CIBERSEGURIDAD
Y MANEJO DE DATOS
INFORMATICOS

AUTORA:
Mgtr. Martha Susana Toapanta Cuastota.

CIBERSEGURIDAD Y MANEJO DE DATOS INFORMATICOS

Mgtr. Martha Susana Toapanta Cuascota

PRIMERA EDICIÓN: Enero de 2025
AUTORA: Mgtr. Martha Susana Toapanta Cuascota
Diseño e impresión: CADHU - EDICIONES
Dirección: Quito-Ecuador

ISBN: 978-9942-45-493-5

DEDICATORIA

A mis queridos padres, por su amor incondicional, enseñanza y apoyo constante, que me guiaron en cada paso de este camino. A mi amado hijo, fuente inagotable de inspiración y alegría, que me motiva a seguir soñando y creando. Este libro es un homenaje a ustedes, mi fuerza y mi hogar.

AGRADECIMIENTOS

A mis padres: Gracias por ser la base de todo lo que soy. Ustedes me enseñaron que el conocimiento se honra con responsabilidad, y que la justicia comienza en casa. Su ejemplo de trabajo, amor y perseverancia me ha dado las herramientas para enfrentar el mundo con la frente en alto y el corazón abierto.

A mi hijo: Tú eres mi impulso, mi horizonte y mi razón para transformar. En tu mirada descubro el futuro que quiero construir, uno donde los derechos, la dignidad y el respeto sean norma. Gracias por recordarme, cada día, que el amor es la fuerza más revolucionaria y que toda lucha tiene sentido cuando es para proteger tu mundo.

A mi comunidad: Ustedes son el tejido vivo de mi historia. En cada diálogo, en cada esfuerzo compartido y en cada resistencia, encuentro la fuerza colectiva que da sentido a mi trabajo. Gracias por caminar conmigo, por sostenerme cuando flaqueo, y por construir día a día un espacio donde pluralidad, justicia y memoria sean principios comunes. Ustedes son prueba de que la transformación empieza por lo que hacemos juntos.

RESUMEN

La ciberseguridad es un campo esencial en la era digital que se ocupa de proteger la información, los sistemas informáticos y las redes frente a amenazas cibernéticas que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos. Su objetivo principal es salvaguardar activos digitales tanto de individuos como de organizaciones mediante estrategias preventivas, técnicas de detección y respuestas efectivas ante incidentes de seguridad.

El libro aborda los fundamentos teóricos y prácticos de la ciberseguridad, presentando los principios básicos como el triángulo CID (Confidencialidad, Integridad y Disponibilidad), junto con las reglas de oro: autenticación, autorización y auditabilidad. Explica las distintas amenazas y vulnerabilidades, desde ataques de malware, phishing y hacking, hasta amenazas internas y fallas en la gestión de datos.

Se profundiza en el manejo seguro de datos informáticos, enfatizando la importancia de la privacidad, el cumplimiento normativo (como el Reglamento General de Protección de Datos) y la implementación de controles técnicos —incluyendo cifrado, firewalls, sistemas de detección (IDS) y prevención de intrusiones (IPS)— para garantizar la protección de la información.

Además, el texto incorpora el enfoque contemporáneo basado en la ciencia de datos y el análisis predictivo, mostrando cómo el machine learning y técnicas de inteligencia artificial están revolucionando la detección de amenazas y la gestión automatizada de incidentes, mejorando la capacidad de anticipar y mitigar ataques sofisticados.

Por último, se presentan metodologías para la gestión integral de la ciberseguridad, cubriendo aspectos organizacionales, normativos y educativos, enfatizando la necesidad de la concienciación y formación continua para usuarios y profesionales, con el objetivo de fortalecer la resiliencia cibernética en un mundo cada vez más interconectado.

INTRODUCCIÓN

En la era digital actual, la información se ha convertido en uno de los activos más valiosos para individuos, organizaciones y gobiernos. La gestión adecuada de datos informáticos y la protección frente a amenazas cibernéticas son elementos esenciales para garantizar la integridad, confidencialidad y disponibilidad de esta información. La ciberseguridad emerge como una disciplina crítica que no solo protege sistemas y redes, sino que también asegura la continuidad operativa y la confianza en los entornos digitales.

Este libro tiene como objetivo ofrecer una visión integral y actualizada sobre los desafíos y las mejores prácticas en ciberseguridad y manejo de datos. Abordaremos desde los fundamentos técnicos y legales hasta las estrategias avanzadas para la prevención, detección y mitigación de ataques cibernéticos. Asimismo, exploraremos la importancia de políticas de manejo responsable de la información y la adaptación a un entorno tecnológico en constante evolución. A través de un enfoque multidisciplinario, este texto busca preparar a profesionales, estudiantes y entusiastas para enfrentar con éxito los retos que plantea la protección de la información en un mundo interconectado, donde la amenaza digital es una realidad constante y en evolución. La seguridad informática ya no es una opción, sino una necesidad vital que afecta a todos los niveles de la sociedad.

En definitiva, este libro es una invitación a comprender y dominar las herramientas y conceptos que permiten asegurar un manejo adecuado de los datos informáticos, promoviendo entornos digitales más seguros y confiables para el presente y el futuro.

La ciberseguridad y el manejo adecuado de datos informáticos son fundamentales para proteger la información digital contra accesos no autorizados, pérdidas y ataques cibernéticos, garantizando la confidencialidad, integridad y disponibilidad de los datos.

CIBERSEGURIDAD

En la era digital contemporánea, donde la información circula a través de redes interconectadas y los sistemas informáticos sostienen procesos críticos en todos los sectores, la **ciberseguridad** se ha consolidado como un componente esencial para la protección de datos, infraestructuras y derechos fundamentales. Esta disciplina abarca el conjunto de prácticas, tecnologías y políticas orientadas a prevenir, detectar y responder a amenazas digitales que puedan comprometer la **confidencialidad**, **integridad** y **disponibilidad** de la información.

La creciente sofisticación de ataques como el *phishing*, el *ransomware*, la suplantación de identidad o las intrusiones en sistemas corporativos ha evidenciado la necesidad de adoptar enfoques integrales que combinen medidas técnicas con marcos normativos robustos. En este sentido, la ciberseguridad no solo es una cuestión tecnológica, sino también jurídica, ética y organizacional.

En Ecuador, la **Ley Orgánica de Protección de Datos Personales (LOPDP)** establece principios clave para el tratamiento seguro de la información, alineándose con estándares internacionales como el **Reglamento General de Protección de Datos (RGPD)** europeo y las normas **ISO/IEC 27001** sobre gestión de seguridad de la información.

La ciberseguridad engloba un conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos de amenazas digitales como malware, ransomware, phishing, y ataques de hackers. Entre los principales pilares están:

- ✓ Confidencialidad: Asegurar que la información solo sea accesible por personas autorizadas.
- ✓ Integridad: Garantizar que los datos no sean alterados de forma no autorizada.
- ✓ Disponibilidad: Asegurar que los datos y servicios estén accesibles cuando se necesitan.
- ✓ Las organizaciones deben implementar estrategias como firewalls, sistemas de detección y prevención de intrusiones, autenticación multifactor y capacitación continua para usuarios, ya que el factor humano es comúnmente la puerta de entrada a ataques.

MANEJO DE DATOS INFORMÁTICOS

En el marco de la transformación digital y la consolidación de gobiernos abiertos, el **manejo de datos públicos** se ha convertido en una herramienta estratégica para fortalecer la transparencia, la participación ciudadana y la eficiencia institucional. Los datos públicos —entendidos como aquellos generados, recolectados o custodiados por entidades estatales en el ejercicio de sus funciones— constituyen un patrimonio informativo colectivo que debe ser gestionado bajo principios de legalidad, accesibilidad, interoperabilidad y reutilización.

El tratamiento adecuado de estos datos implica no solo su publicación en formatos abiertos y accesibles, sino también su organización, preservación y difusión de manera que promuevan el control social, la innovación y la toma de decisiones informadas. En este sentido, iniciativas como los **datos abiertos** permiten que la ciudadanía, la academia y el sector privado puedan analizar, reutilizar y generar valor a partir de la información pública.

Objetivos del manejo de datos públicos

- ✓ **Garantizar el acceso a la información** como derecho fundamental.
- ✓ **Optimizar la gestión pública** mediante el uso de evidencia.
- ✓ **Fomentar la transparencia y la rendición de cuentas.**
- ✓ **Impulsar la innovación social y tecnológica.**
- ✓ **Promover la participación ciudadana informada.**

El manejo de datos públicos no solo responde a obligaciones legales, como las leyes de acceso a la información, sino que también representa una oportunidad para construir una **gobernanza basada en datos**, más inclusiva, eficiente y democrática.

El manejo de datos se refiere a la forma en que se recopilan, almacenan, procesan y protegen los datos digitales. Las buenas prácticas incluyen:

- ✓ Clasificación de datos: Identificar y categorizar la información según su sensibilidad para aplicar niveles adecuados de seguridad.
- ✓ Encriptación: Proteger la información mediante cifrado para que, aun si es interceptada, no pueda ser leída sin la clave apropiada.
- ✓ Control de acceso: Definir y aplicar permisos estrictos para que solo usuarios autorizados puedan acceder o modificar datos.
- ✓ Respaldo y recuperación: Realizar copias de seguridad periódicas para prevenir la pérdida de datos ante incidentes o desastres.
- ✓ Cumplimiento normativo: Ajustarse a leyes y regulaciones locales e internacionales, como GDPR o la Ley Orgánica de Protección de Datos Personales en Ecuador, que establecen estándares para el manejo responsable de información personal.
- ✓ **Manejo de Datos Informáticos**

PLAN DE CONTINGENCIA EN CIBERSEGURIDAD Y MANEJO DE DATOS INFORMÁTICOS

En un entorno digital cada vez más expuesto a riesgos tecnológicos, el diseño e implementación de un **Plan de Contingencia en Ciberseguridad y Manejo de Datos Informáticos** se ha convertido en una necesidad estratégica para garantizar la continuidad operativa, la protección de la información y la resiliencia institucional. Este tipo de plan permite anticiparse a incidentes como ataques cibernéticos, fallos técnicos, desastres naturales o errores humanos, estableciendo protocolos claros para prevenir, responder y recuperar los sistemas afectados.

La creciente dependencia de infraestructuras digitales en sectores críticos —como salud, justicia, educación y administración pública— exige una planificación rigurosa que articule medidas preventivas, mecanismos de respuesta inmediata y estrategias de recuperación. Además, el manejo de datos informáticos debe alinearse con marcos normativos como la **Ley Orgánica de Protección de Datos Personales (LOPDP)** en Ecuador, el **Reglamento General de Protección de Datos (RGPD)** en Europa y estándares internacionales como **ISO/IEC 27001** y **NIST SP 800-34**, que establecen buenas prácticas en seguridad de la información y gestión de incidentes.

Objetivos del Plan de Contingencia

- ✓ Prevenir y mitigar riesgos tecnológicos que afecten la seguridad digital.
- ✓ Establecer protocolos claros de actuación ante incidentes informáticos.

- ✓ Garantizar la recuperación rápida de sistemas y datos críticos.
- ✓ Cumplir con normativas legales sobre protección de datos personales.
- ✓ Fortalecer la cultura organizacional en torno a la seguridad digital.

Este plan no solo responde a la necesidad técnica de proteger activos digitales, sino que también se inscribe en una lógica de **gobernanza responsable**, **derechos digitales** y **soberanía tecnológica**.

Recomendaciones prácticas

Los individuos y organizaciones deben, además:

- ✓ Mantener actualizados los sistemas y software para corregir vulnerabilidades.
- ✓ Utilizar soluciones antivirus y antimalware confiables.
- ✓ Implementar políticas claras de uso aceptable y manejo de dispositivos.
- ✓ Capacitar a los usuarios para identificar intentos de ataques como correos fraudulentos.

La ciberseguridad y el manejo adecuado de los datos informáticos son esenciales para proteger la información ante las crecientes amenazas digitales y garantizar la continuidad de operaciones y la confianza en los sistemas tecnológicos.

CAPITULO I
CIBERSEGURIDAD

LA CIBERSEGURIDAD

La ciberseguridad y el manejo de datos informáticos son fundamentales para proteger la información digital frente a amenazas y garantizar su uso adecuado y seguro en el entorno tecnológico actual. La ciberseguridad se encarga de implementar prácticas, tecnologías y políticas para resguardar sistemas, redes y dispositivos de accesos no autorizados, ataques maliciosos o cualquier tipo de vulneración que pueda comprometer la información. Dado que la información se ha convertido en uno de los activos más valiosos para las personas y organizaciones, mantener su confidencialidad, integridad y disponibilidad es clave.

El manejo de datos informáticos, por su parte, consiste en la correcta recolección, almacenamiento, procesamiento y protección de los datos digitales. Esto incluye asegurar que los datos se mantengan organizados, accesibles solo para usuarios autorizados y protegidos contra pérdidas, manipulaciones o filtraciones. Además, implica cumplir con normativas legales relacionadas con la privacidad y protección de datos personales, como la Ley de Protección de Datos Personales vigente en muchos países.

Juntos, la ciberseguridad y el manejo de datos contribuyen a crear un entorno digital confiable, donde tanto individuos como empresas pueden operar con tranquilidad, minimizando riesgos como el robo de identidad, fraudes, sabotajes o espionaje. En un mundo cada vez más interconectado, estas disciplinas son esenciales para garantizar que el flujo de información sea seguro, eficiente y cumpla con los estándares éticos y legales establecidos.

Por lo tanto, comprender y aplicar principios sólidos de ciberseguridad y manejo de datos es una necesidad imperiosa para proteger la privacidad, mantener la operatividad empresarial y fortalecer la confianza en las tecnologías digitales.

La **ciberseguridad** es una disciplina multidimensional que abarca el diseño, implementación y gestión de estrategias técnicas, organizativas y normativas orientadas a **proteger los activos digitales** frente a amenazas internas y externas. Esto incluye no solo la defensa contra ataques maliciosos como *malware*, *phishing*, *ransomware* o intrusiones, sino también la prevención de errores humanos, fallos técnicos y vulnerabilidades estructurales que puedan comprometer la seguridad de la información.

IMPORTANCIA DE LA CIBERSEGURIDAD

En un mundo cada vez más digitalizado, donde empresas, gobiernos y personas dependen de la tecnología para sus actividades diarias, la ciberseguridad es crucial para evitar perjuicios financieros, pérdida de datos sensibles, daños a la reputación y riesgos a la privacidad personal.

La ciberseguridad es fundamental hoy en día para proteger la información y sistemas digitales frente a amenazas crecientes que pueden afectar la privacidad, economía y seguridad de individuos, empresas y gobiernos.

La ciberseguridad es esencial para proteger la información, garantizar la continuidad operativa, preservar la reputación y cumplir con regulaciones legales, siendo clave para el desarrollo y sostenibilidad de las empresas en la era digital.

1. **Protección de la Información Sensible**

La ciberseguridad salvaguarda datos críticos como información financiera, propiedad intelectual, y datos personales de clientes y empleados, protegiendo a la empresa del robo, pérdida o manipulación de esta información. Un ataque exitoso puede ocasionar fraudes, pérdida de confianza y daños legales y económicos severos

2. **Continuidad y Productividad del Negocio**

Los ataques como ransomware o denegación de servicio (DDoS) pueden detener operaciones, provocando pérdidas financieras importantes y afectando la productividad. La implementación de medidas de seguridad robustas, planes de respuesta y backups es fundamental para minimizar interrupciones y asegurar la operación ininterrumpida

3. **Preservación de la Reputación y la Confianza**

La confianza del cliente es invaluable. Un incidente de seguridad puede erosionarla rápidamente, afectando la imagen empresarial y la lealtad de clientes. Contar con políticas y tecnologías de ciberseguridad demuestra compromiso con la privacidad y protección de datos

4. **Principales Amenazas y Retos**

Las empresas enfrentan amenazas como malware, phishing, ransomware, ataques DDoS, robo de credenciales, vulnerabilidades de software y amenazas internas. La sofisticación y volumen de estos ataques exige una defensa integrada que combine tecnología, capacitación y procesos claros

5. **Inversión y Cultura Corporativa**

Aunque el impacto de la ciberdelincuencia es alto, muchas empresas latinoamericanas destinan presupuestos insuficientes, además de una baja conciencia sobre la ciberseguridad como habilitador estratégico. Es vital incorporar la formación continua del personal, políticas actualizadas y una gobernanza que incluya la ciberseguridad como parte esencial de la gestión empresarial

6. Médidas Recomendadas

- ✓ Implementar autentificación multifactor y gestión segura de contraseñas.
- ✓ Mantener actualizado el software y aplicar parches regularmente.
- ✓ Utilizar firewalls, sistemas de detección de intrusos y soluciones de protección en la nube.
- ✓ Realizar auditorías y simulacros para detectar vulnerabilidades.
- ✓ Fomentar una cultura de ciberseguridad con capacitación y sensibilización.
- ✓ Contar con seguros de riesgos cibernéticos para mitigar impactos económicos

La ciberseguridad no es solo un componente técnico, sino un pilar indispensable para la seguridad integral y sostenibilidad empresarial, especialmente en un mundo cada vez más digitalizado y conectado. Ignorarla puede poner en riesgo la viabilidad económica, legal y reputacional de la empresa. Por ello, una estrategia de ciberseguridad robusta y actualizada es clave para proteger los activos digitales y asegurar el futuro de cualquier organización.

