Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Acciones Para Salvaguardar la Protección de los Datos

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Veintisiete
Sep. de 2024

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupode Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Líder
CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

Revisó
Ing. Daniel Palomo
Prof. Especialización en Seguridad Informática

Estado legal:
Periodicidad: MensualISSN:
2806-0164

Universidad Nacional Abierta y a DistanciaCalle 14 sur No. 14-23 |Bogotá D.C Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 27

Septiembre 2024

Acciones para Salvaguardar la Protecciónde Datos

Autores:

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Freddy Julián Leyton
Estudiante
Esp. Seguridad Informática

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

[1]En la actualidad, el entorno digital se ha convertido en la columna de las operaciones empresariales, facilitando el manejo de grandes volúmenes de información y la interacción continua entre empleados, clientes y socios comerciales. Sin embargo, este panorama también ha expuesto a las organizaciones a una variedad de riesgos cibernéticos que pueden comprometer seriamente la seguridad de los datos. Los ciberataques son cada vez más sofisticados, y las brechas de seguridad se han vuelto comunes, afectando no solo la reputación de las empresas sino también su estabilidad financiera y operativa. Ante esta realidad, la protección de datos ha dejado de ser una opción para convertirse en una necesidad estratégica.

Recuperado de: https://www.ikusi.com/mx/blog/ley-de proteccion-de-datos-en-mexico/

Las regulaciones globales, como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Protección de Datos Personales en Colombia, exigen a las organizaciones adoptar medidas estrictas para salvaguardar la información personal y empresarial. Además, la confianza de los clientes está en juego, puesto que cualquier incidente relacionado con la pérdida o el robo de datos puede erosionar la relación construida a lo largo de los años. hasta la formación del personal, cada medida desempeña un papel crucial en la protección de datos y en la garantía de que la información crítica permanezca segura frente a cualquier intento de acceso no autorizado.

[1]https://repositorio.usam.ac.cr/xmlui/bitstream/handle/11506/2036/LEC%20ING%20SIST%200004%202017.pdf?sequence=1&isAllowed=y).

Desarrollo

1. Implementación de políticas de seguridad de la información.

Recuperado de: https://smilecomunicacion.com/seguridad-informatica/politica-de-seguridad/

[2] La base de un entorno digital seguro radica en la adopción de políticas de seguridad de la información, estas políticas deben establecer directrices claras sobre el manejo y protección de datos, abarcando aspectos como la clasificación de la información, controles de acceso, gestión de incidentes de seguridad y procedimientos de respuesta ante brechas de datos. Las políticas deben ser revisadas y actualizadas regularmente para adaptarse a los cambios tecnológicos y normativos. Esto no solo pone en riesgo la [I] Integridad de la información, sino que también puede resultar en pérdidas financieras y reputacionales significativas, Por lo anterior, es crucial que las empresas comprendan estos riesgos y adopten medidas proactivas para fortalecer su seguridad. (Perafán Ruiz & Caicedo Cuchimba, Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca, 2014)

- Desarrollo y definición de políticas: El primer paso en la implementación de políticas de seguridad es el desarrollo y definición de las mismas. Este proceso debe estar alineado con los objetivos estratégicos de la organización y considerar el cumplimiento de las normativas y leyes aplicables, como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley de Protección de Datos Personales en América Latina.

Evaluación de riesgos: Antes de redactar cualquier política, es esencial realizar una evaluación exhaustiva de riesgos para identificar las amenazas potenciales que enfrenta la organización. Esta evaluación permite priorizar los riesgos más críticos y diseñar políticas que aborden específicamente esos puntos vulnerables.

