SecureEPN: Estrategia de seguridad informática

Quito-Ecuador

DESCRIPCIÓN GENERAL DE LA PRÁCTICA

Título	***SecureEPN: Estrategia de seguridad informática***
Palabras clave	Seguridad informática, prevención, incidentes de seguridad
Criterios de excelencia	Estrategia, Liderazgo
Institución responsable de la práctica	Escuela Politécnica Nacional
Ciudad	Quito
País	Ecuador
Teléfono	+593993362889
Sitio web de la institución/Facultad/Centro	www.csirt-epn.edu.ec

DATOS DE LA PERSONA RESPONSABLE DE LA PRÁCTICA

Nombres y apellidos	MARIA DANIELA CORDOVA PINTADO
Cargo	Oficial de Seguridad
Unidad/Facultad/Escuela	Centro de Respuesta a Incidentes de Seguridad Informática
Correo electrónico	daniela.cordova@epn.edu.ec
Teléfono	+593993362889
Sitio web	www.csirt-epn.edu.ec

SecureEPN: Estrategia de seguridad informática

DESCRIPCIÓN GENERAL DE LA PRÁCTICA

Resumen ejecutivo

La creación de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) en la Escuela Politécnica Nacional, responde a la creciente necesidad de proteger la integridad, confidencialidad y disponibilidad de los recursos informáticos en un entorno académico interconectado y expuesto a ciber amenazas.

Los principales objetivos del CSIRT se centran en la prevención, detección, respuesta, investigación y concienciación en ciberseguridad. La prevención es clave para evitar incidentes de seguridad, y para ello, el equipo desarrolla políticas, normas y procedimientos que promueven buenas prácticas en el uso de recursos tecnológicos por parte de la comunidad universitaria. Además, implementa sistemas de monitoreo y análisis de tráfico para detectar de manera temprana cualquier actividad sospechosa que pueda indicar un posible ataque o violación de la seguridad.

La razón y necesidad de establecer un CSIRT en la EPN son varias. En primer lugar, las instituciones educativas se han convertido en objetivos atractivos para los ciberdelincuentes debido a la abundancia de datos sensibles y recursos valiosos que manejan. La creciente sofisticación de las amenazas exige una respuesta especializada para enfrentar los desafíos de seguridad y proteger la información generada por la comunidad. Además, las universidades están sujetas a regulaciones y leyes como la de protección de datos que exigen el establecimiento de medidas de seguridad adecuadas para cumplir con los estándares requeridos. La imagen institucional puede verse afectada por incidentes de seguridad, lo que disminuye la confianza de estudiantes, personal y colaboradores, por lo que la creación de un CSIRT ayuda a mantener una imagen positiva y generar confianza en la comunidad politécnica.

Desde la creación del CSIRT-EPN, se ha logrado una reducción significativa del 84% en la cantidad de incidentes de seguridad gestionados, lo cual se traduce en una mayor capacidad para detectar y responder a amenazas de seguridad en un plazo más breve, minimizando el impacto potencial en la institución. La implementación de procedimientos, protocolos y la participación activa del equipo de seguridad han permitido una respuesta más rápida y efectiva a los incidentes.

Este proyecto tiene un alto nivel de ser implementado en otras instituciones de educación superior que necesiten fortalecer la seguridad informática en un entorno académico sujeto a amenazas en constante crecimiento, dado su aporte en la construcción de un entorno digital más seguro y confiable para toda la comunidad universitaria.

Esta práctica contribuye al cumplimiento de los objetivos estratégicos de la EPN de "Garantizar un ambiente de trabajo seguro, creativo y productivo con infraestructura de primer orden" y "Proveer soluciones tecnológicas oportunas e innovadoras a los problemas de la sociedad. De igual manera aporta al Objetivo 16 de Desarrollo Sostenible: Promover sociedades justas, pacíficas e inclusivas.

Planificación de la Práctica:

La creación del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-EPN) en la Universidad Politécnica Nacional (EPN) se fundamenta en diversas causas que ponen en riesgo la integridad y confidencialidad de los recursos informáticos. El aumento en la sofisticación de las amenazas cibernéticas representa una preocupación constante para la institución, ya que los ciberdelincuentes buscan acceder a datos sensibles y recursos valiosos. Esta situación afecta

directamente a la comunidad politécnica y a los colaboradores externos, generando una amenaza latente para la reputación institucional y la seguridad de la información.