ESTRATEGIAS EFECTIVAS PARA PREVENIR CIBERATAQUES

La prevención de ciberataques en empresas requiere un enfoque integral que englobe desde la formación al personal hasta la implementación de tecnologías avanzadas y políticas robustas de seguridad.

Prevenir ciberataques requiere una combinación de educación, políticas de seguridad, actualización tecnológica y uso de herramientas avanzadas para proteger datos y sistemas, minimizando riesgos y garantizando la continuidad operativa.

Los ciberataques son intentos maliciosos que buscan acceder, dañar o robar información mediante tecnologías digitales. Estos ataques afectan tanto a individuos como a organizaciones, generando pérdidas económicas, daños reputacionales y comprometiendo la privacidad. La prevención es fundamental debido a la creciente sofisticación y frecuencia de estas amenazas.

1. Capacitación y Concienciación del Personal

El factor humano suele ser el eslabón más vulnerable. Capacitar a los empleados para reconocer correos de phishing, links maliciosos y prácticas inseguras es fundamental para evitar intrusiones a través de tácticas de ingeniería social

2. Políticas de Contraseñas Fuertes y Autenticación Multifactor

Implementar políticas que exijan contraseñas complejas, su renovación periódica y el uso de autenticación multifactor (MFA) para accesos críticos reduce significativamente la probabilidad de acceso no autorizado. En un entorno digital cada vez más expuesto a amenazas

como el phishing, el ransomware y los ataques de fuerza bruta, establecer políticas robustas de contraseñas y autenticación multifactor es esencial para proteger los sistemas, datos y usuarios frente a accesos no autorizados

3. **Actualización y Parcheo Constante de Software**

Mantener sistemas operativos, aplicaciones y antivirus actualizados con los últimos parches de seguridad es vital para cerrar vulnerabilidades que los atacantes podrían explotar.

4. **Uso de Tecnologías de Defensa: Firewalls, Anti-malware y Sistemas IDS**

Implementar firewalls para filtrar tráfico no deseado, software antivirus y anti-malware, así como sistemas de detección de intrusiones (IDS), ayuda a prevenir, detectar y responder a ataques en tiempo real

.

5. **Realización de Auditorías y Evaluaciones de Riesgos**

Las auditorías frecuentes permiten detectar vulnerabilidades y brechas en la infraestructura de TI antes de que sean explotadas. Una evaluación de riesgos periódica ayuda a priorizar medidas de protección según el nivel de amenaza

6. **Estrategias de Respaldo y Recuperación**

Realizar copias de seguridad automáticas y almacenar los datos en lugares seguros facilita la recuperación rápida ante un ataque como ransomware, minimizando pérdidas y tiempos de inactividad

7. **Encriptación de Datos Sensibles**

Proteger la información crítica con encriptación tanto en tránsito como en reposo asegura que los datos sean ilegibles para atacantes incluso si se logra acceder a ellos

.

8. **Control de Accesos y Segmentación de Redes**

Limitar el acceso a sistemas y datos solo al personal autorizado usando controles basados en roles (RBAC) y segmentar la red para evitar movimientos laterales en caso de una intrusión

.

9. **Desarrollo de un Plan de Respuesta a Incidentes**

Un Plan de Respuesta a Incidentes es un documento estratégico que permite a una organización anticipar, gestionar y recuperarse de eventos que comprometan la seguridad de sus sistemas informáticos o datos. Su desarrollo debe ser metódico, interdisciplinario y alineado con marcos

como NIST SP 800-61, ISO/IEC 27035 y normativas locales como la LOPDP en Ecuador. Contar con un protocolo claro para detectar, contener, comunicar y remediar incidentes cibernéticos permite actuar de forma rápida y eficiente ante cualquier ataque, minimizando impactos.

10. Uso de Inteligencia Artificial y Herramientas Avanzadas

La incorporación de IA para monitoreo continuo, análisis de patrones sospechosos y gestión automatizada de alertas mejora la detección temprana y respuesta ante amenazas emergentes. La prevención de ciberataques en empresas es un proceso dinámico que combina tecnología, procesos y educación continua. La implementación coordinada de estas estrategias fortalece la seguridad digital, protege datos y garantiza la continuidad del negocio frente a amenazas cada vez más sofisticadas.

Adaptarse y actualizar constantemente estos enfoques es vital para mantenerse un paso adelante de los ciberdelincuentes y proteger el patrimonio informático empresarial. Además, se recomienda realizar auditorías de seguridad y recibir asesoría especializada para evaluar y mejorar la postura de ciberseguridad según el contexto y necesidades específicas de cada organización.

MEJORES PRÁCTICAS PARA AUDITORÍAS DE SEGURIDAD

En un entorno digital marcado por amenazas crecientes y una dependencia crítica de los sistemas informáticos, las auditorías de seguridad se han convertido en un pilar fundamental para garantizar la integridad, confidencialidad y disponibilidad de los activos digitales. Estas auditorías permiten identificar vulnerabilidades, evaluar controles existentes y proponer mejoras que fortalezcan la postura de seguridad de una organización.

La implementación de buenas prácticas en auditorías no solo responde a exigencias normativas —como las establecidas por ISO/IEC 27001, NIST o la Ley Orgánica de Protección de Datos Personales en Ecuador— sino que también promueve una cultura institucional de prevención, transparencia y mejora continua. Al adoptar un enfoque sistemático y multidisciplinario, las auditorías contribuyen a alinear los objetivos técnicos con los marcos legales y estratégicos, facilitando la toma de decisiones informadas y resilientes frente a riesgos emergentes.

1. Planificación clara y definición de objetivos

- ✓ Establecer objetivos concretos y el alcance de la auditoría: cuáles sistemas, redes y procesos serán auditados.
- ✓ Definir los recursos, responsables y cronograma.
- ✓ Considerar normativas aplicables (ISO 27001, NIST, PCI-DSS, RGPD, etc.).

2. Involucrar a la alta dirección y partes interesadas

- ✓ Asegurar el apoyo y compromiso de la dirección para asignar recursos y facilitar la implementación de mejoras.
- ✓ Involucrar a auditores internos y externos para equilibrar conocimiento técnico y objetividad.

3. Evaluación y gestión de riesgos previa

- ✓ Identificar activos críticos y evaluar amenazas, vulnerabilidades e impactos potenciales.
- ✓ Priorizar riesgos para enfocar el esfuerzo de auditoría donde más se necesita.

4. Recolección exhaustiva de datos

- ✓ Utilizar herramientas automatizadas (escáneres de vulnerabilidades, SIEM) y pruebas manuales (pentesting, revisión de código).
- ✓ Revisar documentación, políticas, configuraciones, controles de acceso, redes y sistemas.

5. Análisis detallado y multidimensional

- ✓ Detectar debilidades técnicamente (firewalls, actualizaciones, cifrado, backups), organizativas (políticas, formación), físicas (control de accesos a instalaciones).
- ✓ Considerar amenazas internas y externas, incluyendo factores humanos y procesos.

6. Elaboración de informes claros y accionables

- ✓ Resumir hallazgos y evaluar riesgos asociados.
- ✓ Proponer recomendaciones específicas, priorizadas según impacto y viabilidad.
- ✓ Presentar informes comprensibles para todos los niveles de la organización.

7. Implementación seguimiento y monitoreo continuo

- ✓ Desarrollar un plan de acción con responsables y plazos definidos.
- ✓ Realizar auditorías periódicas y monitoreo constante para adaptarse a nuevas amenazas.
- ✓ Capacitar y sensibilizar al personal regularmente.

8. Adoptar un enfoque holístico y cultural

- ✓ Considerar tecnología, procesos y personas como elementos interrelacionados de la seguridad.
- ✓ Fomentar una cultura organizacional de seguridad y cumplimiento.

9. Uso de estándares y mejores prácticas reconocidas

- ✓ Aplicar marcos como ISO/IEC 27001, NIST Cybersecurity Framework, ANSSI, entre otros.
- ✓ Asegurar cumplimiento legal y regulatorio según región e industria.

10. Realización de auditorías técnicas complementarias

- ✓ Pruebas de penetración de caja blanca y negra para simular ataques reales.
- ✓ Evaluación de políticas y controles mediante entrevistas y revisiones documentales.

Las mejores prácticas para auditorías de ciberseguridad enfatizan una planificación rigurosa, un enfoque multifacético, la comunicación clara de resultados y un compromiso continuo con la seguridad organizacional. La integración de tecnología, normativa, personas y procesos asegura no solo la identificación efectiva de riesgos, sino su mitigación constante en un entorno dinámico.

Esta metodología garantiza que la auditoría no sea solo un evento puntual, sino parte de un ciclo de mejora continua y resiliencia frente a las amenazas cibernéticas crecientes.

ESTRATEGIAS PARA FOMENTAR LA CULTURA DE SEGURIDAD

Fomentar una cultura de seguridad efectiva requiere compromiso del liderazgo, comunicación abierta, capacitación continua, participación activa, evaluación constante y reconocimiento a buenas prácticas. En un entorno institucional cada vez más interconectado y expuesto a riesgos digitales, físicos y organizativos, fomentar una cultura de seguridad se ha convertido en una prioridad estratégica. Esta cultura no se limita a la implementación de controles técnicos o normativos, sino que implica la construcción de valores, comportamientos y prácticas compartidas que promuevan la protección integral de los activos, las personas y los derechos.

Una cultura de seguridad sólida permite anticipar amenazas, responder eficazmente a incidentes y garantizar la continuidad operativa, al tiempo que fortalece la confianza interna y externa en la organización. Para lograrlo, es necesario articular estrategias que involucren a todos los niveles jerárquicos, integren enfoques multidisciplinarios y se alineen con marcos normativos

como la ISO/IEC 27001, el NIST, la Ley Orgánica de Protección de Datos Personales (LOPDP) y principios constitucionales de derechos humanos.

1. **Liderazgo y Compromiso Visible**

El compromiso de la alta dirección es clave. Los líderes deben actuar como ejemplo, participando activamente en la seguridad laboral, asignando recursos adecuados y estableciendo metas claras. Su involucramiento motiva a los empleados y legitima la importancia de la cultura de seguridad dentro de la organización.

2. **Comunicación Abierta y Transparente**

Establecer canales donde los empleados puedan reportar riesgos o inquietudes sin temor a represalias genera confianza y mejora la gestión de riesgos. La información debe difundirse mediante reuniones, boletines, plataformas digitales y sistemas de sugerencias para asegurar la participación de todos.

3. **Capacitación y Formación Continua**

Ofrecer formación periódica y actualizada en temas de seguridad laboral permite que los empleados conozcan riesgos, mejores prácticas y normativas vigentes. La capacitación debe ser práctica, atractiva y adaptada a las necesidades específicas de la organización y sus trabajadores.

4. **Participación Activa de los Empleados**

Involucrar a los empleados en comités de seguridad, inspecciones y análisis de incidentes genera un sentido de pertenencia y responsabilidad compartida. La colaboración fortalece la cultura y facilita la identificación temprana de riesgos y el desarrollo de soluciones efectivas.

5. **Reconocimiento y Recompensas por Buenas Prácticas**

Implementar sistemas de incentivos fortalece la motivación hacia comportamientos seguros. Premiaciones, reconocimientos públicos o incentivos económicos destacan y refuerzan el compromiso con la seguridad, creando modelos a seguir dentro de la empresa.

6. **Evaluación, Análisis y Mejora Continua**

Realizar auditorías y análisis de accidentes permite detectar áreas de mejora y adaptar políticas y protocolos a las nuevas realidades del entorno laboral. La cultura de seguridad debe ser dinámica, ajustándose para prevenir incidentes y adaptarse a los cambios tecnológicos y normativos.

Beneficios Clave

Una cultura de seguridad sólida reduce accidentes y lesiones, mejora la moral y productividad, asegura el cumplimiento legal y contribuye a un mejor ambiente laboral. Esto resulta en trabajadores más comprometidos y organizaciones más resilientes y exitosas.

Uso de Tecnología

El empleo de software de gestión de seguridad, aplicaciones móviles y plataformas e-learning puede facilitar la formación, el monitoreo y la comunicación, potenciando el desarrollo de una cultura de seguridad moderna y eficiente.

Estas estrategias constituyen un marco integral para transformar la manera en que una organización protege a sus empleados y asegura su bienestar, creando un entorno laboral seguro, saludable y productivo para todos.

BENEFICIOS DE UNA CULTURA DE SEGURIDAD

Una cultura de seguridad efectiva protege a los empleados, reduce accidentes y costos, mejora el ambiente laboral y fortalece la productividad y reputación empresarial.

La cultura de seguridad representa un conjunto de valores, prácticas y comportamientos compartidos que priorizan la protección de las personas, los activos y el entorno organizacional.

En contextos institucionales, empresariales y académicos, consolidar esta cultura no solo responde a exigencias normativas, sino que constituye una estrategia clave para la sostenibilidad, la productividad y el bienestar colectivo.

1. **Protección y bienestar de los empleados**

El beneficio primordial de fomentar una cultura de seguridad sólida es asegurar la salud y el bienestar físico y emocional de los trabajadores. Esta cultura promueve una mentalidad proactiva para prevenir accidentes y mitigar riesgos, generando confianza y compromiso mutuo entre la empresa y su equipo humano

.

2. **Reducción de accidentes y costos asociados**

La implementación continua de medidas preventivas y campañas de concientización reduce la incidencia de accidentes laborales, lo que disminuye considerablemente los gastos en indemnizaciones, atención médica, y pérdidas de productividad Esto implica un impacto financiero favorable para la organización.

3. **Mejora del clima laboral y la satisfacción**

Un entorno seguro propicia espacios de trabajo saludables y satisfactorios donde los empleados se sienten valorados, motivados y seguros, lo que disminuye la rotación de personal y reduce el ausentismo. Esta mejora en el bienestar emocional fortalece la productividad.

4. **Cumplimiento normativo y prevención de sanciones**

Una cultura de seguridad eficaz facilita el cumplimiento de normativas y regulaciones vigentes, evitando multas y sanciones legales. Además, convierte la seguridad en un valor fundamental e inherente a la empresa, más allá del mero cumplimiento obligatorio
.

5. **Incremento de la productividad y la eficiencia**

Al minimizar preocupaciones por riesgos físicos, los empleados pueden concentrarse en su trabajo, propiciando un aumento de la eficiencia y un mejor desempeño organizacional
.

6. **Fortalecimiento de la reputación empresarial**

Las empresas que priorizan la seguridad ganan mayor confianza en clientes, socios y comunidad, lo que se traduce en ventajas competitivas y en la atracción y retención de talento calificado

7. **Estímulo a la innovación y participación activa**

Promover la involucración de los empleados en la identificación y solución de riesgos fomenta la creatividad y el desarrollo de nuevas prácticas que fortalecen la cultura y la seguridad organizacional

Contar con una cultura de seguridad efectiva es una inversión estratégica que mejora la sostenibilidad, productividad y clima laboral de cualquier organización, garantizando un entorno seguro y saludable para todos sus integrantes.

8. **Protección de la Información Personal y Empresarial**

En la era digital, gran parte de nuestras actividades diarias y profesionales dependen de datos almacenados en dispositivos y en la nube. La ciberseguridad garantiza que esta información sensible no sea robada, manipulada o destruida, evitando fraudes, suplantación de identidad y pérdidas económicas.

La protección de la información personal y empresarial es vital en el contexto actual de crecimiento exponencial de los ciberataques, que se han vuelto cada vez más sofisticados y

frecuentes. La seguridad de datos no solo responde a una obligación legal y ética, sino que constituye un pilar estratégico para mantener la confianza de clientes, evitar pérdidas financieras y asegurar la continuidad operativa de las organizaciones.

9. **Prevención de Ataques Cibernéticos y Daños Financieros**

Los ataques de ransomware, phishing, malware y otros tipos de ciberataques están en aumento y pueden paralizar operaciones enteras de empresas o servicios gubernamentales. Contar con mecanismos robustos de seguridad digital ayuda a mitigar estos riesgos y asegurar la continuidad de actividades críticas.

10. **Protección de Infraestructuras Críticas y Nacionales**

En el contexto actual, la ciberseguridad también es vital para proteger infraestructuras estratégicas como sectores energéticos, telecomunicaciones y sistemas de salud, que son objetivos atractivos para actores maliciosos y pueden tener un impacto directo en la seguridad nacional.