Recuperado de: https://grctools.software/2019/10/18/analisis-y-evaluacion-de-riesgos-de- seguridad-de-la-informacion-identificacion-de-amenazas- consecuencias-y-criticidad/

Estructura de las políticas: Las políticas deben ser claras, concisas y estructuradas de manera que sean fácilmente comprensibles por todos los empleados. Una política típica debe incluir el objetivo, el alcance, las responsabilidades, las directrices, y los procedimientos para su aplicación. Es vital que las políticas cubran todos los aspectos de la seguridad de la información, incluyendo la gestión de accesos, el manejo de datos sensibles, la respuesta a incidentes, y el uso de dispositivos móviles, entre otros.

- Aprobación y difusión: Una vez redactadas, las políticas deben ser revisadas y aprobadas por la alta dirección de la organización. Este respaldo es crucial para asegurar que las políticas sean tomadas en serio y se apliquen de manera efectiva en todos los niveles de la empresa.

Comunicación efectiva: Las políticas de seguridad deben ser comunicadas de manera efectiva a todos los empleados y partes interesadas. Esto puede lograrse a través de sesiones de formación, manuales de usuario, y plataformas digitales donde las políticas estén disponibles para consulta en cualquier momento. Es fundamental que los empleados comprendan la importancia de las políticas y cómo su cumplimiento afecta a la seguridad general de la organización.

Asignación de responsabilidades: Cada política debe definir claramente las responsabilidades de las diferentes áreas y personas dentro de la organización. Por ejemplo, el equipo de TI puede ser responsable de implementar las medidas técnicas, mientras que el departamento de recursos humanos podría gestionar la capacitación y concienciación del personal. Asignar estas responsabilidades asegura que cada aspecto de la política se cumpla de manera efectiva.

- Implementación práctica: La implementación práctica de las políticas de seguridad de la información implica traducir las directrices teóricas en acciones concretas que se integren en las operaciones diarias de la organización.

Integración con procesos de negocio: Las políticas de seguridad deben estar integradas en los procesos de negocio existentes. Esto significa que las medidas de seguridad no deben ser vistas como un obstáculo, sino como parte del flujo de trabajo estándar. Por ejemplo, la autenticación multifactor (MFA) debe implementarse en los procesos de inicio de sesión sin afectar la productividad de los empleados.

Uso de tecnología: La tecnología juega un papel crucial en la implementación de políticas de seguridad. Herramientas como firewalls, sistemas de prevención de intrusiones (IPS), y soluciones de cifrado ayudan a reforzar las políticas, protegiendo los datos de accesos no autorizados y ciberataques. Es importante seleccionar y configurar estas herramientas de manera que respalden los objetivos establecidos en las políticas.

Capacitación y concienciación: Los empleados deben recibir capacitación continua para asegurarse de que entienden las políticas de seguridad y cómo aplicarlas. Esta capacitación debe incluir simulaciones de ataques de phishing, talleres sobre el manejo seguro de la información, y sesiones sobre el uso seguro de dispositivos móviles y acceso remoto. La concienciación constante es clave para reducir el riesgo de errores humanos, que son una de las principales causas de incidentes de seguridad.

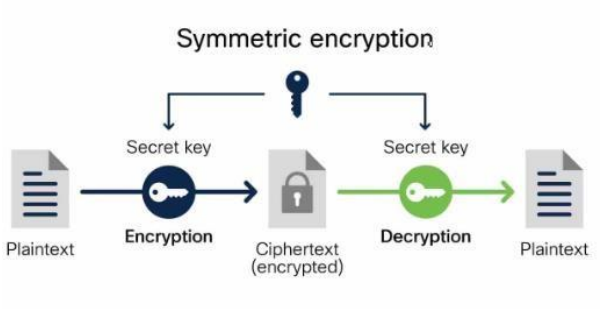
Auditorías de seguridad: Realizar auditorías de seguridad periódicas permite evaluar el cumplimiento de las políticas y detectar posibles brechas o áreas de mejora. Estas auditorías pueden ser internas o externas, y deben ser llevadas a cabo por profesionales con experiencia en seguridad de la información.