La creación del CSIRT-EPN involucra a varios grupos de interés, siendo el equipo que conforma el centro y toda la comunidad politécnica los más relevantes. El equipo del centro desempeña un papel crucial en la identificación y solución del problema, ya que lidera la planificación y ejecución de medidas de seguridad informática. Por otro lado, la comunidad politécnica representa un grupo vital para el CSIRT, ya que son los principales usuarios de los recursos informáticos y, por lo tanto, se beneficiarán directamente de los servicios de seguridad y protección ofrecidos por el equipo.

La metodología utilizada para la identificación de alternativas de solución se basó en un análisis exhaustivo de las estructuras que componen un equipo de respuesta a incidentes informáticos. Se evaluaron procesos, procedimientos, directrices e infraestructura necesaria para establecer un CSIRT eficiente. Las alternativas de solución fueron identificadas a partir de mejores prácticas y experiencias de otros CSIRTs nacionales e internacionales, adaptadas a las necesidades y características de la EPN.

El CSIRT-EPN contribuye a los objetivos estratégicos de la EPN de "Garantizar un ambiente de trabajo seguro, creativo y productivo con infraestructura de primer orden" y "Proveer soluciones tecnológicas oportunas e innovadoras a los problemas de la sociedad". Los objetivos generales que se proponen para crear un CSIRT son:

- Detectar, identificar y apoyar técnicamente a la comunidad politécnica en el manejo de incidentes de seguridad informática.
- Detectar e investigar las amenazas de seguridad informática.
- Publicar los resultados e investigaciones de la institución que estén relacionadas a la gestión del CSIRT-EPN.

Además de estos objetivos generales, se proponen dos objetivos adicionales medibles:

- Reducción del tiempo de respuesta a incidentes: Establecer un indicador de tiempo para evaluar la eficiencia del CSIRT-EPN en responder a incidentes de seguridad. El objetivo será reducir el tiempo de respuesta promedio a incidentes en un 30% en comparación con el año anterior 2022. Tiempo actual promedio de resolución de un incidente de seguridad es 6 días.
- Incremento de la concienciación en ciberseguridad: Medir el nivel de concienciación sobre ciberseguridad en la comunidad politécnica antes y después de la implementación del CSIRT-EPN.

La creación del CSIRT-EPN ha generado valor agregado a la Institución, ya que ha permitido beneficiar directamente a la comunidad politécnica al contar con un ambiente digital más seguro, que fomenta un entorno de aprendizaje y trabajo confiable. Los servicios del CSIRT-EPN, que incluyen medidas proactivas, reactivas y de gestión de calidad, generan protección ante incidentes de seguridad informática, como accesos no autorizados, phishing y robo de identidades. Además, el CSIRT tiene su código de ética, el que fortalece la confianza y la responsabilidad en el manejo de la información.

Desarrollo y ejecución de la Práctica:

Para la implementación del CSIRT-EPN se realizó una planificación que incluyó diversas etapas y estrategias para garantizar la efectividad de esta iniciativa en la Institución.

Diagnóstico y Planificación Inicial:
En esta etapa, se realizó un diagnóstico de la situación de seguridad informática de la EPN. Se identificaron las principales amenazas y vulnerabilidades, así como las necesidades y desafíos específicos de la comunidad politécnica en materia de ciberseguridad. Con base en este

diagnóstico, se elaboró el Plan de Implementación del CSIRT-EPN, definiendo los objetivos, alcance, recursos necesarios y cronograma de actividades.

- **Aprobación y Autorización**:

El proyecto fue sometido a la aprobación de la máxima autoridad Institucional. Una vez obtenida la autorización, se procedió a la asignación de recursos físicos, tecnológicos y humanos para la implementación del equipo de respuesta a incidentes.

- **Conformación del CSIRT-EPN**:

Se designaron los miembros del CSIRT-EPN, quienes contaban con conocimientos en redes, programación y seguridad informática y asumieron el rol de Oficiales de Seguridad. El equipo se integró inicialmente con cuatro miembros, que posteriormente creció a seis para abordar las necesidades crecientes de la universidad.

- **Desarrollo de Políticas y Directrices**:

Como parte de la implementación, se generó una línea base de políticas y directrices como la Política de gestión de incidentes de seguridad informáticos, Política de clasificación de la información, Política de retención de la información, entre otros, que normaron el actuar de los miembros del CSIRT en materia de seguridad. Estas incluyeron políticas internas y procedimientos, como la clasificación de la información, protección de datos, retención de la información, entre otras.

- **Infraestructura Tecnológica**:

El CSIRT-EPN utilizó recursos tecnológicos proporcionados por la institución, complementada con herramientas de código abierto que permitieron desplegar servicios internos para la gestión documental, correo electrónico, tickets de incidentes y gestión de vulnerabilidades.

