 19](#_iz3v6n78waxr)

[Terceras partes 20](#_8ey0ibg9a6xx)

[**Anexos 20**](#_5b3e8w2sryy9)

[Inventario de activos 20](#_yqpt9b1iqywb)

[Informe técnico 20](#_u4u1cave49h6)In

| Aprobación y entrada en vigor |
| --- |
| Este Plan Director de Ciberseguridad es efectivo desde la fecha de su aprobación por la dirección de IES El Rincón, hasta que sea reemplazado por un nuevo plan. |

| Introducción |
| --- |
| El presente Plan Director de Ciberseguridad pretende definir y priorizar un conjunto de proyectos en materia de seguridad de la información, a partir de un análisis de la situación inicial, con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables.  Es fundamental para la realización de un buen Plan Director de Seguridad que éste se alinee con los objetivos estratégicos de la organización, incluya una definición del alcance e incorpore las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización, así como terceros que colaboren con ésta. |
| Para la elaboración y puesta en marcha del presente Plan Director de Seguridad se han ejecutado las siguientes fases o etapas: |
| 1. Análisis inicial. 2. Estudio de la estrategia de la organización 3. Análisis de riesgos informáticos. 4. Definición de proyectos e iniciativas. 5. Clasificación y priorización. 6. Definición de metodología de implantación. |
| Análisis inicial.  Análisis de riesgos informáticos.  Definición de proyectos e iniciativas.  Clasificación y priorización.  Definición de metodología de implantación. |