11. **Fomentar la Confianza Digital**

La confianza en plataformas digitales es clave para la economía digital y la adopción tecnológica. Garantizar la seguridad en procesos online fomenta la participación segura de usuarios y empresas, impulsando el desarrollo tecnológico y económico.

12. **Adaptación a un Entorno en Constante Evolución**

Las amenazas cibernéticas evolucionan continuamente, por lo que mantener actualizadas las medidas de ciberseguridad es esencial para enfrentar nuevos retos como el Internet de las cosas (IoT), la inteligencia artificial y la expansión del teletrabajo.

L**a ciberseguridad es indispensable para salvaguardar datos, mantener la operatividad de servicios esenciales y proteger la confianza en un mundo digital cada vez más interconectado**, siendo un componente clave para el desarrollo sostenible y seguro de la sociedad actual.

13. **Amenazas comunes**

Las amenazas en ciberseguridad incluyen:

- ✓ **Malware** (software malicioso como virus, troyanos o ransomware) que puede dañar o bloquear sistemas.
- ✓ **Phishing**, que busca engañar usuarios para obtener datos personales o credenciales.

- ✓ **Ataques de denegación de servicio (DDoS)**, que saturan servidores para dejarlos inaccesibles.
- ✓ **Exploits y vulnerabilidades** que aprovechan fallos en software o hardware.

Buenas prácticas

Para protegerse se recomienda:

- ✓ Mantener sistemas y software actualizados para corregir vulnerabilidades.
- ✓ Utilizar contraseñas fuertes y autenticación multifactor para el acceso.
- ✓ Realizar copias de seguridad periódicas de datos importantes.
- ✓ Capacitar a usuarios para reconocer intentos de phishing y otras técnicas de ingeniería social.
- ✓ Implementar firewalls, antivirus y sistemas de detección de intrusos.

La ciberseguridad es un campo dinámico que evoluciona rápidamente, demandando vigilancia constante y adaptación a nuevas amenazas para proteger efectivamente los activos digitales.

CÓMO PROTEGER INFRAESTRUCTURAS CRÍTICAS

La protección de infraestructuras críticas en el contexto de la ciberseguridad requiere un enfoque integral, que incluya la implementación de marcos de gobernanza, tecnologías avanzadas y capacitación continua.

Importancia de la Ciberseguridad

Las infraestructuras críticas, que incluyen servicios esenciales como electricidad, agua y telecomunicaciones, son fundamentales para el funcionamiento diario de las sociedades modernas. La seguridad en estos entornos es crucial para evitar interrupciones que podrían tener consecuencias catastróficas, incluyendo daños económicos y riesgos para la vida humana. Con el aumento de las amenazas cibernéticas, como ransomware y ataques dirigidos, proteger estas infraestructuras se ha vuelto una prioridad global

Estrategias para la Protección

1. **Modelo de Cero Confianza (Zero Trust)**: Este enfoque se basa en la premisa de que ningún usuario o dispositivo debe ser confiado automáticamente. Se requiere verificar cada petición de acceso y aplicar políticas de mínimo privilegio y segmentación de redes para limitar el alcance de posibles ataques
2. **Segmentación de Redes**: Dividir las redes de Tecnología de la Información (TI) y Tecnología Operativa (OT) ayuda a limitar el movimiento lateral de los atacantes en caso

de un compromiso. La microsegmentación puede aplicar controles de acceso estrictos para proteger recursos críticos

3. **Inteligencia Artificial y Análisis de Comportamiento**: Implementar tecnologías avanzadas que utilizan machine learning para detectar patrones anómalos puede ayudar a identificar amenazas en tiempo real y actuar antes de que se materialicen en un ataque
4. **Capacitación Continua**: Los empleados deben recibir formación regular sobre ciberseguridad, incluyendo la identificación de fraudes y protocolos de respuesta a incidentes. La educación es clave para fortalecer la cultura de seguridad dentro de una organización.
5. **Evaluación y Gestión de Riesgos**: Realizar auditorías periódicas y evaluaciones de riesgos es esencial para identificar vulnerabilidades y priorizar la implementación de medidas de seguridad
6. **Colaboración y Normativas**. La colaboración entre gobiernos, empresas y otros actores clave es fundamental para establecer un marco regulatorio coherente que facilite la protección de infraestructuras críticas. Normativas como NIST y estándares internacionales proporcionan guías sobre cómo implementar medidas de seguridad robustas

La ciberseguridad en infraestructuras críticas implica desafíos complejos, pero con un enfoque estructurado y multidimensional que incluya tecnologías avanzadas, capacitación, y colaboración pública-privada, es posible mitigar los riesgos y asegurar la continuidad operativa. Adoptar estas estrategias no solo garantiza la seguridad de los servicios esenciales, sino que también refuerza la resiliencia de la infraestructura frente a futuros desafíos cibernéticos. Proteger las infraestructuras críticas es una responsabilidad compartida que requiere atención y acción inmediatas.

ESTRATEGIAS AVANZADAS DE CIBERSEGURIDAD

Compendio de **estrategias avanzadas**, identificadas a partir de la síntesis de múltiples fuentes especializadas para proteger infraestructuras críticas en el contexto de la ciberseguridad, considerando aspectos tecnológicos, organizativos y normativos.

Las estrategias avanzadas de ciberseguridad son esenciales para proteger la información crítica y los sistemas frente a amenazas complejas, aprovechando múltiples capas de defensa, inteligencia artificial y una respuesta rápida y coordinada.

La ciberseguridad avanzada, se refiere a la aplicación de técnicas, tecnologías y metodologías innovadoras para proteger sistemas informáticos y datos sensibles ante ataques cada vez más sofisticados. No solo abarca defensas tradicionales, sino también la integración de inteligencia artificial, aprendizaje automático, automatización, y un enfoque integral que incluye tanto la tecnología como la gestión humana y de procesos

1. **Adopción de Marcos y Normativas Internacionales**

- ✓ **ISO/IEC 27001**: Sistema de gestión de seguridad de la información que asegura confidencialidad, integridad y disponibilidad.
- ✓ **NIST Cybersecurity Framework (incluyendo SP 800-53 y SP 800-82r3 para entornos OT)**: Guía para la gestión de riesgos, con controles específicos para sistemas industriales.
- ✓ **IEC 62443**: Normativa para la seguridad en sistemas de control industrial (ICS).

2. **Modelo de Seguridad Zero Trust (Confianza Cero)**

- ✓ No asumir ninguna identidad o dispositivo como seguro por defecto.
- ✓ Implanta autenticación multifactor (MFA) y certificados digitales para cada acceso.
- ✓ Aplica el principio de mínimo privilegio.
- ✓ Microsegmentación granular en redes para limitar accesos.
- ✓ Monitoreo y auditoría continua de accesos y comportamientos.

3. **Segmentación y Microsegmentación de Redes**

- ✓ Separar claramente redes TI, OT, e IoT para restringir el movimiento lateral.
- ✓ Definir zonas de seguridad (por ejemplo: DMZ, zonas OT, IoT).
- ✓ Uso de firewalls definidos por software para controlar y aislar accesos sin afectar la operación.
- ✓ Especial atención a las interfaces de programación de aplicaciones (APIs) que son vectores críticos de ataque.

4. **Gestión Integral de Riesgos y Evaluación Continua**

- ✓ Evaluación profunda y holística que considere amenazas externas e internas y el impacto en la operatividad.
- ✓ Análisis cualitativo y cuantitativo para priorizar recursos.
- ✓ Implementación de sistemas de monitoreo en tiempo real y participación en redes de intercambio de inteligencia (ISACs).
- ✓ Revisión y actualización constante de planes y políticas de seguridad.

5. **Implementación de Tecnologías Avanzadas**

- ✓ Sistemas de Detección y Prevención de Intrusiones (IDPS) con análisis de comportamiento.
- ✓ Seguridad en punto final fortalecida especialmente para dispositivos móviles y remotos.

- ✓ Aplicación de inteligencia artificial (IA) y machine learning para detección proactiva y rápida de anomalías.
- ✓ Modelos explicables (XAI) para facilitar la confianza y comprensión en decisiones automatizadas.
- ✓ Honeypots industriales para atraer, estudiar y mitigar ataques dirigido.

6. Fortalecimiento de la Seguridad en Entornos OT & ICS

- ✓ Inventario y gestión precisa de activos conectados.
- ✓ Actualizaciones y parches planificados offline para evitar interrupciones.
- ✓ Controles de acceso específicos para protocolos industriales.
- ✓ Monitorización de la integridad de configuraciones y firmware.

7. Capacitación Continua y Cultura de Seguridad

- ✓ Programas permanentes para entrenar sobre phishing, ingeniería social y respuesta a incidentes.
- ✓ Simulacros regulares de tipo tabletop y red team vs blue team para mejorar tiempos y calidad de respuesta.
- ✓ Concienciar a todos los niveles organizativos sobre su papel en la seguridad.

8. Planificación de Respuesta, Mitigación y Recuperación

- ✓ Protocolos claros y actualizados para respuesta rápida ante incidentes.
- ✓ Backups offline (air-gapped) para protección ante ransomware y pérdida masiva de datos.
- ✓ Planes de continuidad del negocio (BCP) y recuperación ante desastres comprobados periódicamente.
- ✓ Monitoreo y SOC (Centro de Operaciones de Seguridad) 24/7, interno o contratado.

9. Gestión y Seguridad de la Cadena de Suministro

- ✓ Evaluación rigurosa de proveedores y componentes de hardware/software.
- ✓ Certificados de integridad y pruebas de vulnerabilidades antes del despliegue.
- ✓ Cláusulas contractuales para notificación temprana de fallos de seguridad.

10. Colaboración Intersectorial e Internacional

- ✓ Participación activa en comunidades sectoriales y gubernamentales para compartir indicadores de compromiso (IoC) y mejores prácticas.
- ✓ Coordinación público-privada para fortalecer la resiliencia conjunta.

- ✓ Adaptación a regulaciones internacionales y nacionales, como NIS2 y GDPR.

PROTECCIÓN AVANZADA DE INFRAESTRUCTURAS CRÍTICAS

La protección avanzada de infraestructuras críticas demanda un **enfoque multidimensional**, que combine un sólido marco normativo, tecnologías punteras, una gestión dinámica de riesgos y una fuerte cultura organizacional. La aplicación insistente del modelo Zero Trust, la modernización de redes mediante segmentación, el uso de IA explicable, y la colaboración estrecha entre sectores y gobiernos son pilares imprescindibles.

Solo mediante un plan de defensa coordinado, innovador y adaptativo, las infraestructuras críticas podrán anticipar, detectar y neutralizar amenaces cada vez más sofisticadas, garantizando la continuidad y seguridad de los servicios esenciales para la sociedad.

En el año 2025, la ciberseguridad ha dejado de ser una función técnica aislada para convertirse en un componente estratégico transversal en organizaciones públicas, privadas y académicas. La creciente sofisticación de los ataques —como el ransomware, el phishing y las campañas de ingeniería social— ha obligado a adoptar un enfoque de **gestión integral de amenazas**, que combine prevención, detección, respuesta y recuperación en tiempo real.

Uno de los cambios más significativos ha sido el reconocimiento del **factor humano** como eslabón crítico en la cadena de seguridad. La formación continua, la concienciación y la cultura organizacional se han consolidado como pilares para mitigar riesgos internos y externos.

Paralelamente, la **inteligencia artificial** ha irrumpido como herramienta clave para la defensa proactiva. Desde la automatización de respuestas hasta la detección de anomalías y la simulación de ataques, la IA permite anticipar amenazas antes de que se materialicen, aunque también plantea nuevos desafíos éticos y regulatorios.

1. **Elevado impacto del factor humano**

El elemento humano sigue siendo la mayor vulnerabilidad: aproximadamente el 74 % de las violaciones de datos involucran errores humanos, robo de credenciales o ingeniería social. Por ello, la concienciación y capacitación continua en ciberseguridad es una prioridad para minimizar estos riesgos y fortalecer la primera línea de defensa dentro de las organizaciones

2. **Gestión avanzada y ecosistemas resilientes**

Se destaca la gestión de la exposición a amenazas de forma continua, buscando mejorar la detección y respuesta rápida. Además, la "inmunidad del tejido de identidades" promueve sistemas que reducen fallos y errores a nivel de identidad digital, asegurando protección antes y durante un ataque. Estas prácticas marcan un cambio hacia ecosistemas de seguridad integrados y adaptativos

3. **Incremento de ataques sofisticados**

   - **Ransomware** sigue siendo una amenaza crítica: más del 66 % de las organizaciones sufrieron ataques en 2023, con rescates promedio cada vez más elevados y modalidades de doble extorsión que afectan infraestructuras críticas

   - **Ataques DDoS** crecieron en frecuencia y escala, dañando grandes proveedores tecnológicos con métodos cada vez más complejos

   - El phishing, principalmente en redes sociales como Instagram, Facebook y Twitter, continúa siendo la vía más usada para acceder a sistemas y provocar brechas de seguridad

4. **Tecnologías emergentes en la defensa**

La aplicación de **inteligencia artificial y aprendizaje automático** se consolida para la detección proactiva y análisis de amenazas basadas en grandes volúmenes de datos, mejorando la capacidad de anticipación y respuesta en tiempo real. También crece la seguridad basada en la nube y la protección mejorada para el Internet de las cosas (IoT), estableciendo métodos robustos de autenticación y cifrado

5. **Cambios estratégicos y normativos**

El modelo Zero Trust gana terreno como enfoque integral, tratando cualquier dispositivo o conexión como una potencial amenaza. Asimismo, la ampliación de competencias en los consejos de administración obliga a un mayor conocimiento y supervisión de la ciberseguridad por parte de máximos responsables empresariales. Las normativas internacionales, como ISO/IEC 27001, continúan siendo clave para mantener la seguridad y cumplir con regulaciones cada vez más estrictas.

Retos y oportunidades

- ✓ La escasez de talento cualificado en ciberseguridad sigue siendo un desafío global.
- ✓ La profesionalización del negocio delictivo, que ahora incluso ofrece malware como servicio, exige colaboración entre organizaciones y expertos para anticipar y neutralizar amenazas.
- ✓ Se espera un crecimiento en mecanismos de autenticación alternativos, incluyendo biometría y autenticación basada en riesgos para mejorar la seguridad de acceso

En resumen, 2025 ha sido un año en que la transformación digital ha intensificado las necesidades de defensa integrada, combinando tecnología, procesos y personas para un enfoque equilibrado y adaptativo frente a amenazas cada vez más sofisticadas y dinámicas.

La capacitación continua, la inversión en tecnologías avanzadas y la gestión estratégica de riesgos son los pilares esenciales para proteger datos y activos digitales en este contexto global.

SEGURIDAD INFORMÁTICA

Es la especialidad que se centra en proteger dispositivos físicos, software y redes para garantizar la integridad, confidencialidad y disponibilidad de la información y sistemas informáticos. Incluye protección contra accesos no autorizados, sabotajes, robo o daños a los recursos tecnológicos. Algunos principios clave son la autenticación, confidencialidad, integridad, disponibilidad, control de acceso, y copias de seguridad.

La seguridad informática incluye métodos y herramientas para proteger sistemas, datos y redes; la ciberseguridad es un subconjunto enfocado en prevenir amenazas digitales; y el manejo de datos informáticos se refiere al control y protección de la información almacenada o transmitida en sistemas digitales mediante diversas técnicas de seguridad.

1. Definición de Seguridad

(Alvarez A, 2005). El principio que hace una seguridad efectiva radica esencialmente en programas que detallan de forma minuciosa la observación y dentro de un contexto severo, en un tiempo y un espacio previo. Es el protagonismo de los hombres que con una clara orientación y definición organiza, planifica, opera y dirige las actividades que independiente señalan formas, los casos que hacen posibles una realidad.

2. Definición de Informática

(De Pablos C, 2004): La informática es entendida por otros especialistas como una ciencia encargada del estudio y desarrollo de máquinas para tratar y transmitir información, así como, de los métodos para procesarla. Aunque también podríamos decir de ella que es un conjunto de conocimientos, tanto teóricos como prácticos, sobre cómo se constituyen, como funcionan y como se utilizan los ordenadores electrónicos.

3. Seguridad Informática.

(Baca G, 2016) La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físico como lógicos, a los que está expuesta.

Esta definición se puede complementar señalando que en caso de que una amenaza a la seguridad se haga efectiva, debe procurar recupera la información dañada o robada.