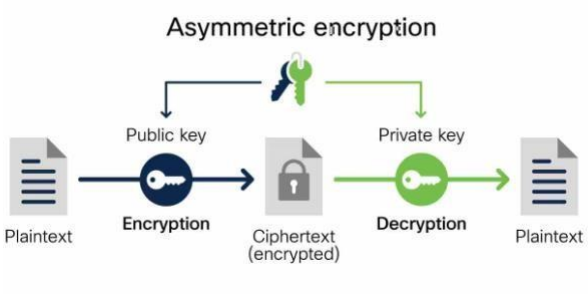
Actualización y mejora continua: Las amenazas a la seguridad de la información evolucionan rápidamente, por lo que las políticas deben ser revisadas y actualizadas regularmente para mantenerse efectivas. Esta revisión debe considerar nuevos riesgos, cambios en la legislación, y la introducción de nuevas tecnologías en la organización

2. Uso de tecnologías de cifrado:

El cifrado es una de las tecnologías más efectivas para proteger la confidencialidad y la integridad de la información, tanto en tránsito como en reposo, este uso de tecnologías de cifrado garantiza que los datos solo sean accesibles para las personas autorizadas, incluso si caen en manos equivocadas. A continuación, se profundizan los aspectos clave del uso de tecnologías de cifrado en el contexto de la seguridad de la información.

- ✓ Cifrado Simétrico.
- ✓ Cifrado Asimétrico





Recuperado de: https://kinsta.com/es/base-de-conocimiento/que-es-la-encriptacion/

[3] https://pdfs.semanticscholar.org/4c28/3c51c7d07e720466c57d17ca9ed422d3bfc4.pdf

Boletín de Ciberseguridad

CIFRADO DE DATOS EN REPOSO

CIFRADO DE DISCOS COMPLETOS — 01

Este enfoque cifra todos los datos en un disco duro o un dispositivo de almacenamiento, lo que garantiza que los archivos estén protegidos incluso si el dispositivo cae en manos

CIFRADO DE BASES DE DATOS — 02

Las bases de datos contienen información crítica y a menudo sensible. Implementar cifrado a nivel de base de datos, ya sea a través de cifrado a nivel de columna o de cifrado completo, ayuda a proteger la información almacenada, incluso si la base de datos es comprometida.

CIFRADO DE DISPOSITIVOS MÓVILES: — 03

Dado el creciente uso de dispositivos móviles en el entorno corporativo, el cifrado de estos dispositivos es esencial. La mayoría de los smartphones modernos ofrecen cifrado de datos de manera predeterminada, asegurando que la información esté protegida si el dispositivo se pierde o es robado

GESTIÓN DE CLAVES

ALMACENAMIENTO SEGURO DE CLAVES: — 01

Las claves criptográficas deben almacenarse de manera segura, utilizando módulos de seguridad de hardware (HSM) o soluciones de gestión de claves específicas. Las claves no deben almacenarse en texto plano ni en ubicaciones no seguras.

ROTACIÓN DE CLAVES — 02

claves criptográficas deben cambiarse regularmente para minimizar el riesgo de que sean comprometidas. La rotación de claves es una práctica recomendada que implica generar nuevas claves y retirar las antiguas, garantizando que los datos cifrados permanezcan seguros a lo largo del tiempo

DISTRIBUCIÓN SEGURA DE CLAVES — 03

La distribución de claves, especialmente en el cifrado simétrico, debe realizarse a través de canales seguros para evitar que las claves sean interceptadas. El uso de cifrado asimétrico para la transmisión de claves simétricas es una práctica común para resolver este problema.