| Análisis inicial |
| --- |
| Alcance |
| El ámbito de aplicación del Plan Director de Seguridad abarca todos los servicios ofrecidos por IES El Rincón que se basen en Tecnologías de la Información y las Comunicaciones, así como a todo el personal, sin excepciones. Específicamente, incluye:   * Todos los departamentos, tanto sus directivos como empleados. * Los contratistas, clientes u cualquier otra tercera parte que acceda a la información o sistemas de la organización. * Bases de datos, archivos electrónicos y en formato papel, procesos, equipos, programas y sistemas. * La información generada, procesada y almacenada, sin importar su medio o formato, utilizada en tareas operativas o administrativas. * La información cedida dentro de un marco legal establecido, considerada como propia para su protección exclusiva. * Todos los sistemas empleados para la administración y gestión de la información, ya sean propios, alquilados o licenciados. |
| Gestión de activos |
| Los activos de la organización son aquellos que poseen un valor para la misma.  En el caso de los activos de información, se refieren a todos los equipos, instalaciones o software de cualquier naturaleza que contengan, procesen o manejen información de alguna manera. |
| /\*\* Realizar un análisis con nmap, volcarlo a un excel y que cumpla al menos los siguientes campos  IP, MAC, HOSTNAME, comentarios   * Con ip’s y macs con:   sudo arp-scan 192.168.1.1 - 192.168.255.255   * SO y hostname con nmap, nessus, y crackmapexec   \*\*/ |
| El inventariado de activos se encuentra recogido en el documento: |
| Objetivo |
| El objetivo principal del presente Plan Director de Ciberseguridad es establecer un marco de seguridad que facilite el análisis, la propuesta y el diseño de políticas, procedimientos y proyectos destinados a reducir los riesgos asociados con la seguridad de la información. Este objetivo se desglosa en varias acciones clave:  - Realizar un estudio exhaustivo de la situación actual para evaluar el nivel de seguridad de la infraestructura de red, servicios y aplicaciones.  - Llevar a cabo un análisis de riesgos basado en la información recopilada, con el fin de determinar el impacto en la seguridad que podría afectar a IES El Rincón.  - Establecer políticas y procedimientos como medidas de seguridad que contribuyan a preservar la integridad, confidencialidad y disponibilidad de la información.  - Promover entre el personal y las principales autoridades la adopción de una cultura de seguridad.  - Reforzar el nivel de seguridad a través de proyectos e iniciativas que garanticen la protección de la información frente a diversas amenazas, asegurando así la continuidad del negocio. |
| Auditorías de seguridad |
| Se llevaron a cabo dos auditorías sobre el sistema de información de la organización:   1. **Auditoría de sistemas (Pentesting)**: Se realizó un análisis técnico exhaustivo para identificar y evaluar los riesgos a los que están expuestos todos los activos que conforman la red corporativa. 2. **Auditoría de procesos y usuarios (Cumplimiento)**: Se llevó a cabo un análisis detallado para determinar los riesgos a los que están expuestos los usuarios que acceden a la red corporativa, así como para evaluar el cumplimiento de los procesos establecidos.   A continuación se presenta un resumen de los hallazgos obtenidos en ambas auditorías. |
| Auditoría de sistemas |
| Después de completar la auditoría de seguridad (Pentesting) para todos los activos de la red corporativa, se ha determinado que el nivel de riesgo es MEDIO. Esta evaluación se basa en un análisis de los resultados obtenidos durante la ejecución, siguiendo la metodología de trabajo establecida.  Durante la auditoría, se identificaron vulnerabilidades críticas en algunos activos. Estas vulnerabilidades podrían permitir a un atacante obtener información personal e identificativa de trabajadores como alumnos. Se recomienda con urgencia la implementación de soluciones técnicas detalladas en el informe para los activos con un nivel de riesgo crítico.  Se considera que la seguridad de la red corporativa es de nivel medio y necesita mejoras para una implementación efectiva de un Sistema Gestionado de Seguridad de la Información (SGSI), basado en la mejora continua del sistema.  Esto requiere análisis periódicos de riesgos y la planificación de acciones de tratamiento o mejora basadas en estos análisis, incidencias del sistema y la eficacia de las políticas de seguridad internas. La gestión adecuada de este plan de mejora es esencial.  La planificación de las acciones de tratamiento de riesgos se basa en un análisis de probabilidad e impacto, priorizando las medidas correctivas o mitigadoras de los riesgos detectados.  El tratamiento de riesgos tiene dos objetivos principales: prevenir la ocurrencia del riesgo y minimizar su impacto en caso de que ocurra. Esto está en línea con el objetivo del Esquema Nacional de Seguridad, que busca proteger la información y los servicios prestados por las entidades en su ámbito de aplicación.  Es crucial establecer una cultura de seguridad dentro de la organización para el correcto funcionamiento de un SGSI. Esto implica la elaboración de un **Plan Director de Seguridad y Políticas de Seguridad**, así como su difusión a todos los departamentos. La formación continua de los usuarios del sistema es fundamental para esta concienciación, y se deben mantener registros del cumplimiento de estas políticas para evidenciar su implementación y seguimiento. |
| Para un mayor entendimiento del análisis revisar el documento adjunto: |
| /\*\* Informe técnico con los siguientes apartados. Es muy denso y largo, herramientas como pwndoc ayudan a evitar HORAS.   * Objetivo   + Análisis de adecuación ( lo que se va a hacer, verboso y poco técnico)   + Especificaciones funcionales ( conciso y algo más técnico)   + Estudio de costes   + Desarrollo e implementación   + Formación   + Explotación * Metodología (explicación, bases)   + Inventario de activos   + Diagrama de red   + Auditoria pentesting   + Evaluación y mitigación   + Tablas para cálculos de probabilidad, impacto   + Cálculo de riesgo * Alcance ( fechas, activos,, redes, dominios e ip’s) * Resumen ejecutivo ( criticidad, porqué, y urgir/repetir la importancia del plan director y su concordancia con el en)   + Vulnerabilidades: recuento, en graficas, cantidad, % y riesgos, definición de las criticidades     - Tablas con la vulnerabilidades más criticas con los campos mínimos ( riesgo, Vulnerabilidad, ip’s afectadas, añadiría mac)   + Discrepancias del personal auditado ( eximición de responsabilidades en caso de errores)   + Limitaciones (se puede comentar falta de credenciales en algun caso) * Detalles técnicos (por vulnerabilidad)   + Nombre   + Ip’s   + Severidad   + Puntuacion cvssv3,   + Vector de ataque, complejidad del ataque, privilegios, interacción del usuario, alcance, confidencialidad, integridad, disponibilidad   + Descripción   + Observaciones   + Evidencia (paso a paso)   \*\*/ |
| Auditoría de procesos y usuarios |
| Políticas debidamente implementadas |
| /\*\*  Es necesario realizar encuestas ( y elaborarlas ) a directivos, empleados, y en este caso alumnos.  Esto es el análisis de los resultados de dichas encuestas  Añadir copia de seguridad de routers  \*\*/ |
| La política de copias está correctamente implementada, garantizando la realización anual de copias de seguridad de los sistemas de información. |
| La política de inventario de activos se encuentra parcialmente implementada, cuenta con un responsable de material, existe un registro de objetos que están involucrados con la información del centro y existen un protocolo referente al reporte de incidencias del material.  Además, en cada aula se encuentra correctamente visible un código qr y email para dicho reporte. |
| Políticas no implementadas |
| No se estipulan tiempos máximos de respuesta ni resolución de incidentes relacionados con el material. Lo que conllevará mayores pérdidas de la calidad de la infraestructura en el largo plazo |
| No se han desarrollado formación a los integrantes de la organización respecto a políticas de escritorio seguro. |
| No se dispone de una Política de Seguridad de la Información. |
| No se han establecido procesos formales para la Gestión de Incidentes de Seguridad y Continuidad de la actividad, que son fundamentales para identificar, responder, **registrar** y analizar la exposición a riesgos de seguridad, así como para mantener las funciones esenciales tras una emergencia o interrupción. |
| Análisis de riesgos |
| El análisis de riesgos informáticos es un proceso que abarca la identificación de activos informáticos, sus vulnerabilidades y amenazas, así como la evaluación de su probabilidad de ocurrencia y el impacto resultante. Esto permite determinar los controles adecuados para aceptar, disminuir, transferir o evitar el riesgo. Durante el análisis, se asigna a cada riesgo una categoría correspondiente junto con su amenaza asociada. Luego, se calcula el nivel de riesgo utilizando la fórmula:  ***Probabilidad×Impacto=Riesgo***  Este riesgo se clasifica en la siguiente escala:   * **Probabilidad (P)**   + 1 Muy baja   + 2 Baja   + 3 Moderada   + 4 Alta   + 5 Muy alta * **Impacto (I)**   + 1 Muy bajo   + 2 Bajo   + 3 Moderado   + 4 Alto   + 5 Muy alto * **Riesgo (R)** Se calcula multiplicando la probabilidad por el impacto.   + 1-5 Bajo   + 6-10 Medio   + 11-15 Alto   + 16-20 Muy alto   + 21-25 Extremadamente alto |
|  |