4. **Ejemplos de seguridad informática:**

- ✓ Uso de firewalls (cortafuegos) para controlar el tráfico de red.
- ✓ Software antivirus que detecta y bloquea malware.
- ✓ Copias de seguridad periódicas para restaurar datos en caso de pérdida.
- ✓ Autenticación de dos factores para acceso seguro a sistemas.
- ✓ Filtros antispam que evitan correos maliciosos o phishing

5. **Objetivo de la Seguridad Informática.**

(Gómez A, 2011)

Entre los principales objetivos de la seguridad informática podríamos destacar los siguientes:

- ✓ Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas de seguridad.
- ✓ Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- ✓ Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- ✓ Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

6. **Importancia de la Seguridad Informática.**

(Garcia A, Hurtado C, Alegre M, 2011)

Preservar la información y la integridad de un sistema informático es algo muy importante para una empresa u organización, por lo que en pérdidas económicas y de tiempo podría suponer, sin olvidarnos del peligro que podría acarrear el acceso al sistema de un usuario no autorizado. Dentro de la seguridad informática podemos encontrar elementos y técnicas tanto hardware, como software, así como dispositivos físicos y medios humanos.

- ✓ Saber los motivos de la seguridad informática y valorar la importancia de mantener un sistema seguro.
- ✓ Conocer y saber diferenciar los tipos de seguridad existentes.
- ✓ Saber cuáles son los objetivos de seguridad.
- ✓ Conocer y distinguir los tipos de amenazas.
- ✓ Conocer la necesidad de proteger físicamente los sistemas informáticos y controlar sus condiciones ambientales.
- ✓ Conocer las leyes y normas relativas a la seguridad informática.

7. Vulnerabilidades.

(Areitio J, 2008)

> Una vulnerabilidad, por sí misma, no causa daño alguno; es, simplemente, una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo.

Las vulnerabilidades pueden ser permanentes, a no ser que se produzcan cambios en el activo, de forma que lo haga insensible a la vulnerabilidad. Las vulnerabilidades provocan debilidades en el sistema que pueden explotarse y dar lugar a consecuencias no deseadas.

8. Amenazas

(Gómez A, 2011)

> Se considera una amenaza a cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

Se puede establecer la siguiente clasificación a la hora de estudiar las amenazas a la seguridad:

- ✓ Amenazas naturales
- ✓ Amenazas de Agentes Externos.
- ✓ Amenazas de Agentes Internos.

(Corrales, 2005)

> Existen cuatro categorías generales de agresión a la seguridad de un sistema informático:

a) **Interrupción:** Un recurso del sistema se destruye o no llega a estar disponible o se inutiliza. Esta es una agresión de disponibilidad. Ejemplos: destrucción de un disco duro, ruptura de una línea de comunicación.

b) **Intercepción:** Un sujeto no autorizado consigue acceder a un recurso. Esta es una agresión a la confidencialidad. El ente no autorizado puede ser una persona, un programa o un ordenador. Ejemplos: intervención de las líneas, copia ilícita de ficheros o programas.

c) **Modificación:** Un sujeto no autorizado no sólo gana acceso, sino que deteriora el recurso. Esta es una agresión a la integridad. Ejemplo: cambios de valores en un fichero de datos, alteración de un programa para que funcione

de una forma diferente.

d) **Fabricación:** Una parte no autorizada inserta objetos falsos en el sistema. Esta es una agresión a la autenticidad.

9. Riesgos

(Aguilera P, 2010)

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- ✓ Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría de la reparación del daño.
- ✓ Aplicar medidas para disminuirlo o anularlo.
- ✓ Transferirlo.

(Areitio J, 2008)

En su libro argumenta que "Los factores de riesgo que atenta contra la seguridad de la información son los ambientes físicos, tecnológicos y humanos", como a continuación se detallan:

- ✓ Ambientales/Físicos:
- ✓ Tecnológicos
- ✓ Humanos.

SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

Los servicios de seguridad de la información son un conjunto de soluciones técnicas, organizativas y normativas diseñadas para proteger los activos informativos de una organización frente a amenazas internas y externas. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de los datos, conforme a marcos como ISO/IEC 27001, NIST, y normativas locales como la LOPDP en Ecuador.

(Gómez A, 2011)

Dentro del proceso de gestión de la seguridad informática es necesario contemplar una serie de servicios o funciones de seguridad de la información:

1. **Confidencialidad.**

Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático sólo podrá ser leído por su legítimo destinatario. Por lo tanto, este servicio pretende garantizar la confidencialidad de los daos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos transmitidos a través de redes de comunicaciones.

2. **Autenticación.**

La autenticación garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje.

3. **Integridad**

La función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática. De este modo, es posible detectar si se ha añadido o eliminado algún dato en un mensaje o fichero almacenado, procesado o transmitido por un sistema o red informática.

4. **No Repudiación.**

El objetivo de este servicio de seguridad consiste en implementar un mecanismo probatorio que permita demostrar la autoría y envío de un determinado mensaje, de tal modo que el usuario que lo ha creado y enviado a través del sistema no pueda posteriormente negar esta circunstancia, situación que también se aplica al destinatario del envió.

5. **Disponibilidad.**

La disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanente a disposición de los usuarios que deseen acceder a sus servicios.

CONSECUENCIAS DE LA FALTA DE SEGURIDAD

(Gómez A, 2011)

> En la actualidad el negocio y el desarrollo de las actividades de muchas organizaciones dependen de los datos e información registrada en sus sistemas informáticos, así como

el soporte adecuado de las TIC para facilitar su almacenamiento, procesamiento, análisis y distribución. La eliminación de todas las transacciones de un día en una empresa podría ocasionarle más pérdidas económicas que sufrir un robo o un acto de sabotaje contra alguna de sus instalaciones, y por ello es necesario trasladar a los directivos la importancia de valorar y protegeré la información de sus empresas.

1. **Seguridad de la Información**

(Del Peso E, 2003)

> Una definición de Seguridad de la información podría ser decir que es el conjunto de sistemas y procedimientos que garantizan: la confidencialidad, la integridad y la disponibilidad de la información. Quizás echemos de menos en ella la falta de autenticación, en no repudio tanto en origen como en destino y el sellado de tiempo.

En un principio se podría considerar que con que garantizasen tan sólo la confidencialidad, la integridad y la disponibilidad era bastante, pero con el uso masivo de redes, especialmente de internet, esto ya no es suficiente.

2. **Seguridad Activa y Pasiva.**

(García A, Hurtado C, Alegre M, 2011)

> La seguridad se divide en seguridad activa y pasiva, dependiendo de los elementos utilizaos para la misma, así como de la actuación que van a tener en la seguridad los mismos.

3. **Activa.**

Se entiende por seguridad activa todas aquellas medidas que se utilizan para detectar las amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema.

Una contraseña, cuanto más compleja sea, más segura y más difícil será descubrirla o desencriptarla, es decir, mayor fortaleza tendrá. Su longitud (8 caracteres como mínimo) y el uso conjunto de letras mayúsculas, minúsculas, números y caracteres especiales hacen que la seguridad de la contraseña sea mayor. No es conveniente para la seguridad de la contraseña el uso del mismo nombre de usuario, del nombre o del apellido real.

4. **Pasiva.**

Comprende todo el conjunto de medidas utilizadas para que una vez que se produzca el ataque o el fallo en la seguridad de nuestro sistema, hacer que el impacto sea el menor posible, y activar

mecanismos de recuperación del mismo.

5. **Seguridad Física y Lógica.**

(García A, Hurtado C, Alegre M, 2011)

> Desde el punto de vista de la naturaleza de la amenaza, podemos hablar de seguridad a nivel físico o material o seguridad a nivel lógico o software.

6. **Física.**

Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático.

Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales (López P, 2010) La seguridad física hace referencia a todos aquellos mecanismos que generalmente son de prevención y detección, los mismos que están destinados a proteger físicamente cualquier recurso del sistema

7. **Problema de Seguridad Física**

La Protección del hardware frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.
Problemas a los que nos enfrentamos:

- ✓ Acceso físico
- ✓ Desastres naturales
- ✓ Alteraciones del entorno

8. **Lógica.**

La seguridad lógica se encarga de asegurar la parte de software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y los datos.

La seguridad lógica se encarga de controlar que el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuario autorizados, ya sea desde dentro del sistema informático, como desde fuera, es decir, desde una red externa, usando una VPN.

Dentro de la seguridad lógica, tenemos una serie de programas, o software, como el sistema operativo, que se debe encargar de controlar el acceso de los procesos o usuarios a los recursos del sistema.

POLÍTICAS DE SEGURIDAD

(Aguilera P, 2010)

> Recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección.

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrad directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de la seguridad planificadas. Por tanto, la política de seguridad deberá redactarse de forma que pueda ser comprendida por todo el personal de una organización.

No todas las políticas de seguridad son iguales. El contenido depende de la realidad y de las necesidades de la organización para la que se elabore.

Existen algunos estándares de políticas de seguridad por países y por áreas (gobiernos, medicina, militar…), pero los más internacionales son los definidos por ISO (International Organization for Standardization).

1. Objetivos de las Políticas de Seguridad.

(Aguilera P, 2010)

Una política de seguridad contendrá los objetivos de la empresa en materia de seguridad del sistema de información, generalmente englobados en cuatro grupos:

- ✓ Identificar las necesidades de seguridad y los riesgos que amenazan al sistema de información, así como evaluar los impactos ante un eventual ataque.
- ✓ Relacionar todas las medidas de seguridad que deben implementarse para afrontar los riesgos de cada activo o grupo de activos.
- ✓ Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.
- ✓ Detectar todas las vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.
- ✓ Definir un plan de contingencias.

PLAN DE RESPUESTA A INCIDENTES

Un Plan de Respuesta a Incidentes en Ciberseguridad y Manejo de Datos es una estrategia formal que permite a una organización detectar, contener, erradicar y recuperarse de incidentes que comprometan la seguridad de sus sistemas o datos. Aquí te presento una estructura técnica y práctica basada en marcos internacionales como NIST, ISO/IEC 27035 y experiencias latinoamericanas:

1. **Componentes Clave del Plan**

Preparación

- ✓ Definición de roles y responsabilidades (CSIRT, líderes técnicos, comunicaciones).
- ✓ Inventario de activos críticos y evaluación de riesgos.
- ✓ Capacitación continua y simulacros.

Detección y Análisis

- ✓ Monitoreo de sistemas (SIEM, IDS/IPS).
- ✓ Identificación de indicadores de compromiso (IoCs).
- ✓ Clasificación del incidente (malware, fuga de datos, acceso no autorizado).

Contención

- ✓ Aislamiento de sistemas afectados.
- ✓ Activación de protocolos de emergencia.
- ✓ Preservación de evidencia para análisis forense.

Erradicación

- ✓ Eliminación de la amenaza (malware, cuentas comprometidas).
- ✓ Aplicación de parches y mejoras de seguridad.
- ✓ Validación de limpieza.

Recuperación

- ✓ Restauración de sistemas y servicios.
- ✓ Validación de integridad de datos.
- ✓ Comunicación interna y externa (clientes, autoridades).

Lecciones Aprendidas

- ✓ Revisión del incidente y del desempeño del equipo.
- ✓ Actualización del plan y políticas.
- ✓ Informe técnico y legal.

Manejo de Datos Sensibles

- ✓ Clasificación de datos (públicos, privados, sensibles).
- ✓ Aplicación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.
- ✓ Notificación a la autoridad competente (Superintendencia de Protección de Datos).
- ✓ Registro de incidentes y trazabilidad.

2. Marcos y Normativas Relevantes

Marco/ Norma	Descripción
NIST SP 800-61	Guía para la gestión de incidentes de seguridad informática.
ISO/IEC 27035	Estándar internacional para respuesta a incidentes.
LOPDP (Ecuador)	Regula el tratamiento y protección de datos personales.
COBIT / ITIL	Buenas prácticas en gestión de TI y servicios.

(Terán D, 2014)

El plan de respuesta de incidentes puede ser dividido en cuatro fases:

- ✓ Acción inmediata para detener o minimizar el incidente.
- ✓ Investigación de incidente.
- ✓ Restauración de los recursos afectados.
- ✓ Reporte de incidentes a los canales apropiados.

Una respuesta a incidente deber ser decisiva y ejecutarse rápidamente. Debido a que hay muy poco espacio para errores, es crítico que se efectúen prácticas de emergencias y se midan los tiempos de respuesta. De esta forma, es posible desarrollar una metodología que fomenta la velocidad y la precisión, minimizando el impacto de la indisponibilidad de los recursos y el daño potencial causado por el sistema en peligro.

3. Detección y respuesta ante incidentes de seguridad.

(Chicano E, 2014)

La detención y respuesta ante incidentes de seguridad, permite a las organizaciones la automatización de números procesos de respuestas ante incidentes y la reducción considerable de los daños ocasionados, a la vez que se facilita la recuperación de los sistemas afectados.

El equipo de respuesta ante incidentes de seguridad, además del a confección del Plan de Gestión de Incidentes, deberá encargarse de establecer:

- ✓ Una política general de gestión de incidentes en la que se deberá basar el plan de gestión.
- ✓ Los procedimientos a seguir para la gestión de incidentes basados en la política e incluidos en el plan.
- ✓ Relaciones entre el equipo de respuesta a incidentes y otros grupos de la organización internos y externos.
- ✓ Las guías en las que se defina el procedimiento a seguir en la comunicación de las organizaciones con terceros en caso de ocurrencia de incidentes.
- ✓ Organización de los responsables de la gestión de respuesta a incidentes y definiciones y asignaciones de funciones.

CAPITULO II
MANEJO DE DATOS INFORMATICOS

MANEJO DE DATOS INFORMATICOS

El manejo adecuado de los datos informáticos es una piedra angular en la ciberseguridad, pues garantizar su protección, integridad y confidencialidad es esencial para evitar amenazas y vulnerabilidades en el entorno digital**.**

En la era digital actual, los datos se han convertido en uno de los activos más valiosos para individuos y organizaciones. El manejo de datos informáticos dentro del ámbito de la ciberseguridad no solo implica su almacenamiento o transferencia, sino también la aplicación de estrategias y controles que aseguren su confidencialidad, integridad y disponibilidad. La forma en que se recolectan, procesan y protegen los datos determina en gran medida la resistencia de los sistemas ante ataques cibernéticos, pérdidas de información o accesos no autorizados.

Este capítulo explorará los principios fundamentales del manejo de datos en ciberseguridad, resaltando la importancia de adoptar buenas prácticas como la encriptación, la gestión de accesos, la auditoría constante y el cumplimiento de normativas legales. Además, se abordarán los escenarios más comunes en los que la mala gestión de datos puede poner en riesgo la seguridad informática, como las fugas de información, el robo de identidad o la manipulación maliciosa de datos.

Comprender el manejo de los datos informáticos desde una perspectiva de ciberseguridad es clave para desarrollar políticas sólidas, implementar tecnologías efectivas y crear conciencia en los usuarios, con el fin de proteger tanto la infraestructura digital como la privacidad de las personas. Este conocimiento se vuelve indispensable en un mundo donde las amenazas evolutivas demandan una respuesta proactiva, integral y adaptada a las nuevas realidades tecnológicas.

1. Manejo de Datos en Ciberseguridad

El manejo de datos informáticos dentro de la ciberseguridad consiste en proteger, administrar y controlar la información digital para garantizar su **confidencialidad, integridad, disponibilidad y autenticidad**. Estos principios son la base para resguardar los activos digitales frente a amenazas, accesos no autorizados, pérdida o alteración maliciosa.

2. Principios Fundamentales de la Seguridad de Datos en Ciberseguridad

- ✓ **Confidencialidad:** Asegurar que la información solo sea accesible para personas autorizadas mediante controles de acceso y técnicas como el cifrado.

- ✓ **Integridad:** Garantizar que los datos se mantengan completos, sin modificaciones indebidas, con mecanismos de verificación de cambios y auditorías.
- ✓ **Disponibilidad:** Asegurar que los datos estén accesibles y recuperables cuando los usuarios legítimos lo requieran, minimizando interrupciones por ataques o fallos.
- ✓ **Autenticidad:** Verificar la identidad del origen o propietario de la información para evitar suplantaciones o fraudes.

3. Componentes Clave en el Manejo de Datos para Ciberseguridad

- ✓ **Clasificación de datos:** Categorizar la información según su sensibilidad y criticidad (pública, interna, confidencial, secreta) para aplicar controles adecuados.
- ✓ **Control de acceso y gestión de identidades:** Definir quién, cuándo y cómo puede acceder o modificar los datos mediante autenticación robusta (contraseñas complejas, autenticación multifactor).
- ✓ **Cifrado de datos:** Aplicar técnicas criptográficas para proteger datos en reposo y en tránsito, dificultando su lectura o robo por usuarios no autorizados.
- ✓ **Monitoreo y análisis de datos:** Utilizar herramientas avanzadas (SIEM, análisis de comportamiento, inteligencia artificial) para detectar actividad sospechosa, anomalías o brechas de seguridad.
- ✓ **Gestión de incidentes:** Definir procedimientos para detectar, responder y recuperarse de eventos que comprometan la seguridad de los datos (ataques, fugas, corrupción).
- ✓ **Gestión de vulnerabilidades:** Identificación y mitigación continua de debilidades en infraestructuras de TI que puedan ser explotadas para acceder o dañar datos.