Boletín de Ciberseguridad

CIFRADO DE DATOS EN TRÁNSITO

01 SSL/TLS

Son protocolos criptográficos que proporcionan una comunicación segura en Internet. Estos protocolos se utilizan para cifrar la conexión entre un cliente (por ejemplo, un navegador web) y un servidor, asegurando que los datos intercambiados no puedan ser interceptados o alterados. Los certificados digitales juegan un papel clave en la autenticación de los servidores y la implementación de SSL/TLS

02 VPNS (REDES PRIVADAS VIRTUALES):

Las VPNs utilizan el cifrado para crear una conexión segura entre el dispositivo del usuario y la red de la empresa. Esto es especialmente útil para empleados que trabajan de forma remota o que acceden a la red corporativa desde ubicaciones no seguras, como redes Wi-Fi públicas. El cifrado asegura que los datos transmitidos a través de la VPN no puedan ser interceptados por terceros.

03 CIFRADO DE CORREOS ELECTRÓNICOS

El correo electrónico es una de las formas de comunicación más vulnerables. Utilizar tecnologías como PGP (Pretty Good Privacy) o S/MIME (Secure/Multipurpose Internet Mail Extensions) para cifrar los correos electrónicos garantiza que solo el destinatario pueda leer el mensaje. Estos sistemas utilizan tanto cifrado asimétrico como firmas digitales para proteger la información

3. Formación y concienciación de empleados.

Los empleados son la primera línea de defensa en la protección de datos. Es vital proporcionarles formación continua sobre prácticas de seguridad, como la identificación de correos electrónicos de phishing, la gestión segura de contraseñas y el manejo responsable de la información. Una cultura organizacional que prioriza la seguridad y la protección de datos contribuye significativamente a la reducción de riegos.

Cultura de seguridad: La formación regular promueve una cultura de seguridad dentro de la organización, donde todos los empleados comprenden la importancia de proteger la información y asumen la responsabilidad de mantenerla segura

Reducción del riesgo de errores humanos: La mayoría de las brechas de seguridad son el resultado de errores humanos, como hacer clic en enlaces de phishing, utilizar contraseñas débiles, o compartir información sensible inadvertidamente. A través de la formación, los empleados aprenden a reconocer y evitar estos errores, lo que reduce considerablemente el riesgo para la organización.

Cumplimiento normativo: Muchas normativas de seguridad, como el GDPR o la ISO 27001, requieren que las organizaciones capaciten a sus empleados en temas de seguridad de la información. La formación ayuda a garantizar que la organización cumpla con estas regulaciones, evitando sanciones legales y daños a la reputación. (Bonilla Montoya, Garate Aguirre, & Narváez Zurita, 2024)

4. Control de acceso y autenticación

Establecer controles de acceso sólidos y mecanismos de autenticación multifactor (MFA) es esencial para limitar el acceso a la información solo a personal autorizado. Los sistemas deben estar configurados para registrar y monitorear las actividades de acceso, permitiendo la detección temprana de posibles incidentes de seguridad. Además, la gestión de identidades y accesos (IAM) debe integrarse en todos los niveles de la organización.

(Patiño, Caicedo, & Reina Guaña, 2019)

5. Auditorias y monitoreo continuo

La implementación de auditorías regulares y monitoreo continuo de los sistemas permite identificar y corregir vulnerabilidades antes de que sean explotadas. Herramientas de monitoreo de seguridad, como los sistemas de detección de intrusiones (IDS), juegan un papel crucial en la supervisión del tráfico de red y la identificación de comportamientos sospechosos. Las auditorías periódicas también aseguran que las prácticas de seguridad se mantengan alineadas con las políticas y normativas vigentes.

6. Respuesta a incidentes y plan de recuperación de desastres

Desarrollar un plan de respuesta a incidentes y un plan de recuperación de desastres es fundamental para minimizar el impacto de cualquier brecha de seguridad o incidente cibernético. Este plan debe incluir procedimientos detallados para la contención, erradicación y recuperación de sistemas afectados, así como la comunicación con las partes interesadas. La realización de simulacros regulares ayuda a asegurar que el personal esté preparado para actuar de manera eficaz en caso de un incidente real.