Baremo de Riesgo

| Muy alta | 5 | 7 | 16 | 20 | 25 |
| --- | --- | --- | --- | --- | --- |
| Alta | 4 | 5 | 9 | 16 | 21 |
| Moderada | 3 | 4 | 7 | 12 | 18 |
| Baja | 2 | 3 | 5 | 11 | 16 |
| Muy Baja | 1 | 2 | 4 | 9 | 15 |
| Probabilidad | X | 1 | 2 | 3 | 4 |
|  | Impacto | Irrelevante | Menor | Serio | Grave |

### Riesgos Inherentes

| **Categoría** | **Amenaza** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- |
| Infraestructura física | Falta de subsanación | Muy alta(5) | Medio (3) | 15 | Establecer plazo máximo para subsanación de incidencias |
| Usuarios | Desconocimiento Seguridad | Alta(4) | Alta(4) | (16) | Planes de formación |
| Puesto de trabajo | Robo Documentación | Alta(4) | Medio(3) | 12 | Planes de formación. Establecimiento de protocolos |
| Usuarios | Desconocimiento de protocolo de reporte | Alta(4) | Medio(3) | 12 | Planes de formación. Establecimiento de protocolos |

### Nivel de riesgo aceptable

El nivel de Riesgo Aceptable es aquel que se ha conseguido reducir o mitigar de tal forma que pueda ser tolerado por la organización teniendo en cuenta los controles y medidas de seguridad a implementar:

| **Categoría** | **Amenaza** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** | **Riesgo Residual** |
| --- | --- | --- | --- | --- |
| Infraestructura física | Falta de subsanación | 15 | Establecer plazo máximo para subsanación de incidencias | 9 |
| Usuarios | Desconocimiento Seguridad | (16) | Planes de formación | 8 |
| Puesto de trabajo | Robo Documentación | 12 | Planes de formación. Establecimiento de protocolos | 6 |
| Usuarios | Desconocimiento de protocolo de reporte | 12 | Planes de formación. Establecimiento de protocolos | 3 |

| Definición de proyectos e iniciativas |
| --- |
| Basándonos en los descubrimientos y pruebas reunidos hasta ahora, es imperativo desarrollar una serie de proyectos e iniciativas en el ámbito de la seguridad de la información. Estos esfuerzos serán fundamentales para contrarrestar los riesgos identificados y garantizar un nivel de riesgo aceptable. |
| A continuación, enumeramos los principales proyectos y políticas a implantar: |

| Id | Medida | Descripción |
| --- | --- | --- |
| 1 | Formación y concienciación | Garantizar que todos los empleados estén siempre al tanto, comprendan y sigan rigurosamente las normativas y medidas de protección en ciberseguridad implementadas. Es crucial informarles sobre los riesgos asociados con el uso indebido de dispositivos y soluciones tecnológicas disponibles. |
| 2 | Procedimiento de Gestión de Incidentes | Garantizar que todos los integrantes de la organización estén familiarizados y utilicen un procedimiento ágil y efectivo para responder ante cualquier incidente relacionado con la seguridad de la información. Comprometiendo a la gestión a cumplir unos plazos definidos y registro de resolución. |