4. Prácticas Recomendadas en el Manejo de Datos para Ciberseguridad

- ✓ Mantener el software y sistemas siempre actualizados con los últimos parches de seguridad.
- ✓ Implementar segmentación y separación de redes para limitar el acceso según roles y departamentos.
- ✓ Realizar copias de seguridad periódicas y verificar su integridad para asegurar la recuperación ante incidentes.
- ✓ Capacitar y sensibilizar al personal en torno a la protección de datos, riesgos y amenazas comunes (phishing, malware, ingeniería social).
- ✓ Utilizar soluciones avanzadas de análisis para prever ataques y responder tempranamente.
- ✓ Cumplir con normativas legales y estándares internacionales relevantes (ISO 27001, NIST, GDPR, LOPDP, entre otros).

IMPORTANCIA DE MANEJO DE DATOS INFORMATICOS

El manejo adecuado de datos informáticos es fundamental para proteger la integridad, confidencialidad y disponibilidad de la información en organizaciones que priorizan una cultura de seguridad consciente y preventiva.

El manejo eficiente de datos informáticos implica procesos estructurados para la recolección, almacenamiento, protección, acceso y eliminación segura de datos. En un entorno guiado por una cultura de seguridad, esta gestión se realiza bajo principios y normativas que buscan minimizar riesgos como pérdidas, filtraciones o alteraciones de información.

La cultura de seguridad es el conjunto de valores, prácticas y comportamientos compartidos dentro de una organización que promueve la conciencia sobre la importancia de la protección de la información y la responsabilidad de cada individuo en mantenerla segura. Esta cultura impulsa políticas claras, formación continua y una vigilancia constante frente a amenazas internas y externas.

1. **Ventajas clave del manejo de datos en este contexto incluyen**:

   - ✓ **Protección contra ciberataques y fraudes**: Evitar accesos no autorizados y ataques que puedan comprometer datos sensibles.
   - ✓ **Cumplimiento normativo**: Garantizar que el tratamiento de datos cumpla con leyes y estándares nacionales e internacionales.
   - ✓ **Mejora en la toma de decisiones**: Datos confiables y seguros permiten análisis precisos y estratégicos para el negocio.
   - ✓ **Confianza y reputación**: Resguardar la información personal y empresarial fortalece la credibilidad ante clientes y socios.
   - ✓ **Reducción de impactos frente a incidentes**: Protocolos de manejo de datos bien implementados facilitan respuestas rápidas y efectivas ante fallas o brechas de seguridad.
   - ✓ Finalmente, el manejo de datos y la cultura de seguridad son indivisibles: sin un ambiente que valore la seguridad, incluso las mejores tecnologías y prácticas técnicas pueden ser insuficientes. Fomentar un compromiso generalizado y continuo con la protección de datos es la base para cualquier estrategia efectiva de seguridad informática.

ESTRATEGIAS PARA PROTEGER DATOS INFORMÁTICOS

A continuación, se presentan estrategias clave para proteger datos informáticos integradas en un entorno donde la cultura de seguridad es el pilar fundamental, con foco en prácticas, tecnología y formación continua:

1. **Fomento de una Cultura de Seguridad Integral**

   - ✓ **Concienciación continua:** Educar a todos los niveles de la organización para que entiendan la importancia de la seguridad de la información, fomentando un compromiso compartido.
   - ✓ **Políticas claras y comunicación abierta:** Establecer normas y protocolos accesibles y bien comunicados que promuevan comportamientos responsables y conscientes en el manejo de datos.
   - ✓ **Responsabilidad colectiva:** Incentivar que cada persona asuma su rol en la protección de datos, creando un ambiente donde la seguridad es valorada y practicada diariamente.

2. **Gestión Robusta de Contraseñas y Autenticación**

   - ✓ Uso obligatorio de **contraseñas fuertes y únicas** que combinen mayúsculas, minúsculas, números y símbolos.
   - ✓ Implementación de **autenticación multifactor (MFA)** para añadir capas adicionales de seguridad al acceso a sistemas y aplicaciones sensibles.
   - ✓ Políticas para el cambio periódico y la no reutilización de contraseñas.

3. **Actualización y Mantenimiento Constante**

   - ✓ Establecer protocolos de actualización automática y regular para sistemas operativos, aplicaciones y software de seguridad para cerrar vulnerabilidades conocidas.
   - ✓ Aplicar parches de seguridad apenas estén disponibles y realizar auditorías periódicas para identificar posibles brechas.

4. **Uso de Tecnologías de Protección Avanzadas**

   - ✓ **Firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS)** para monitorear y bloquear accesos no autorizados.
   - ✓ Software **antivirus y antimalware actualizado** en todos los dispositivos conectados a la red.
   - ✓ **Cifrado de datos** en tránsito y en reposo, usando estándares robustos como AES-256 y protocolos TLS/SSL.
   - ✓ Implementación de redes privadas virtuales (**VPN**) para proteger conexiones, especialmente en redes públicas o no confiables.

5. **Control de Accesos y Principio de Mínimos Privilegios**

- ✓ Definir roles y permisos de acceso basados en responsabilidades reales mediante sistemas como RBAC (control de acceso basado en roles).
- ✓ Aplicar el principio de **mínimo privilegio** para minimizar el riesgo de accesos indebidos o malintencionados.
- ✓ Monitorear y auditar accesos para detectar actividades anómalas o sospechosas.

6. Respaldo y Recuperación de Datos

- ✓ Realizar copias de seguridad periódicas, almacenadas en ubicaciones seguras y, preferentemente, fuera de línea o en la nube con altos estándares de seguridad.
- ✓ Tener un plan de recuperación ante incidentes que permita restaurar datos y sistemas con la mínima interrupción operativa.

7. Monitoreo, Auditoría y Respuesta a Incidentes

- ✓ Implementar sistemas de monitoreo continuo que detecten patrones inusuales y alerten en tiempo real.
- ✓ Realizar auditorías y simulacros regulares para evaluar la efectividad de las medidas de protección.
- ✓ Contar con planes de respuesta bien definidos para contener, mitigar y resolver incidentes de seguridad de manera rápida y coordinada.

9. Protección Contra Ingeniería Social y Phishing

- ✓ Capacitar a usuarios para reconocer correos y comunicaciones sospechosas.
- ✓ Promover la verificación de remitentes, evitar enlaces no confiables y no compartir información sensible sin comprobar la legitimidad.
- ✓ Simulaciones de phishing periódicas para aumentar la resistencia organizacional.

10. Políticas y Normativas de Seguridad

- ✓ Adoptar estándares internacionales (como ISO/IEC 27001) y cumplir con regulaciones locales e internacionales (RGPD, CCPA).
- ✓ Revisar y actualizar las políticas de seguridad periódicamente para adaptarse a nuevas amenazas y tecnologías.

11. Formación y Capacitación Continua

- ✓ Programas regulares de entrenamiento en ciberseguridad para empleados y usuarios finales.

- ✓ Fomentar una cultura en la que la seguridad sea una práctica diaria, no solo una obligación puntual.
- ✓ Promover el reporte proactivo de incidentes o vulnerabilidades.

La protección efectiva de datos en un entorno guiado por una cultura de seguridad requiere integrar **tecnologías avanzadas**, **procesos rigurosos**, y, fundamentalmente, **educación y compromiso humano**. Solo a través de una visión holística que combine estos elementos es posible minimizar riesgos, responder efectivamente a las amenazas y mantener la integridad, confidencialidad y disponibilidad de la información.

GESTIÓN RESPONSABLE Y ÉTICA DE LOS DATOS

Además de la seguridad técnica, el manejo de datos informáticos en ciberseguridad implica respetar la privacidad y uso responsable de la información, fomentando la transparencia y confianza tanto dentro de organizaciones como con usuarios externos.

El manejo de datos informáticos en ciberseguridad es un proceso integral que involucra la aplicación de principios, controles técnicos, procedimientos organizativos y formación para proteger la información digital contra riesgos y ataques. El objetivo último es preservar la **confidencialidad, integridad, disponibilidad y autenticidad** de los datos, favoreciendo un entorno digital seguro y confiable

La encriptación de datos es fundamental para proteger la información digital, garantizar la confidencialidad y prevenir accesos no autorizados en entornos informáticos y de ciberseguridad.

1. Protección de la Confidencialidad y Privacidad

La encriptación convierte los datos en un formato ilegible para cualquier persona que no tenga la clave correcta, asegurando que información sensible como datos personales, financieros o corporativos permanezca protegida durante su almacenamiento o transmisión. Esto es vital para cumplir con normativas legales sobre privacidad y evitar filtraciones que puedan causar daños económicos o reputacionales.

2. Salvaguarda contra Ataques Cibernéticos

En un mundo donde el robo de datos, el phishing y el acceso malicioso son comunes, la encriptación funciona como una capa de defensa que dificulta el uso indebido de la información robada. Aunque un atacante logre obtener datos cifrados, sin la clave adecuada, esos datos no serán útiles, reduciendo el impacto de brechas de seguridad.

3. Integridad y Autenticidad

Además de proteger la confidencialidad, la encriptación se incorpora en protocolos que garantizan que los datos no han sido alterados y provienen de fuentes confiables, aportando integridad y autenticidad a la información procesada o transmitida.

4. Facilita la Confianza y Cumplimiento Normativo

Empresas y usuarios confían en sistemas que aseguran la protección de sus datos, lo que es crucial para mantener relaciones comerciales y reputación. La encriptación es requerida por diversos estándares internacionales y regulaciones de seguridad para la protección de datos, como el GDPR en Europa o la Ley de Protección de Datos Personales en Ecuador.

La encriptación es una herramienta esencial e irremplazable en la gestión segura de datos informáticos, clave para mantener la privacidad, evitar fraudes digitales y proteger la infraestructura informática frente a amenazas actuales y futuras.

5. Consecuencias de fallar en la encriptación

- ✓ **Exposición de datos sensibles**

La falla en la encriptación puede llevar a que datos confidenciales (como información personal, financiera, médica o corporativa) queden expuestos a atacantes, aumentando la probabilidad de fugas o robos de información crítica

- ✓ **Pérdida de integridad y autenticidad de datos**

Sin un cifrado adecuado, es posible que los datos sean modificados, corrompidos o falsificados durante su transmisión o almacenamiento, lo que degrada la fiabilidad y confianza en los sistemas

- ✓ **Impacto económico significativo**

Los incidentes derivados de fallos criptográficos pueden causar pérdidas financieras cuantiosas, incluyendo costos por recuperación, multas regulatorias (hasta un 4% del volumen global de negocios, según GDPR), demandas legales y pago de rescates en casos de ransomware.

- ✓ **Daño reputacional y pérdida de confianza**

La exposición pública de vulnerabilidades en la seguridad provoca pérdida de credibilidad ante clientes, proveedores y socios, afectando la continuidad del negocio y la captación de nuevos clientes

- ✓ .**Vulnerabilidad ante ataques específicos:**

  - **Ataques Man-in-the-Middle (MitM):** Interceptación y alteración de datos no cifrados
  - **Ataques por fuerza bruta o robo de claves:** Si las llaves criptográficas son débiles, reutilizadas o mal gestionadas, se facilita la desencriptación ilícita
  - **Uso de algoritmos débiles u obsoletos:** Provoca que el cifrado sea vulnerable a ataques conocidos, comprometiendo la seguridad

- ✓ **Interrupción operativa y riesgos regulatorios**

La encriptación pueden causar bloqueo o secuestro de datos (ransomware), lo que implica interrupción de actividades y sanciones legales por incumplimiento de normativas de protección de datos encriptación impacta gravemente en la seguridad y continuidad organizacional, facilitando la exposición, manipulación y robo de datos sensibles, generando severos daños económicos, legales y reputacionales. La gestión segura de claves, actualización de algoritmos y protocolos robustos son esenciales para mitigar estos riesgos.

EL MODELO ZERO TRUST

El modelo Zero Trust es un enfoque de seguridad que parte del principio "nunca confiar, siempre verificar", eliminando la confianza implícita y validando rigurosamente cada acceso dentro de una red, sin importar su origen.

1. Concepto básico

En lugar de asumir que los usuarios o dispositivos dentro de una red son confiables por defecto, el modelo Zero Trust exige una verificación continua y estricta de identidad y autorización para cada solicitud de acceso. Esto significa que, incluso si un usuario o dispositivo ya está dentro de la red corporativa, debe seguir siendo autenticado y autorizado antes de acceder a cualquier recurso o dato.

2. Características clave

- ✓ Validación continua: Cada acceso es evaluado en función del contexto, como identidad del usuario, dispositivo, ubicación y estado de seguridad.
- ✓ Principio de mínimo privilegio: Los usuarios solo obtienen los permisos necesarios para realizar sus tareas, limitando el acceso excesivo.
- ✓ Microsegmentación: La red se divide en zonas pequeñas para contener posibles brechas y limitar movimientos laterales de atacantes.

- ✓ Monitoreo y análisis constantes: Se recopilan datos sobre accesos y actividades para detectar comportamientos anómalos y amenazas en tiempo real.
- ✓ Ventajas del modelo Zero Trust
- ✓ Reduce el riesgo de ataques internos y externos al minimizar la confianza implícita.
- ✓ Mejora la protección frente a amenazas avanzadas y ransomware.
- ✓ Facilita la seguridad en entornos modernos, como cloud computing y trabajo remoto.
- ✓ Aumenta el control y visibilidad sobre quién accede a qué recursos y cuándo.
- ✓ En resumen, Zero Trust representa una evolución en la ciberseguridad que reconoce que las amenazas pueden venir de cualquier lugar, y por ello, la confianza nunca es automática sino siempre ganada y renovada para proteger mejor los sistemas y datos críticos.

CÓMO IMPLEMENTAR ZERO TRUST EN EMPRESAS

La implementación del modelo de seguridad **Zero Trust** (Confianza Cero) es un proceso estratégico y gradual que transforma la manera en que una organización protege sus activos digitales. A continuación, se describen los pasos principales y consideraciones fundamentales basados en referencias recientes y las mejores prácticas del sector.

1. Principios Básicos de Zero Trust

- ✓ **Nunca confiar, siempre verificar:** No se confía automáticamente en ningún usuario, dispositivo o aplicación, incluso si están dentro del perímetro corporativo.
- ✓ **Acceso mínimo necesario (principio de menor privilegio):** Cada usuario o sistema recibe solo los permisos estrictamente necesarios.
- ✓ **Monitoreo y validación continua:** Todos los accesos y actividades son constantemente supervisados y validados.

2. Pasos para implementar Zero Trust en tu empresa

1. Realizar un inventario completo de activos y usuarios

- ✓ Identificar y clasificar los **activos críticos** (datos, aplicaciones, dispositivos, servicios).
- ✓ Conocer los flujos de datos y procesos de negocio.
- ✓ Levantar un listado detallado de usuarios, dispositivos y aplicaciones que acceden a esos activos.

2. Evaluar riesgos y procesos

- ✓ Analizar los riesgos asociados a cada proceso o recurso.

- ✓ Clasificar según nivel de sensibilidad y vulnerabilidad.
- ✓ Iniciar la implementación en procesos o sistemas de bajo riesgo para facilitar la transición.

3. Definir políticas claras de acceso y control

- ✓ Crear políticas que consideren identidad del usuario, estado del dispositivo, ubicación, hora, entre otros factores.
- ✓ Establecer controles basados en el principio de **mínimos privilegios**.
- ✓ Incorporar reglas dinámicas ajustables según el contexto.

4. Implementar autenticación multifactor (MFA)

- ✓ Exigir múltiples factores de autenticación para todos los accesos a sistemas críticos.
- ✓ MFA puede incluir contraseñas, tokens, biometría o códigos temporales.
- ✓ Es un pilar central para reducir accesos no autorizados.

5. Aplicar microsegmentación de red y control de acceso granular

- ✓ Dividir la red en segmentos seguros que limitan el movimiento lateral de posibles atacantes.
- ✓ Controlar que usuarios y dispositivos accedan solo a los recursos necesarios.
- ✓ Utilizar tecnologías como firewalls de nueva generación y soluciones SASE (Secure Access Service Edge).

6. Monitoreo, detección y respuesta continua

- ✓ Implementar herramientas de monitorización en tiempo real para detectar comportamientos anómalos.
- ✓ Desarrollar una estrategia de respuesta rápida para mitigar amenazas o accesos indebidos.
- ✓ Utilizar SIEM (Security Information and Event Management) y análisis con inteligencia artificial para optimizar la detección.

7. Automatización de la seguridad y ajustes constantes

- ✓ Automatizar respuestas frente a incidentes para minimizar daños sin necesidad de intervención humana inmediata.
- ✓ Actualizar políticas regularmente en función de patrones de uso y amenazas emergentes.