Conclusiones

La protección de datos en el entorno digital es un desafío continuo que requiere un enfoque integral, abarcando desde la implementación de políticas de seguridad hasta la capacitación de losempleados; en este análisis, se ha destacado la importancia de establecer mecanismos robustos de control de acceso y autenticación, la adopción de tecnologías de cifrado y la necesidad de una formación y concienciación constante entre los empleados. Cada uno de estos elementos juega unpapel fundamental en la creación de un entorno digital seguro y confiable.

El control de acceso y la autenticación son esenciales para garantizar que solo las personas autorizadas puedan acceder a los recursos críticos de la organización, mediante de la implementación de tecnologías como la autenticación multifactor y la gestión de privilegios, las empresas pueden reducir significativamente el riesgo de acceso no autorizado y proteger la integridad de los datos.

Por otro lado, el uso de tecnologías de cifrado es crucial para salvaguardar la confidencialidad de la información tanto en tránsito como en reposo. A través de algoritmos de cifrado robustos y una gestión adecuada de las claves criptográficas, las organizaciones pueden proteger sus datossensibles contra el espionaje y el acceso indebido, incluso si la información es interceptada o robada.

Finalmente, la formación y concienciación de los empleados se han identificado como un componente clave en la estrategia de seguridad de la información. Al educar a los empleados sobre las mejores prácticas de seguridad y concienciarlos sobre las amenazas emergentes, las organizaciones pueden mitigar el riesgo de errores humanos, que a menudo son la causa de muchas brechas de seguridad. Además, una cultura de seguridad bien establecida, respaldada porun programa de capacitación continuo y metodologías de aprendizaje variadas, asegura que todoslos miembros de la organización estén alineados con los objetivos de seguridad y contribuyan activamente a proteger los activos digitales.

En conjunto, estas estrategias crean un entorno de seguridad holístico que no solo protege a la organización contra las amenazas actuales, sino que también la prepara para enfrentar desafíos futuros, garantizando la resiliencia y sostenibilidad en el complejo panorama digital.

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- Correo: csirt@unad.edu.co
- Página web: https://csirt.unad.edu.co

Bibliografía

Bonilla Montoya, A. F., Garate Aguirre, J. C., & Narváez Zurita, I. (30 de abril de 2024). *Scielo.* Obtenido de Efectividad de programas de formación en seguridad laboral respecto a la prevención de accidentes laborales: http://scielo.sld.cu/scielo.php?pid=S1990-86442024000200115&script=sci_arttext

Patiño, S., Caicedo, A., & Reina Guaña, E. (29 de abril de 2019). *Modelo de evaluación del Dominio Control de.* Obtenido de https://www.researchgate.net/profile/Paul-Baldeon-Egas/publication/338157912_Personalizacion_de_algoritmo_para_auditar_base_de_datos_en_instituciones_de_educacion_superior/links/5e441e36299bf1cdb924bc0b/Personalizacion-de-algoritmo-para-auditar-base-de-da

Perafán Ruiz, J. J., & Caicedo Cuchimba, M. (2014). *Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf?sequence=3&isAllowed=y

Perafán Ruiz, J. J., & Caicedo Cuchimba, M. (s.f.). *Análisis de Riesgos de la Seguridad de la Información para la Institución.* Obtenido de https://repository.unad.edu.co/bitstream/handle/10596/2655/76327474.pdf?sequence=3&isAllowed=y

Altamirano Yupanqui, J., & Bayona Ore, S. (21 de junio de 2017). *Políticas de Seguridad de la Información: Revisión.* Obtenido de https://pdfs.semanticscholar.org/4c28/3c51c7d07e720466c57d17ca9ed422d3bfc4.pdf

Morales Sandoval, M., Molina de la Fuente, J. A., & De la fuente Anaya, H. H. (2022). *Criptografía: una tecnología antigua en aplicaciones modernas de.* Obtenido de https://www.tamps.cinvestav.mx/~mmorales/divulg/JD06.pdf