| Formación y concienciación |
| --- |
| La implementación de esta política se divide en: |
| **Difusión de la Política de Seguridad.**  Documentación correctamente redactada y accesible para todo el personal.  **Plan de Formación**   * Procedimientos y controles de seguridad básicos * Necesidad de conocer y cumplir, normas, leyes, contratos y acuerdos. * Concienciar sobre la existencia y peligros de la ingeniería social. * Responsabilidad personal por acción u omisión y posibles sanciones.   **Programas Específicos**  Es conveniente analizar los integrantes del sistema para elaborar perfiles según sus privilegios y criticidad sobre la información. Además, de una actividad formativa introductoria para nuevos empleados.  **Periodicidad de la Formación:**  Establecimiento de frecuencia y actualización de contenidos y refuerzo de mensajes importantes.  **Cultura de Seguridad de la Información:**  Exigencia de alineación de políticas con entidades externas.  **Evaluación del Aprendizaje:**  Evaluaciones periódicas entre empleados. Identificación de áreas de mejora y efectividad de la formación. |
| Procedimiento de Gestión de Incidentes |
| Responsabilidades en la Gestión de Incidentes: |
| 1. **Equipo de respuestas a incidentes.** Dirigida por el delegado designado.    1. Establecer y mantener un marco de gestión de incidentes efectivo.    2. Coordinar la respuesta y el manejo de los incidentes.    3. Realizar análisis posteriores para identificar causas raíz.    4. Tomar medidas preventivas para evitar futuros incidentes similares. 2. **Empleados.** Tienen el *derecho y responsabilidad* de:    * Reportar cualquier incidente que observen, directa o indirectamente. Así como los reportes recibidos.    * Colaborar con el Equipo de Respuesta a Incidentes (ERT) para responder y manejar los incidentes de manera efectiva. |
| Procedimientos en la gestión de incidentes |
| 1. **Identificación de Incidentes:** Todos los empleados tienen el derecho y deber de notificar cualquier incidente que detecten, ya sea de forma directa o indirecta. 2. **Evaluación de Incidentes**: El equipo de respuesta de incidentes (ERI) debe evaluar la gravedad y el alcance de cada incidente. Para ello, es esencial que cuenten con horas dedicadas para la gestión de incidencias y herramientas de ticketing especializadas. Debe quedar constancia de la recepción de la incidencia. 3. **Manejo de Incidentes:** El ERI debe coordinar la respuesta y el manejo de cada incidente conforme a los procedimientos establecidos. Esto incluye la mitigación del impacto y la recuperación de los sistemas y datos afectados, así como la implementación de soluciones de contingencia, el aislamiento de sistemas comprometidos y la restauración de servicios. 4. **Reporte de Incidentes:** El ERT debe informar periódicamente, en un plazo no mayor a 1 mes, de todos los incidentes al equipo directivo de la organización y a las autoridades correspondientes si corresponde, cumpliendo con los requisitos legales y reglamentarios. Es crucial mantener un registro detallado de cada incidente y de la respuesta proporcionada para futuras referencias. 5. **Análisis de Incidentes:** Tras cada incidente, el ERT debe llevar a cabo un análisis exhaustivo para identificar las causas subyacentes y tomar medidas preventivas. Esto puede incluir la implementación de medidas adicionales de seguridad, la actualización de políticas y procedimientos, y la formación del personal. 6. **Comunicación y Entrenamiento:** Es esencial proporcionar formación a todos los empleados y contratistas sobre cómo informar de los incidentes y cómo responder eficazmente a ellos. Asimismo, mantener una comunicación efectiva entre el ERT y los empleados garantiza que todos estén informados sobre la respuesta y el manejo de los incidentes. 7. **Revisión de la Política:** La política de gestión de incidentes debe ser revisada periódicamente para asegurar su eficacia y adecuación a las cambiantes necesidades de la organización. Esto implica revisar los procedimientos, políticas y herramientas utilizadas por el equipo de respuesta. |
| Reporte de eventos |
| La directriz para el Reporte de Eventos de Seguridad de la Información, tiene como propósito establecer procedimientos claros y consistentes para la documentación y el reporte de incidentes de seguridad de la información.  A continuación, se detallan algunas consideraciones importantes:   1. **Identificación de los elementos necesarios para el reporte:**    * Fecha y hora.    * Descripción.    * Sistemas o datos afectados.    * Acciones tomadas para mitigar el incidente.    * Resultados de la evaluación de riesgos. 2. **Proceso de reporte:**    * Los reportes de eventos de seguridad de la información deben realizarse de manera telemática, por defecto, por correo electrónico a la dirección dedicada para este propósito. Es recomendado el uso de herramientas de reporte como glpi.    * El reporte debe hacerse tan pronto como sea posible después de la detección del incidente. 3. **Obligaciones de los reportadores**    * Es obligatorio reportar cualquier evento de seguridad de la información tan pronto como sea posible después de su detección. 4. **Obligaciones de los receptores del reporte**    * Todos los reportes deben ser recibidos y documentados de modo que quede constancia de su recepción.    * Se debe investigar el incidente para determinar la causa y la magnitud del mismo.    * Debe mantenerse la confidencialidad y seguridad de la información en todo momento. 5. **Registro y seguimiento**    * Se debe realizar un seguimiento hasta la resolución, con actualizaciones del estado no mayores a 2 meses.    * Los resultados del seguimiento deben documentarse y archivarse adecuadamente para referencia futura. |
| Clasificación / Taxonomía de los Ciberincidentes |
| Se recomienda usar la siguiente clasificación de incidentes de seguridad estándar de INCIBE → <https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2019/Guia-Nacional-de-Notificacion-y-Gestion-de-Ciberincidentes.pdf> |