- ✓ Capacitar y concientizar a los colaboradores sobre su rol en la seguridad Zero Trust.

Ciclo de vida y pilares fundamentales de seguridad Zero Trust (por ManageEngine)

- ✓ **Visibilidad:** Conocer qué está pasando en la red y quién accede a qué.
- ✓ **Deducción:** Identificar amenazas, cambios o incidentes.
- ✓ **Respuesta:** Actuar para mitigar riesgos detectados.
- ✓ **Resolución:** Fortalecer la infraestructura de seguridad para evitar futuras brechas.

Los cinco pilares que se deben cuidar son:

- ✓ Identidades
- ✓ Dispositivos
- ✓ Datos
- ✓ Aplicaciones
- ✓ Seguridad de la red

Consideraciones para una implementación exitosa

- ✓ **No es un cambio inmediato:** Es un proceso gradual, que debe adaptarse a las capacidades y estructura de la organización.
- ✓ **Cultura organizacional:** Es fundamental que todos comprendan y apoyen el modelo.
- ✓ **Adaptabilidad:** Los sistemas y políticas deben ser flexibles para responder a cambios tecnológicos y emergentes amenazas.
- ✓ **Integración tecnológica:** Usar soluciones que se complementen (IAM, MFA, microsegmentación, SASE, análisis avanzado).

Resumen práctico para comenzar

- ✓ Haz un inventario de tus activos y usuarios críticos.
- ✓ Evalúa riesgos y define políticas Zero Trust claras.
- ✓ Implementa MFA y segmenta tu red.
- ✓ Monitorea y responde de forma continua.
- ✓ Revisa y ajusta constantemente tu estrategia.
- ✓ Con este enfoque, tu empresa puede aumentar sustancialmente la seguridad, proteger los datos y minimizar el impacto de posibles brechas.

La clave está en adoptar un enfoque progresivo, basado en la evaluación constante y la validación rigurosa, donde ninguna entidad se asuma fiable sin previa comprobación.

CAPITULO III
PLAN DE CONTIGENCIA

PLAN DE CONTIGENCIA

En un entorno digital cada vez más interconectado y vulnerable, la implementación de un Plan de Contingencia en Ciberseguridad y Manejo de Datos Informáticos constituye una herramienta estratégica esencial para garantizar la continuidad operativa, la protección de la información y la resiliencia institucional frente a incidentes tecnológicos. Este tipo de plan permite anticipar, mitigar y responder eficazmente ante amenazas como ataques cibernéticos, fallos técnicos, desastres naturales o errores humanos que puedan comprometer la integridad, disponibilidad y confidencialidad de los sistemas y datos.

La creciente dependencia de infraestructuras digitales en sectores críticos —como salud, justicia, educación y administración pública— exige una planificación rigurosa que articule medidas preventivas, protocolos de respuesta y mecanismos de recuperación. Además, el manejo de datos informáticos debe alinearse con marcos normativos como la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador, el Reglamento General de Protección de Datos (RGPD) en Europa y estándares internacionales como ISO/IEC 27001 y NIST SP 800-34, que establecen buenas prácticas en seguridad de la información y gestión de incidentes.

1. Objetivos del Plan de Contingencia

- ✓ Prevenir y mitigar riesgos tecnológicos que afecten la seguridad digital.
- ✓ Establecer protocolos claros de actuación ante incidentes informáticos.
- ✓ Garantizar la recuperación rápida de sistemas y datos críticos.
- ✓ Cumplir con normativas legales sobre protección de datos personales.
- ✓ Fortalecer la cultura organizacional en torno a la seguridad digital.

Este plan no solo responde a la necesidad técnica de proteger activos digitales, sino que también se inscribe en una lógica de gobernanza responsable, derechos digitales y soberanía tecnológica. Si deseas, puedo ayudarte a desarrollar el cuerpo completo del documento, adaptarlo a una institución específica o vincularlo con políticas públicas de transformación digital.

2. Plan de contingencia

(Aguilera P, 2010)

> Determinadas amenazas a cualquiera de los activos del sistema de información pueden poner en peligro la continuidad de un negocio. El plan de contingencias es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de

información de los peligros que lo amenazan o recuperándolo tras un impacto.

3. **El plan de contingencias consta de tres sub planes independientes:**

   - ✓ **Plan de Respaldo**.- Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daña. Por ejemplo, restaurar de inmediato las copias de seguridad o activar el sistema automático de extinción de incendios.

   - ✓ **Plan de Emergencia**.- Contempla qué medidas tomar cuando se está materializando una amenaza o cuando acaba de producirse. Por ejemplo, restaurar de inmediato las copias de seguridad o activar el sistema automático de extinción de incendios.

   - ✓ **Plan de Recuperación.-** Indica las medidas que se aplicarán cuando se ha producido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento del sistema y de la organización. Por ejemplo, tener un lugar alternativo donde continuar la actividad si el habitual hubiese sido destruido, sustituir el material deteriorado, reinstalar aplicaciones y restaurar copias de seguridad.

4. **Objetivos Generales de un Plan de Contingencia.**

(Martínez J, 2004)

> Conseguir que el desarrollo e implantación de un Plan de Contingencia sea un proyecto estratégico de toda la organización, involucrando a todos los departamentos y divisiones para que la información necesaria fluya de forma continua en la medida de las necesidades de los responsables de llevarlo adelante.

Su desarrollo, implementación y mantenimiento propiciará a la organización los beneficios siguientes, en caso de posibles interrupciones:

- ✓ Minimizar las potencias pérdidas económicas.
- ✓ Reducir riesgos potenciales.
- ✓ Reducir las probabilidades de que ocurran interrupciones.
- ✓ Reducir interrupciones en las operaciones.
- ✓ Asegurar la estabilidad de la organización
- ✓ Facilitar una recuperación ordenada.
- ✓ Minimizar las primas de seguros
- ✓ Reducir la dependencia de ciertos elementos clave.
- ✓ Proteger los activos de la organización.
- ✓ Ampliar la seguridad del personal y de los clientes.

- ✓ Minimizar la necesidad de toma de decisiones durante un incidente.
- ✓ Minimizar las responsabilidades legales.

En primer lugar, es necesario que la organización establezca la necesidad de disponer de una gestión de la continuidad de las operaciones mediante la elaboración y gestión de un Plan de Continuidad de Negocio, incluyendo el apoyo de la Dirección y organizando y gestionando el proyecto de forma que se cumpla con los plazos y coste previamente establecidos.

5. Plan de Contingencia Informática.

(Aguilera P, 2010)

> "El Plan de Contingencia informática es un proceso de manejo integrado que identifica el impacto de potenciales amenazas que tiene la institución el mismo provee un marco de procesos y procedimientos para construir una respuesta con las capacidades necesarias para que sea efectiva, salvaguardando los intereses institucionales, conforme a la naturaleza, escala y complejidad de las actividades de la institución."

El mayor reto del departamento de sistemas puede ser la reanudación de las actividades y no poder regresar a su lugar habitual de trabajo y realizar sus actividades normalmente.

6. Objetivos del Plan De Contingencia Informática

- ✓ Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- ✓ Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.
- ✓ Establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas.
- ✓ Establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups.

7. Eventos considerados para el plan de contingencia

- ✓ Frecuencia de la amenaza. Cuántas veces se espera que ocurra un determinado suceso, normalmente referido a un periodo de un año.
- ✓ Impacto de la amenaza. La medida del daño o coste resultante como consecuencia de la ocurrencia del suceso. Normalmente expresado en porcentaje del valor del activo dañado.
- ✓ Eficacia de las medidas de seguridad adoptadas.
- ✓ Incertidumbre. Característica típica de riesgo, basada en el grado de confianza en

las cantidades aplicadas a los elementos anteriores.

8. Plan de Recuperación de Desastres.

(Marchionni E, Formoso O, 2012)

> DRP viene de las siglas Disaster Recovery Plan o, lo que es lo mismo en castellano, Plan de Recuperación de Desastres. Consiste en un plan en el cual se aseguran el hardware, el software y los datos de una empresa para que esta pueda continuar con su operatoria diaria. En muchos casos, no se piensa en un probable pero no imposible imprevisto que nos puede generar grandes pérdidas económicas si no estamos a la altura de las circunstancias. Es por eso que siempre debemos estar provistos de un plan de contingencias, prever una estrategia de recuperación ante desastres de cualquier tipo.

(Marchionni E, Formoso O, 2012)

> Los sistemas de DRP a lo largo de la historia fueron elementos esenciales para mantener la operatividad de una empresa, Como su nombre lo indica, son utilizados para la recuperación de sistemas antes la ocurrencia de desastres imprevistos, corte de energía, catástrofes naturales y de cualquier tipo. Esta clase de sistemas nos asegura la continuidad del negocio más allá de los desastres posibles. En las grandes empresas es de extrema importancia establecer un plan conciso de recuperación para los sistemas críticos de la compañía. Generalmente, lo vemos implementado en sistemas de correo, de base de datos, de intranet y de negocios como SAP.

(Marchionni E, Formoso O, 2012)

> En caso de producirse algún desastre se tenía los datos replicados del otro lado, si la empresa era previsora. El modo opuesto de llegar a la misma solución era teniendo discos espejados en algunos servidores productivos, que luego se trasladaban al sitio de recuperación. La recuperación con la traslación de discos era factible si el sistema era chico, con pocos discos, ya que si se necesitaba mover un storage completo era muy posible que se corrompiera toda la información en el traslado, por alguna caída o choque en el camino.

En muchas ocasiones, también ocurría que, si los datos eran replicados, se debía reinstalar el sistema operativo y recuperar los datos desde dicha réplica, todas estas recuperaciones eran válidas hace tiempo. Si bien se generaban pérdidas ante la eventualidad en un fallo, se podía continuar con la operatoria del negocio a más tardar en 24 o 48 horas.

(Marchionni E, Formoso O, 2012)

> Hoy en día, estos tiempos de recuperación se acortaron mucho con los ambientes virtualizados. En pocos minutos podemos tener todo restaurado y operando como si nada hubiese ocurrido y para arreglar lo que esté fuera de línea en un tiempo futuro, en caso de catástrofe, y también evita dolores de cabeza en la administración.

La infraestructura virtual permite flexibilizar este tipo de planes de contingencia y pensar en varias soluciones posibles. Podemos hacer una copia de respaldo cada determinado tiempo sobre las máquinas virtuales productivas, para luego recuperarlas en otro sitio; también, replicarlas directamente a discos en storages interconectados o implementar el tipo de soluciones que ofrece VMware de manera automatizada sobre todo el proceso.

(Marchionni E, Formoso O, 2012)

> DRP no solo depende de una herramienta tecnológica sino de varios procesos y responsables, coordinación y gran cadena de aprobaciones. Cada servidor debe contar con su propio DRP lo que nos lleva a tener que coordinarlos a todos, en conjunto, en el plan de recuperación del datacenter. Por otro lado, cada servidor debe tener un plan en donde se establezca cuándo y cómo puede dejar de dar servicio y cuáles son los pasos para ponerlo nuevamente en línea, además de las posibles conexiones y direcciones en la red, así como contemplar las configuraciones de seguridad. Más adelante veremos cómo con SRM estas tareas son muchísimo más fáciles de implementar y mantener en el tiempo.

Antes de dar comienzo con los detalles de SRM, explicaremos dos conceptos clave en los sistemas de DRP. Se trata de dos indicadores de excelencia en este tipo de sistemas, uno es el RTO y el otro se llama RPO. El RTO (Recovery Time Objective) es el tiempo que pasará hasta que una infraestructura esté nuevamente disponible para utilizarse. Cuanto menor sea este número mayor será la performance del sistema de DRP. El RPO (Recovery Point Objective) es básicament la cantidad de datos que la organización está dispuesta a perder en caso de ejecución de un DRP. Si queremos reducir este número es necesario maximizar los esfuerzos en la réplica de datos para lograr una sincronización acorde. Cuanto menor sea este valor, el DPR tendrá un mejor rendimiento. SRM ayuda a que estos números bajen drásticamente en comparación con los antiguos sistemas, lo que se traduce como una enorme reducción de pérdidas de dinero.

(Baud, Jean Luc, 2017)

> Desarrolla las normas para reiniciar todas las actividades de proceso en el propio Centro de Proyecto de Datos o en un Centro de Respaldo. Para la recuperación en el propio centro incluye normas referentes a:

- ✓ Activación de equipos duplicados o auxiliares (si no es automática)
- ✓ Uso de soporte de procesamiento alternativos.
- ✓ La recuperación inmediata (o recuperación muy en caliente). Inmediata quiere decir que se trata de una recuperación que se puede llevar algunos minutos, incluso algunas horas. Esto es muy complicado de realizar y se reserva a contexto en los que el impacto de la parada de la actividad es muy fuerte para la empresa. Este tipo de recuperación se encuentra en los dominios como la banca o las empresas de telecomunicaciones.
- ✓ La recuperación inmediata (o recuperación en caliente). Intermedia significa una recuperación de las actividades que se puede extender entre 24 y 72 horas.
- ✓ La recuperación gradual (o recuperación suave). Gradual quiere decir que se trata de una recuperación progresiva de los diferentes servicios informáticos. Eventualmente puede llevar más de tres días, pasando por un modo degradado de las diferentes actividades.

9. Plan de Emergencias

(Corrales, J, 2005)

Guía que recogen las normas de actuación durante o inmediatamente después de cada fallo o daño. Para cada incidente; leve o grave, se determinan:

Acciones inmediatas:

- ✓ **Seguridad Física:** para equipos, dar aviso y/o activar o desactivar alarmas, emplear extintores, llamar a mantenimiento.
- ✓ **Seguridad Lógica:** para el ordenador central, periféricos o comunicaciones, llamar al jefe de sala, llamar lanzar salvaguardas.

Acciones posteriores:

- ✓ **Seguridad Física:** Acciones de salvamento, valoración de daños, elaboración de informes.
- ✓ **Seguridad Lógica:** relanzar procesos, relanzar el sistema operativo, valor los daños causados, usar copias de seguridad en soporte alternativos, saltar procesos.
- ✓ **Asignación de Responsabilidades:** Se asignarán responsabilidades tanto para acciones primarias como para la coordinación de tareas.

Backups

(Corrales, J, 2005)

El éxito de una compañía depende entre otros factores de la disponibilidad continúa de sus sistemas de información. Se deben afrontar inversiones apropiadas para tratar con los inevitables fallos de sistemas, tanto hardware como software, desastres naturales o cualquier otro. Una de las medidas más importantes es la planificación de copias de seguridad, salvaguardias o Backups y procedimientos de recuperación apropiados,

De acuerdo con el IEEE (Institute of Electrical and Electronics Engineers, pronunciando IE cubo)**,** los fallos se clasifican en tipos, que pueden ser agrupados en las siguientes categorías:

- ✓ **Físicos:** Causados generalmente por fallos hardware, como fallos de medio o un fallo en la CPU.
- ✓ **De Diseño (errores software)**: Causados por fallos o errores de los programas.

De operación: Causados por la intervención humana. Algunos ejemplos de fallos de operación son los fallos atribuidos a la inexperiencia de los administradores de datos, errores de usuarios, configuraciones inadecuadas del sistema o procedimientos inapropiados de Backups.

SEGURIDAD INTEGRAL DE LA INFORMACIÓN

(Del Peso E, 2003) Una definición de Seguridad de la información podría ser decir que es el conjunto de sistemas y procedimientos que garantizan: la confidencialidad, la integridad y la disponibilidad de la información. Quizás echemos de menos en ella la falta de autenticación, en no repudio tanto en origen como en destino y el sellado de tiempo.

La función del procesamiento de datos es un servicio de toda la institución, que apoya no sólo a los sistemas de información administrativa sino también a las operaciones funcionales. La Seguridad un aspecto de mucha importancia en la correcta Administración Informática, lo es también de toda la Institución.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren.

En relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para evitar la pérdida o modificación de los datos, Información o software Inclusive, por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas, entre las cuales figurarán el asignar números de Identificación y contraseñas a los usuarios.

1. **Fases de la Metodología para el Desarrollo de un Plan de Contingencia de los Sistemas de Información.**

(MONCADA G, 2001)

> Debemos de tener presente que mucho dependerá de la infraestructura de la empresa y de los servicios que ésta ofrezca para determinar un modelo de desarrollo de plan, no existe un modelo único para todos, lo que se intenta es dar los puntos más importantes a tener en cuenta.

La metodología empleada para el desarrollo y aplicación del plan de contingencias de los sistemas de información, ha sido desarrollada por el INEI, en base a la experiencia lograda en el desarrollo de planes de contingencia para el problema del año 2000.