- **Capacitación del Personal**:

El equipo de respuesta a incidentes recibió y actualmente continúa recibiendo capacitación en diversas áreas de seguridad informática, incluyendo Ethical Hacking, Gestión de Proyectos, Gestión de Incidentes y Vulnerabilidades, entre otros. Esto garantiza que el personal esté preparado para enfrentar los desafíos de seguridad de manera efectiva.

- **Plan de Trabajo y Cronograma de Actividades:**

A continuación, se describen las actividades clave y los recursos humanos, físicos e infraestructura asignados a cada etapa:

Mes 1: Diagnóstico y Planificación Inicial

Actividades:
Realización del diagnóstico de seguridad informática, identificando amenazas y vulnerabilidades.
Elaboración del Proyecto para implementación del CSIRT-EPN, definiendo objetivos y alcance.
Asignación del equipo de proyecto y responsabilidades.
Recursos Humanos:
Equipo del CSIRT-EPN: Coordinador de Proyecto, Oficiales de Seguridad.

Mes 2: Conformación del CSIRT-EPN
Actividades:
Integración de los miembros del CSIRT-EPN.
Capacitación del equipo en áreas de seguridad informática.

Mes 3: Desarrollo de Políticas y Directrices

Actividades:
Generación de políticas y procedimientos de seguridad para el CSIRT-EPN.
Recursos Humanos:
Equipo del CSIRT-EPN: Coordinador de Proyecto, Oficiales de Seguridad.
Expertos legales para asesoramiento en políticas.

Mes 4: Infraestructura Tecnológica
Actividades:
Implementación de infraestructura física proporcionada por la institución.
Configuración de herramientas de código abierto para gestión documental, correo electrónico, tickets de incidentes y gestión de vulnerabilidades.
Recursos Humanos:
Equipo del CSIRT-EPN: Coordinador de Proyecto, Oficiales de Seguridad.
Personal de TI para la configuración de herramientas.
Recursos Físicos e Infraestructura:
Espacios físicos para el funcionamiento del CSIRT-EPN.
Servidores y equipos de TI para la infraestructura tecnológica.

Mes 5: Cooperación con CSIRTs Nacionales e Internacionales

Actividades:
Establecimiento de relaciones de cooperación con otros CSIRTs.
Intercambio de experiencias y mejores prácticas en seguridad informática.
Recursos Humanos:
Equipo del CSIRT-EPN: Coordinador de Proyecto, Oficiales de Seguridad.

Mes 6: Evaluación y Ajustes
Actividades:
Evaluación del progreso y cumplimiento de objetivos.
Identificación de posibles ajustes o mejoras en el plan de trabajo.
Recursos Humanos:
Equipo del CSIRT-EPN: Coordinador de Proyecto, Oficiales de Seguridad.

Presupuesto Inicial:

El presupuesto inicial de aproximadamente 300.000,00 dólares se distribuyó de la siguiente manera:

Recursos Humanos: Sueldos y capacitación para el equipo del CSIRT-EPN.
Recursos Físicos e Infraestructura: Mantenimiento y actualización de equipos de TI y servidores.
Herramientas de Código Abierto: Implementación y actualización de herramientas de seguridad.
Gastos Operativos: Licencias, capacitaciones y otros gastos relacionados con la operación del CSIRT-EPN.

Durante la implementación, pueden surgir cambios sustantivos en la planificación debido a factores imprevistos o nuevas necesidades identificadas. En el CSIRT-EPN no existieron estos cambios. Sin embargo, en caso de que se den, estos deben ser justificados adecuadamente para garantizar la eficacia en el proceso de implementación.

Para lograr los objetivos del CSIRT-EPN, se contó con la colaboración y apoyo de otras áreas de la institución. Esto incluyó el trabajo conjunto con el área de tecnologías de la información, comunicaciones y otros departamentos para asegurar el éxito de la implementación. Además, se estableció una cooperación activa con CSIRTs nacionales e internacionales, lo que permitió el intercambio de experiencias y mejores prácticas para fortalecer la capacidad de respuesta del CSIRT-EPN.