| Clasificación y priorización |
| --- |

| Prioridad | Política | Descripción |
| --- | --- | --- |
| Alta | Formación y concienciación | Asegurar que, en  todo momento, los  empleados conocen,  entienden y cumplen  las  normas y las  medidas de  protección en  materia de  ciberseguridad  adoptadas,  advirtiéndoles de los  riesgos que puede  suponer un mal uso  de los dispositivos y  soluciones  tecnológicas a su  alcance |
| Alta | Procedimiento de Gestión de Incidentes | Asegurarnos de que  todos los miembros  de la organización  conocen y aplican  un procedimiento  rápido y eficaz para  actuar ante  cualquier incidente  en materia de  seguridad de la  información. |

| Implementación del Plan Director de Seguridad |
| --- |
| Tras la aprobación del PDS, se procederá a su ejecución, adaptando su metodología de gestión a la empleada habitualmente por la organización.  Con el fin de promover el éxito en el logro de los objetivos, se llevarán a cabo las siguientes acciones:   1. Realizar una presentación general del plan a las personas implicadas, asegurando una comprensión clara de sus objetivos y estrategias. 2. Asignar las responsabilidades para cada uno de los proyectos incluidos en el plan y proporcionar los recursos necesarios para su implementación efectiva. 3. Establecer la periodicidad de revisión de cada proyecto y del plan en su conjunto, considerando que cambios significativos en la organización pueden requerir una revisión integral del plan. 4. A medida que se alcancen los hitos acordados, se verificará que los riesgos identificados hayan sido tratados adecuadamente, garantizando así la gestión eficaz de los mismos durante la ejecución del plan. |

| Obligaciones del personal |
| --- |
| Todos los miembros del IES El Rincón tienen la obligación de conocer y cumplir el Plan Director de Seguridad.  Se implementará un programa de concienciación en seguridad que abarque a todos los miembros al menos una vez al año. Además, se establecerá un programa de concienciación continua para garantizar que todos los miembros, especialmente los nuevos, reciban formación periódica en materia de seguridad.  Aquellas personas con responsabilidad en el uso, operación o administración de sistemas de Tecnologías de la Información y Comunicación (TIC) recibirán formación para el manejo seguro de los sistemas según lo requiera su función. Esta formación será obligatoria antes de asumir cualquier responsabilidad, ya sea en una primera asignación o en caso de cambio de puesto de trabajo o de responsabilidades dentro de la organización. |

| Terceras partes |
| --- |
| Cuando IES El Rincón establezca relaciones estratégicas con otros organismos o maneje información proveniente de estos, se les involucrará en el Plan Director de Seguridad. Se establecerán canales para la comunicación y coordinación, así como procedimientos de actuación para responder a incidentes de seguridad de manera efectiva.  En el caso de utilizar servicios de terceros o compartir información con ellos, se les informará sobre esta Política de Seguridad y la Normativa correspondiente. Estos terceros estarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para cumplirla. Se establecerán procedimientos específicos para reportar y resolver incidentes, y se garantizará que el personal de terceros esté debidamente capacitado en seguridad, al menos al mismo nivel que lo establecido en esta Política.  Si alguna parte de la Política no puede ser cumplida por un tercero según lo requerido, se solicitará un informe al Responsable de Seguridad que detalle los riesgos y cómo abordarlos. Este informe deberá ser aprobado por los responsables de la información y los servicios involucrados antes de proceder. |

| Anexos |
| --- |
| Inventario de activos |
|  |
| Informe técnico |
|  |