La presente metodología se podría resumir en ocho fases de la siguiente manera:

- ✓ Planificación: Preparación y aprobación de esfuerzos y costos.
- ✓ Identificación de riesgos: Funciones y flujos del proceso de la empresa.
- ✓ Identificación de soluciones: Evaluación de Riesgos de fallas o interrupciones.
- ✓ Estrategias: Otras opciones, soluciones alternativas, procedimientos manuales.
- ✓ Documentación del proceso: Creación de un manual del proceso.
- ✓ Realización de pruebas: Selección de casos soluciones que probablemente funcionen.
- ✓ Implementación: Creación de las soluciones requeridas, documentación de los casos.
- ✓ Monitoreo: Probar nuevas soluciones o validar los casos.

Fase 1: Planificación.

Diagnóstico

(MONCADA G, 2001)

> Cada vez que nos encontremos en una actividad que requiere el diseño de una propuesta de solución para un determinado problema, es necesario siempre la revisión exhaustiva de cada uno de los componentes que conforman nuestro sistema, es por esta razón siempre debemos de realizar una etapa de diagnóstico para poder asegurar que las acciones de solución propuestas tengan un fundamento realista y no tener que volver a rehacer toda propuesta.

Fase 2: Identificación de Riesgos.

(MONCADA G, 2001)

> Deberían identificarse los riesgos de los procesos del proyecto y de los sistemas de telecomunicaciones e informáticos (como producto), y los medios para determinar cuándo se superan los límites aceptables. Deberían utilizarse la experiencia y los datos de proyectos anteriores.

La identidad de riesgos debería realizarse al inicio del proyecto, en las evaluaciones de la marcha del proyecto y en otras ocasiones en las que se tomen decisiones significativas.

La identificación de riesgos debería considerar no solo los riesgos en términos de costes, tiempo y producto, sino también en aspectos tales como la seguridad, la seguridad de funcionamiento, la responsabilidad profesional, la tecnología de la información, la seguridad en el trabajo, salud y el medio ambiente, teniendo en cuenta los requisitos estatutarios o reglamentarios aplicables, actuales y previstos. Es necesario considerar las interacciones entre los distintos riesgos. También conveniente identificar las tecnologías nuevas y críticas.

Un riesgo identificado con un impacto significativo debería tener una persona asignada especialmente, con la responsabilidad, la autoridad y los recursos necesarios para gestionar el riesgo en cuestión.

Análisis y Evaluación de Riesgos

Es conveniente evaluar la probabilidad de que ocurran las situaciones de riesgos identificadas y su impacto, teniendo en cuenta la experiencia y los datos de proyecto anteriores; se deberían registra los criterios y las técnicas utilizados. Siempre es conveniente realizar un análisis cualitativo, al que debería seguir un análisis cuantitativo siempre que sea posible.

Fase 3: Identificación de Soluciones

(MONCADA G, 2001)

> Un proyecto de plan de contingencia no sirve si se queda en plan o papel. El cual debe contemplar todos los procesos institucionales sean estos manuales y/o automatizados, evaluando el volumen de información o materiales afectados, a fin de definir la complejidad de los sistemas.

La magnitud, de un plan de contingencia será proporcional a la complejidad, Importancia, costo del servicio al cual está destinado a proteger y el riesgo asociado a la misma.

El esquema general del plan de contingencias de los sistemas de información, está constituido por tres grandes fases:

1. Fasede Reducción de Riesgos

2. Fasede Recuperación de Contingencia
3. Fasede Organización de un Sistema de Alerta contra Fallas

Fase 4: Estrategias.

(MONCADA G, 2001)

> Las estrategias de contingencia o continuidad de los negocios están diseñadas para identificar prioridades y determinar en forma razonable las soluciones a ser seleccionadas en primera instancia o los riesgos a ser encarados en primer lugar. Hay que decidir si se adoptarán las soluciones a gran escala, como las opciones de recuperación de desastres para un centro de datos.

Fase 5: Documentación de Proceso.

(MONCADA G, 2001)

> Todo el proceso de lograr identificar soluciones ante determinados problemas no tendrá su efecto verdadero si es que no se realiza una difusión adecuada de todos los puntos importantes que este implica, y un plan de Contingencia con mucho mayor razón necesita de la elaboración de una documentación que sea eficientemente orientada.

Como puntos importantes que debe de incluir esta documentación podremos citar las siguientes:

- ✓ Cuadro de descripción de los equipos y las tareas para ubicar las soluciones a las contingencias.
- ✓ La documentación de los riesgos, opciones y soluciones por escrito y en detalle.
- ✓ La identificación y documentación de listas de contacto de emergencia, la identificación de responsables de las funciones con el fin de garantizar que siempre haya alguien a cargo, y que pueda ser contactada si falla un proceso de importancia.

Fase 6: Realización de Pruebas y Validación.

(MONCADA G, 2001)

> Los procedimientos de las pruebas y validación es para asegurar que los sistemas y servicios están funcionando correctamente, establecer parámetros de verificación. Identificar los equipos o personas responsables de cada procedimiento. Procedimientos detallados de pruebas de operación de bases de datos, redes y equipos.

Fase 7: Implementación.

(MONCADA G, 2001)

> La fase de implementación se da cuando han ocurrido o están por ocurrir los problemas para este caso se tiene que tener preparado los planes de contingencia para poder aplicarlos. Puede también tratarse esta etapa como una prueba controlada.

Fase 8: Monitoreo

(MONCADA G, 2001)

> La fase de Monitoreo nos dará la seguridad de que podamos reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da un cambio en la infraestructura, debemos de realizar un mantenimiento correctivo o de adaptación.

Un punto donde se tiene que actuar es por ejemplo cuando se ha identificado un nuevo riesgo o una nueva solución. En este caso, toda la evaluación del riesgo se cambia, y comienza un nuevo ciclo completo, a pesar de que este esfuerzo podría ser menos exigente que el primero.

Esto es importante ya que nos alimentamos de las nuevas posibilidades de soluciones ante nuevos casos que se puedan presentar. Podríamos enumerar las actividades principales a realizar:

- ✓ Desarrollo de un mapa de funciones y factores de riesgo.
- ✓ Establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos.
- ✓ Revisión continua de las aplicaciones.
- ✓ Revisión continua del sistema de backup.
- ✓ Revisión de los Sistemas de soporte eléctrico del Centro de Procesamiento de Datos.

ESTRATEGIAS EFECTIVAS DE CIBERSEGURIDAD

Implementar políticas claras, gestionar vulnerabilidades, utilizar arquitecturas de seguridad multicapa, capacitar al personal y preparar planes de respuesta a incidentes son esenciales para proteger los sistemas y datos frente a ciberamenazas modernas.

- ✓ **Establecer Políticas Sólidas de Ciberseguridad**

Definir políticas claras sobre el acceso a datos, uso de dispositivos, control de permisos y

protocolos de respuesta a incidentes es fundamental para asegurar la protección sistemática de la organización. Estas políticas deben revisarse y actualizarse regularmente, involucrando a todos los departamentos para garantizar cobertura integral y cumplimiento efectivo.

- ✓ **Gestión Proactiva de Vulnerabilidades y Actualizaciones**

Realizar evaluaciones y escaneos regulares para identificar vulnerabilidades en software, hardware y puntos finales permite priorizar y aplicar parches críticos a tiempo. Automatizar la gestión de actualizaciones de sistemas operativos, antivirus y aplicaciones reduce riesgos frente a exploits y ataques de malware

- ✓ **Arquitectura de Seguridad Multicapa**

Adoptar una defensa en profundidad, con múltiples capas que incluyen firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), segmentación de redes, cifrado de datos y control de acceso estricto (como autenticación multifactor) fortalece la resiliencia ante ataques externos e internos

- ✓ **Protección y Gestión de Datos**

Garantizar la confidencialidad, integridad y disponibilidad de la información mediante cifrado en tránsito y reposo, uso de VPNs seguras, copias de seguridad frecuentes y soluciones de gestión de dispositivos móviles (MDM) previene la filtración y pérdida de datos críticos.

- ✓ **Capacitación y Concienciación del Personal**

El factor humano es frecuentemente el eslabón más débil. Programas de formación regulares para enseñar a detectar phishing, manejar contraseñas seguras y buenas prácticas reducen exponencialmente el riesgo de incidentes causados por errores humanos.

- ✓ **Monitoreo Continuo y Detección Temprana**

Implementar tecnologías que permitan la vigilancia constante del tráfico de red y actividades sospechosas (Sistemas SIEM, análisis inteligente mediante IA) facilita la identificación rápida de intrusiones o anomalías para activar respuestas oportunas.

- ✓ **Plan de Respuesta a Incidentes y Recuperación**

Contar con un plan formal que establezca roles, procedimientos para contener, erradicar amenazas y recuperar sistemas es vital para minimizar impactos. Realizar simulacros y pruebas fortalece la preparación y reduce tiempos de reacción ante ataques reales.

- ✓ **Evaluación Permanente y Colaboración**

Realizar auditorías de seguridad constantes y análisis de riesgos ayuda a priorizar recursos. Además, fomentar alianzas con expertos en ciberseguridad y compartir inteligencia sobre amenazas mejora la capacidad de defensa colectiva frente a ciberataques sofisticados. Conjuntamente, estas estrategias forman un enfoque integral y actualizado para proteger activos digitales en entornos cada vez más expuestos y vulnerables. La ciberseguridad no es solo técnica, sino también un compromiso organizacional que debe permeabilizar a todos los niveles para lograr una defensa efectiva y sostenible.

MEJORES PRÁCTICAS PARA LA CAPACITACIÓN EN CIBERSEGURIDAD

La capacitación efectiva en ciberseguridad debe ser continua, práctica, actualizada y orientada a crear una cultura de responsabilidad compartida para proteger a la organización frente a amenazas digitales.

- ✓ **Capacitar desde el primer día y con actualización continua**

Es fundamental que la formación en ciberseguridad sea obligatoria desde la incorporación de nuevos empleados, incluyendo políticas claras sobre el manejo de datos y seguridad digital. La capacitación debe repetirse regularmente para crear hábitos arraigados y estar al día con las últimas amenazas y tecnologías, evitando que la información quede obsoleta o sea olvidada

- ✓ **Diseñar contenidos relevantes y atractivos**

Los programas deben cubrir temas clave como identificación y reporte de phishing, ingeniería social, buenas prácticas en contraseñas, seguridad en dispositivos móviles, uso seguro de la nube, y políticas de correo electrónico e Internet. Incorporar metodologías activas, como ejercicios interactivos, simulaciones (phishing simulado), vídeos y gamificación, aumenta el compromiso y la retención del conocimiento

- ✓ **Evaluar necesidades y medir eficacia**

Antes de implementar, se recomienda evaluar las brechas de conocimiento de los empleados para adaptar contenidos de manera precisa. La evaluación continua mediante pruebas, simulacros y métricas permite conocer la eficacia de la capacitación y realizar ajustes oportunos para mejorarla

- ✓ **Involucrar a toda la organización y socios externos**

No solo los empleados regulares necesitan formación, también supervisores, ejecutivos, proveedores y terceros deben participar, ya que cualquiera con acceso a sistemas puede

representar un riesgo. Se debe fomentar una cultura de seguridad compartida y responsable entre todos los niveles y áreas

- ✓ **Fomentar una cultura proactiva de ciberseguridad**

El objetivo es que los empleados no solo conozcan las políticas, sino que se sientan protagonistas en la defensa digital, desarrollando conciencia, responsabilidad y actitud preventiva. Reconocer sus logros y comunicar éxitos ayuda a consolidar esta cultura

- ✓ **Complementar con herramientas tecnológicas y políticas claras**

Hacer énfasis en el uso adecuado de contraseñas seguras, autenticación multifactor, actualizaciones constantes de software, y control riguroso de accesos y dispositivos. Integrar la capacitación con prácticas organizativas fortalecidas mejora sustancialmente la seguridad global.

- ✓ **Planificar y documentar un programa formal de capacitación**

Tener un plan estructurado y documentado, actualizado con las últimas amenazas, que defina roles, responsabilidades y métodos para impartir la formación, así como un canal de comunicación claro para alertas y reportes de incidencias

- ✓ **La capacitación continua y multidimensional**

La capacitación continua y multidimensional junto con una cultura de seguridad sólida es clave para minimizar errores humanos, principal causa de incidentes, y fortalecer las defensas organizacionales ante un entorno de amenazas cada vez más sofisticado.

ESTRATEGIAS PARA FOMENTAR LA CULTURA DE SEGURIDAD

Crear una cultura sólida de ciberseguridad requiere compromiso desde la alta dirección, educación continua, políticas claras y un enfoque centrado en las personas para integrar hábitos seguros en el día a día laboral.

- ✓ **Compromiso y liderazgo de la alta dirección**

Es fundamental que los líderes de la organización apoyen y promuevan la ciberseguridad como un valor estratégico. Esto implica asignar recursos, participar activamente en iniciativas de seguridad y comunicar la importancia de esta cultura a todos los niveles para fomentar un sentido de responsabilidad compartida y colaboración.

- ✓ **Formación y concienciación continua**

La educación constante es clave para que los empleados comprendan las amenazas actuales y desarrollen hábitos seguros. Esto incluye talleres, seminarios, simulacros de phishing y contenidos personalizados según roles o departamentos. La capacitación debe ser práctica, diversa y actualizada para mantener la atención y efectividad.

- ✓ **Políticas claras y accesibles**

Establecer políticas comprensibles y flexibles que definan las normas de seguridad, el manejo de información y la respuesta ante incidentes ayuda a mantener la disciplina y la claridad de responsabilidades. Además, deben revisarse regularmente para ajustarse a nuevas amenazas y tecnologías.

- ✓ **Integración de tecnologías y herramientas de soporte**

Implementar métodos tecnológicos como autenticación multifactor, gestión de accesos, monitoreo continuo y detección de amenazas ayuda a fortalecer la seguridad técnica. Sin embargo, estas herramientas deben complementarse con formación que mejore su uso efectivo por parte de los empleados

.

- ✓ **Fomento de la comunicación abierta y reporte sin represalias**

Crear canales seguros donde el personal pueda reportar incidentes o comportamientos sospechosos sin temor a sanciones promueve la vigilancia colectiva y mejora la detección temprana de riesgos. Además, recompensar las buenas prácticas a través de gamificación o incentivos impulsa un ambiente positivo y motivador.

- ✓ **Evaluación y mejora continua**

Una cultura de ciberseguridad no es estática, sino un proceso constante de evaluación mediante auditorías, simulacros y análisis de incidentes. Esto permite ajustar planes, medir el impacto de las formaciones y adaptar las estrategias a la evolución del panorama de amenazas.

Ejemplos prácticos y acciones recomendadas

- Realizar simulacros de phishing para medir la vulnerabilidad y reforzar la capacidad de respuesta.
- Impulsar programas de embajadores de seguridad en cada área.
- Organizar eventos temáticos como “Cybersecurity Day” para sensibilizar de forma atractiva.
- Personalizar las formaciones según el perfil y necesidades de los empleados.
- Integrar políticas de seguridad desde el diseño de proyectos y productos para que la

seguridad sea proactiva, no reactiva

Fomentar una cultura de ciberseguridad implica un enfoque integral que combine liderazgo, educación, normas claras, tecnología y comunicación continua orientada a que la seguridad sea un hábito natural para todos en la organización. Así, las empresas pueden mejorar significativamente su resiliencia frente a los crecientes riesgos cibernéticos.

ANÁLISIS DE RIESGOS

Se realiza un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada, y que deben ser protegidos, entre ellos se presentan los siguientes:

- ✓ Personal
- ✓ Hardware.
- ✓ Software y utilitarios d. Datos e información.
- ✓ Documentación.
- ✓ Suministros de energía eléctrica
- ✓ Suministros de telecomunicaciones

En cada uno de los riesgos mencionados, existen posibles daños como lo son:

- ✓ Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.
- ✓ Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- ✓ Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante robo o deslealtad a la institución.

A continuación, se da a conocer las posibles fuentes de daños, las cuales no permitirían el correcto funcionamiento de la institución:

- ✓ Acceso no autorizado
- ✓ Ruptura de las claves de acceso al sistema computacionales
- ✓ Desastres Naturales
- ✓ Fallas de Personal estratégico, por los siguientes inconvenientes: enfermedad, accidentes, renuncias, abandono de sus puestos de trabajo, entre otros.
- ✓ Fallas de Hardware: falla en los Servidores (Hw), falla en el hardware de Red (Switches, cableado de la Red, Router, FireWall).

CLASES DE RIESGO.

Es el factor de probabilidad por clase de riesgo en función a la ubicación geográfica de la institución y a su entorno institucional, por lo cual se debe considerar lo siguiente en la institución:

- ✓ Se ubica en zona sísmica el factor de probabilidad de desastre por terremotos será alta.
- ✓ Se ubica en una zona marginal con alto índice de delincuencia, las probabilidades de robo, asalto o vandalismo será de un riesgo considerablemente alto.
- ✓ Se ubica en zona industrial las probabilidades de fallas en los equipos será alto por la magnitud de variaciones en tensiones eléctricas que se generan en la zona.
- ✓ Cambia constantemente de personal, las probabilidades de equivocaciones y sabotaje será alto.