Resultados de la práctica:

Los resultados obtenidos con la implementación del CSIRT-EPN en la Escuela Politécnica Nacional son los siguientes:

Nivel de Eficacia Alcanzado:

Uno de los objetivos principales de la creación del CSIRT-EPN fue mejorar la eficacia en la gestión de incidentes de seguridad informática en la institución. Antes de la implementación, los incidentes de seguridad no se reportaban y, por lo tanto, no se abordaban a tiempo. Sin embargo, desde la creación del CSIRT-EPN, se ha logrado una reducción significativa del 84% en la cantidad de incidentes de seguridad gestionados. Esto se traduce en una mayor capacidad para detectar y responder a amenazas de seguridad en un plazo más breve, minimizando el impacto potencial en la institución.

Nivel de Eficiencia Alcanzado:

Antes de la implementación del CSIRT-EPN, la atención a incidentes carecía de un enfoque estructurado. Con la creación del equipo, se estableció un proceso de gestión de incidentes más eficiente y estructurado. Actualmente, el CSIRT-EPN gestiona un promedio de 0.5 incidentes de seguridad por año, lo que representa una mejora en términos de eficiencia. La implementación de procedimientos, protocolos y la participación activa del equipo de seguridad han permitido una respuesta más rápida y efectiva a los incidentes.

Incremento de la concienciación en ciberseguridad:

Se logró que la comunidad politécnica mejorara su nivel conocimiento y comprensión de las prácticas seguras de uso de recursos informáticos, pasando del 13% en 2019 al 47% en 2022, lo cual evidencia el nivel de compromiso de los estamentos universitarios de implantar una cultura de seguridad en la comunidad politécnica.

Relación Costo-Beneficio:

El presupuesto anual asignado al equipo asciende a aproximadamente 300,000 dólares e incluye conceptos como capacitación, licencias, mantenimiento de equipos, adquisición de servidores, actualizaciones y otros gastos operativos. No obstante, es importante destacar que este gasto se traduce en una notable disminución de incidentes y vulnerabilidades, lo que, en última instancia, se traduce en un potencial ahorro significativo en términos de pérdida de datos, tiempo y recursos.

Indicadores de Satisfacción de Grupos de Interés:

Los grupos de interés, que incluyen la comunidad politécnica en su conjunto, han experimentado una mejora significativa en la percepción de la seguridad de la información. La posibilidad de reportar incidentes y recibir una respuesta efectiva ha aumentado la confianza en la institución. Además, se han implementado mecanismos de retroalimentación y encuestas para medir la satisfacción, y los resultados positivos.

Sostenibilidad en el Tiempo:

Desde sus inicios, el CSIRT-EPN ha venido evolucionando en el tiempo. Esto se ha logrado a través de la revisión y actualización anual de las directrices y políticas, lo que garantiza que la práctica siga siendo relevante y efectiva en un entorno de seguridad de la información en constante evolución.

Además de los aspectos cuantitativos mencionados, es importante destacar los logros cualitativos derivados de la implementación del CSIRT-EPN. Estos incluyen la creación de una cultura de seguridad en la comunidad politécnica, la generación de herramientas innovadoras para el monitoreo de aplicaciones y la promoción de la investigación en seguridad informática a través de

tesis de grado. El CSIRT-EPN también ha colaborado activamente a nivel internacional con otros CSIRTs en la detección de amenazas, lo que refuerza su posición en la comunidad de nacional e internacional.

Evaluación y revisión de la práctica:

Dentro de la evaluación de esta práctica, en la planificación que se realiza cada año, se han generado diferentes métricas, las cuales incluyen:

- Porcentaje de solicitudes resueltas en el soporte más básico N1 (nivel 1) sobre seguridad informática
- Porcentaje de solicitudes resueltas en el soporte especializado N2 (nivel 2) sobre seguridad informática
- Porcentaje de proyectos ejecutados de seguridad informática

Estos indicadores son analizados con la finalidad de detectar los mayores puntos de incidencias y de esta forma fomentar la mejora en donde se considera se tiene más solicitudes. Con estos resultados se implementan los planes de concientización de ser el caso y la creación de nuevos proyectos.

Cada año se revisan las directrices que se han generado con el fin de actualizarlas en los casos pertinentes, o implementar nuevas para seguir coordinando el trabajo de seguridad informática con la realidad nacional.

Además, desde el CSIRT-EPN se han propuesto varias políticas como por ejemplo la "Política de uso de la información, activos de información institucional y seguridad informática" y la "Política de Tratamiento y Protección de Datos Públicos". De esta forma el CSIRT-EPN continua a la vanguardia en temas de seguridad y facilita la ejecución de las tareas de seguridad en la Institución.

El dejar de actuar frente a las posibles amenazas o dejar de implantar una cultura de seguridad en los funcionarios de la EPN mediante las continuas charlas y conferencias de seguridad, conlleva un riesgo en las operaciones de la EPN, por lo que es de suma importancia encontrar los puntos críticos en la gestión de las seguridades para generar las estrategias que permitan mitigarlas.

Carácter Innovador de la práctica

Entre los aspectos innovadores de esta buena práctica de implementar un CSIRT, se pueden destacar:

- Implantación de Nuevos Procedimientos de Seguridad de la Información:

El CSIRT-EPN ha desarrollado nuevos procedimientos para la gestión de incidentes de seguridad. Estos procedimientos incluyen la identificación oportuna de incidentes, su clasificación y resolución. La metodología implementada es un estándar utilizado en otros equipos de seguridad en la región.

- Atención y Resolución de Incidentes de Seguridad Informática:

Capacidad para la detección y respuesta a incidentes de seguridad oportuno. La creación e implementación de sistemas para el monitoreo y respuesta a incidentes que permite minimizar posibles vulnerabilidades o perdidas en la institución.

- Creación de una Cultura de Seguridad:

El CSIRT-EPN ha desempeñado un papel relevante en la creación de una cultura de seguridad en toda la comunidad politécnica. La sensibilización y educación en seguridad informática son

componentes clave de esta cultura y han resultado en una mayor conciencia y responsabilidad por parte de los usuarios finales.

- Desarrollo de Herramientas Innovadoras:

El equipo ha desarrollado herramientas innovadoras para el monitoreo de aplicaciones y sistemas. Estas herramientas permiten una supervisión constante y proactiva, lo que es esencial en un entorno de seguridad informática en constante cambio.

- Promoción de la Investigación en Seguridad Informática:

El CSIRT-EPN ha fomentado la investigación en seguridad informática al plantear temas para tesis de grado y trabajos de doctorado. Esta iniciativa contribuye al crecimiento del conocimiento en el campo de la seguridad informática.

- Colaboración Internacional:

El equipo ha establecido colaboraciones internacionales con otros CSIRTs, no solo a nivel nacional sino también en América y Europa. Esta colaboración en pro de la detección de nuevas amenazas.

Finalmente, el CSIRT-EPN continúa implantando dentro de la Institución una cultura de seguridad informática, logrando que la gestión de información tanto física como digital se lleve con mayor cuidado por parte de nuestra comunidad, previniendo de esta manera intrusiones no autorizadas en las redes y en los sistemas.

Divulgación de la práctica

El equipo ha implementado algunos mecanismos de divulgación como los que se presentan a continuación:

- Participación en Redes de Colaboración:

El CSIRT-EPN ha establecido colaboraciones con otros equipos de respuesta a incidentes de seguridad informática a nivel nacional e internacional, tanto es así que pertenece al Foro de equipos de respuesta a Incidentes (FIRST). Esta colaboración no solo fortalece la capacidad del equipo para responder a amenazas, sino que también promueve el intercambio de conocimientos y experiencias entre sus miembros acerca de la seguridad.

- Formación y Capacitación:

El equipo ha desarrollado charlas de formación y capacitación en seguridad informática para todos los miembros de la Comunidad. Estos programas incluyen las sesiones de concienciación diseñados para mejorar la seguridad informática a nivel organizacional.

En el año 2019, el CSIRT participó en el primer evento de seguridad organizado para dar charlas a escuelas fiscales de Quito, donde se trató el tema del Grooming en la red.

- Participación en Iniciativas de Seguridad Colaborativa:

El CSIRT-EPN ha contribuido a iniciativas de seguridad que incluyen la participación en proyectos de investigación y desarrollo en colaboración con otros equipos de seguridad.

Divulgación en Eventos y Conferencias de Seguridad:

El CSIRT-EPN ha participado en eventos y conferencias relacionados con la seguridad informática, así como los organizados por OWASP LatamTour del año 2019, con la charla "Incident response aplicado en el campo educativo".

FUENTES COMPLEMENTARIAS

Añadir páginas web o enlaces. (En caso de enviar varios archivos comprimirlo en un.Zip o .rar)

» Añadir páginas webs o enlaces.

https://www.csirt-epn.edu.ec/
https://www.csirt-epn.edu.ec/normativa
https://url.epn.edu.ec/politica
https://issuu.com/revistaitahora/docs/document_27_ página 32 Revista IT ahora diciembre 2021. Entrega de Premios Líder IT Ecuador 2021.
https://www.epn.edu.ec/cert-seguridad-informatica/
https://www.first.org/members/teams/csirt-epn
https://events.vtools.ieee.org/m/208372