REDES DE COMUNICACIÓN DE DATOS

Las redes de comunicación de datos son sistemas que permiten la transmisión de información entre dispositivos interconectados, como computadoras, servidores, sensores, teléfonos móviles y otros equipos digitales. Estas redes constituyen la infraestructura esencial para el funcionamiento de internet, servicios en la nube, telecomunicaciones, sistemas empresariales y entornos domésticos inteligentes

En el Consejo Nacional Electoral existen varias redes internas cableada y una inalámbrica que brinda servicio de internet a los diferentes departamentos. La red local es cableada categoría 5e, la red Wireless posee puntos de acceso distribuidos en diferentes espacios de la empresa. La topología física de la red cableada es estrella, el proveedor del servicio de internet es CNT, el mismo que suministra el servicio mediante cable de fibra óptica, la red existente es de clase C.

1. Relaciones de coordinación

Las redes de coordinación en el manejo de datos son estructuras colaborativas que permiten a múltiples actores —instituciones, sistemas, dispositivos o personas— interactuar de manera horizontal para gestionar, compartir, proteger y utilizar información de forma eficiente, segura y legal. Estas redes son clave en entornos donde la interoperabilidad, la gobernanza de datos y la protección de derechos digitales son prioritarias.

Permitirá establecer relaciones con diversas entidades, tanto internas como externas a la institución, con el fin de contar con apoyo estratégico en caso de que se presente algún imprevisto que comprometa la seguridad de la información o se registre un evento de carácter catastrófico que afecte la infraestructura informática y deje fuera de servicio las operaciones

institucionales. Estas entidades podrán colaborar activamente en la gestión de la crisis, facilitando la recuperación oportuna de los servicios y la reanudación de las actividades operativas en el menor tiempo posible.

2. Relaciones de coordinación internas

Las **relaciones de coordinación internas** en el manejo de datos se refieren a los vínculos colaborativos que se establecen entre distintas áreas, unidades o equipos dentro de una misma organización para **gestionar, proteger y utilizar la información de manera eficiente, segura y conforme a la normativa vigente**. Estas relaciones son fundamentales para garantizar la calidad del dato, la interoperabilidad entre sistemas y la toma de decisiones basada en evidencia.

Características clave

- ✓ **Horizontalidad operativa**: Se da entre áreas que comparten responsabilidades en el ciclo de vida del dato (ej. TI, jurídico, estadística, planificación).
- ✓ **Interdependencia funcional**: Las acciones de una unidad (como la recolección de datos) impactan directamente en otras (como el análisis o la protección legal).
- ✓ **Comunicación estructurada**: Requiere canales formales para compartir metadatos, criterios de clasificación, políticas de acceso y protocolos de seguridad.
- ✓ **Autonomía coordinada**: Cada área conserva sus competencias, pero coopera bajo marcos comunes como políticas de gobernanza de datos.

Ejemplos prácticos

Area	Relación de coordinación interna
Unidad de TI	Coordina con jurídico para aplicar medidas de seguridad conforme a la LOPDP.
Estadistica institucional	Coordina con planificación para generar indicadores confiables.
Archivo y documentanción	Coordina con sistemas para digitalizar y preservar datos históricos.
Juridico	Coordina con todas las áreas para asegurar el cumplimiento normativo en el tratamiento de datos.

Importancia estratégica

- ✓ Evita duplicidad de esfuerzos y errores en el tratamiento de datos.
- ✓ Facilita el cumplimiento de normativas como la LOPDP y estándares ISO.
- ✓ Promueve la gobernanza de datos basada en principios de calidad, seguridad y transparencia.

- ✓ Fortalece la capacidad institucional para responder ante auditorías, incidentes o requerimientos ciudadanos.

3. Relaciones de coordinación externas

Las **relaciones de coordinación externas** en el manejo de datos se refieren a los vínculos colaborativos que una organización establece con **entidades ajenas** —públicas, privadas, académicas o comunitarias— para **intercambiar, proteger, procesar o reutilizar información** de manera segura, legal y eficiente. Estas relaciones son clave para garantizar la interoperabilidad, el cumplimiento normativo y la generación de valor público a partir de los datos.

Características principales

- ✓ **Horizontalidad institucional**: No existe subordinación entre las partes; se coopera desde la autonomía.
- ✓ **Interdependencia estratégica**: Las decisiones de una entidad pueden afectar la gestión de datos de otra.
- ✓ **Acuerdos formales**: Se sustentan en convenios, protocolos, memorandos de entendimiento o contratos.
- ✓ **Objetivos compartidos**: Se busca mejorar la calidad, seguridad y utilidad de los datos para fines comunes.

Ejemplos de coordinación externa

Sector	Ejemplo de relación externa en manejo de datos
Salud	Intercambio de historiales clínicos entre hospitales y el Ministerio de Salud bajo estándares HL7.
Educación	Coordinación entre universidades y el SENESCYT para validar títulos y registros académicos.
Justicia	Integración de datos entre Fiscalía, Policía Nacional y Registro Civil para investigaciones penales.
Gobierno abierto	Publicación de datos abiertos en portales interoperables con ONGs y ciudadanía.
Investigacion cientifica	Redes académicas que comparten bases de datos bajo licencias abiertas y estándares FAIR.

Marco normativo y técnico aplicable

- ✓ **LOPDP (Ecuador)**: Regula el tratamiento de datos personales y exige responsabilidad compartida entre responsables y encargados externos.

- ✓ **ISO/IEC 27001 & 27701**: Estándares para gestión de seguridad de la información y privacidad.
- ✓ **RGPD (si aplica)**: Establece obligaciones para transferencias internacionales de datos.
- ✓ **Principios FAIR**: Promueven que los datos sean *localizables, accesibles, interoperables y reutilizables*.

Mecanismos de coordinación efectiva

- ✓ **Confianza mutua**: Base para compartir datos sensibles sin vulnerar derechos.
- ✓ **Traducción interinstitucional**: Adaptación de lenguajes técnicos, legales y organizativos.
- ✓ **Negociación de estándares**: Acuerdos sobre formatos, niveles de acceso y responsabilidades.
- ✓ **Deliberación conjunta**: Toma de decisiones sobre gobernanza de datos y políticas públicas.

IDENTIFICACIÓN DE RIESGOS Y SOLUCIONES

Clase de riesgo: Incendio o Fuego

- Grado de Negatividad: Muy Severo.
- Frecuencia de Evento: Aleatorio.
- Grado de Impacto: Grave.
- Grado de Certidumbre: Probable.
- Situación actual: Acción correctiva.

Clase de riesgo: Robo Común de Equipos y Archivos

- Grado de Negatividad: Grave.
- Frecuencia de Evento: Aleatorio.
- Grado de Impacto: Moderado.
- Grado de Certidumbre: Aleatorio.
- Situación actual Acción preventiva

1. **Problema**

Debido a la gran cantidad de entrada y salida de personas particulares a la institución, no son registradas con el personal de seguridad y tienen libre acceso en todos los pisos.

Se han reportado casos en la cual haya existido manipulación y reubicación de equipos sin el debido conocimiento y autorización entre la Unidad Administrativa y la Unidad de

Tecnologías de Información y Comunicación.

La salida de un equipo informático es registrada por el personal de la Oficina y por el personal de seguridad en turno. No se verifica si el Personal de Seguridad cumple con la inspección de los usuarios, sobre su obligación de cerrar puertas y ventanas al finalizar su jornada. Al respecto Personal de Seguridad emite recomendaciones sobre medidas de Alerta y seguridad.

2. **Identificación de la solución**

Para evitar el robo común de equipos y archivos es necesario analizar las siguientes situaciones:

- ¿En qué lugar se encuentra ubicada la Institución?
- ¿Si las computadoras están expuestas a la visibilidad de las personas que pasan desde la calle?
- ¿Si el personal de seguridad en la Institución, se encuentran ubicadas en zonas estratégicas?
- ¿Cuánto valor tiene actualmente las bases de datos?
- ¿Cuánta pérdida podría causar en caso de que se hicieran públicas las bases de datos?
- Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.
- Trabajo no supervisado, especialmente durante el turno de noche, malas técnicas de contratación, evaluación y de despido de personal.
- Disponer de los números telefónicos de los principales medios de rescate como (Ecu-911, Policía Nacional, Seguridad Privada de la Empresa)

3. **Clase de riesgo: Vandalismo**

- Grado de Negatividad: Moderado.
- Frecuencia de Evento: Aleatorio.
- Grado de Impacto: Grave.
- Grado de Certidumbre: Probable.
- Situación actual Acción correctiva.

Problema

El Consejo Nacional Electoral se encuentra ubicado donde el índice de vandalismo es bajo, pero en el caso que se presente este inconveniente y el intento de vandalismo sea mayor, este representaría un gran riesgo dentro del centro de cómputo, ya que se podría perder toda la información almacenada y por ende las actividades dentro de la empresa se verían afectadas en gran parte.

Identificación de la solución

A continuación, se menciona una serie de medidas preventivas:

- Establecer vigilancia mediante cámaras de seguridad en el sitio, para registrar la entrada y salida del personal.
- Instalar identificadores mediante tarjetas de acceso.
- Determinar lugares especiales fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de la empresa.
- Aplicar los medios necesarios para la recuperación inmediata de la base de datos de la empresa en el local alterno.

4. Clase de riesgo: falla en los equipos

- Grado de Negatividad: Grave.
- Frecuencia de Evento: Aleatorio.
- Grado de Impacto: Grave.
- Grado de Certidumbre: Probable.
- Situación actual Acción correctiva.

Problema

La Red de energía en los Servidores, en la Unidad de Tecnologías de Información y Comunicación cuenta con una instalación eléctrica estabilizada, no existe un adecuado tendido eléctrico dentro de algunas oficinas de la institución. La falta de energía en éstos, origina la ausencia de uso de los servicios de red, los Sistemas Informáticos, teléfonos IP, mantenimiento remoto, su adecuado apagado y encendido, dependen los servicios de red eléctrica en el Área.

Identificación de la solución

La falla en el hardware de los equipos informáticos, requiere un rápido mantenimiento o reemplazo, existe mantenimiento de los equipos de cómputo, para lo que es importante contar con proveedores, en caso de requerir reemplazo de piezas, y de ser posible contar con repuestos. Dado el caso crítico de que los discos duros presentan fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

- Ubicar el disco malogrado.
- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a

jefes de área.
- Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
- Bajar el sistema y apagar el equipo.
- Retirar el disco duro malo y reponerlo con otro del mismo tipo, y formatearlo para su correcta utilización.
- Restaurar el último backup, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
- Verificación el buen estado de los sistemas.
- Habilitar las entradas al sistema para los usuarios.

En el caso de las memorias RAM, se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto, si hubiese un error de paridad, el servidor se autocorregirá.
- Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la Empresa, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

- Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a los directivos de área.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Retirar la conexión del servidor con el concentrador, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
- Probar los sistemas que están en red en diferentes estaciones.
- Finalmente, luego de los resultados, habilitar las entradas al sistema para los usuarios

Problema 1. Clase de riesgo: equivocaciones

- Grado de Negatividad: Moderado.
- Frecuencia de Evento: Periódico.
- Grado de Impacto: Moderado.

- Grado de Certidumbre: Probable.
- Situación actual Acción correctiva.

Problema

Cuando el usuario es practicante y tiene conocimientos de informática, tiene el impulso de navegar por los sistemas. En lo posible se debe cortar estos accesos, limitando su accionar en función a su labor de rutina, ya que no se sabe hasta qué punto el reemplazo tiene conocimientos sobre computación y si está capacitado para manejar debidamente el software.

Ejemplo: La Unidad de Tecnología de la Información y Comunicación del CNE no recibe comunicación del personal de reemplazo, por vacaciones, por lo tanto, supone que es la Oficina usuaria la que capacita al reemplazante. Se debe informar al Unidad de Tecnología de la Información y Comunicación del reemplazo para su registro y accesos a la Red y los Sistemas, por el tiempo que dure el reemplazo. Al término del periodo de reemplazo se restituye los valores originales a ambos usuarios.

Identificación de la solución

Se debe considerar las siguientes medidas preventivas:

- ¿Cuál es el conocimiento sobre computadoras o redes que tienen los empleados?
- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?
- Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.

Problema 2. Clase de riesgo: acción de virus informático

- Grado de Negatividad: Muy Severo.
- Frecuencia de Evento: Continuo.
- Grado de Impacto: Grave.
- Grado de Certidumbre: Probable.
- Situación actual Acción correctiva.

Problema

Se cuenta con un Software Antivirus corporativo. Pero no hay un contrato anual para su actualización. Se debe evitar que las licencias no expiren, se requiere la renovación de contrato anualmente este se cumpla.

Identificación de la solución

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

- Se contará con antivirus para el sistema; que nos permite aislar el virus para su futura investigación.
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe el virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

- Utilizar los discos de instalación que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado.
- Insertar el disco de instalación antivirus, luego instalar el sistema operativo, de tal forma que revise todos los archivos y no sólo los ejecutables. De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del escaneado. Finalizado el escaneado, reconstruir el Master Boot del disco duro.

Problema 3. Clase de riesgo: accesos no autorizados

- Grado de Negatividad: Grave.
- Frecuencia de Evento: Aleatorio.
- Grado de Impacto: Grave.
- Grado de Certidumbre: Probable.
- Situación actual Acción correctiva.

Problema

Se controla el acceso al Sistema de Red mediante la definición de “Cuenta” o “Login” con su respectiva clave para verificar si esta acción se cumple. A cada usuario de Red se le asigna los “Atributos de confianza” para el manejo de archivos y acceso a los sistemas.

Identificación de la solución

Cuando el personal cesa en sus funciones y/o es asignado a otra área, se le redefinen los accesos

y autorizaciones, quedando sin efecto la primera. Esto se cumple de modo extemporáneo, siendo lo indicado actualizar los accesos al momento de producirse el cese o cambio.

Todos los usuarios sin excepción tienen un "login" o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de cinco (5) dígitos. No se permiten claves en blanco. Además, están registrados en un grupo de trabajo a través del cual se otorga los permisos debidamente asignados por el responsable de área.

Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla. Ello se aplica tanto a su autenticación como usuario de Red como usuario de Sistemas en la institución, si lo tuviere.

Problema 4. Clase de riesgo: robo de datos o pérdida de la información

- Grado de Negatividad: Grave.
- Frecuencia de Evento: Aleatorio.
- Grado de Impacto: Grave.
- Grado de Certidumbre: Probable.
- Situación actual Acción correctiva.

Problema

Las Oficinas tienen quemadoras de CD/DVD, puertos USB, pero no se lleva un control sobre la información que ingresa y/o sale del ordenador. El servicio de Internet es potencialmente una ventana abierta para el robo de información electrónica, existen políticas que regulan el uso y acceso del Servicio de Internet. Los documentos impresos (informes, reportes, contratos, etc.) normalmente están expuestos al robo por que no se acostumbra guardarlos como debe ser.

Identificación de la solución

El acceso a los terminales se controla, mediante claves de acceso, de esta manera se impide el robo de información electrónica. A través de las políticas se seguridad se impide el ingreso a los Servidores.

El Robo de datos se puede llevarse a cabo bajo tres modalidades:

a) La primera modalidad consiste en sacar "copia no autorizada" a nuestros archivos electrónicos aun medio magnético y retirarla fuera de la institución.
b) La segunda modalidad y tal vez la más sensible, es la sustracción de reportes impresos y/o informes confidenciales.
c) La tercera modalidad es mediante acceso telefónico no autorizado, se remite vía Internet a direcciones de Correo que no corresponden a la Gestión Empresarial. A las cuales se

las previene a través de las siguientes acciones:

- Control de acceso al Área de Sistemas: El acceso al área de Informática estará restringido:
- Sólo ingresan al área el personal que trabaja en el área.
- El ingreso de personas extrañas solo podrá ser bajo una autorización.
- Limitación del uso de programas para usuario o terminales.
- Límite de tentativas para la verificación del usuario, tiempo de validez de las contraseñas, o uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 minutos).

Problema 5. Clase de riesgo: manipulación y sabotaje

- Grado de Negatividad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave
- Grado de Certidumbre: Probable
- Situación actual Acción correctiva

Problema

Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadas a causar daños físicos y lógicos en el sistema de información de la institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje.

Identificación de la solución

No se comunica el movimiento de personal a la Unidad de Tecnología de Información y Comunicación de la institución, para restringir accesos del personal que es reubicado y/o cesado del Consejo Nacional Electoral. Es conveniente la comunicación anticipada del personal que será reubicado y/o cesado con el objeto de retirar los derechos de operación de escritura para otorgarle los derechos de consulta antes de desactivar la cuenta.

La protección contra el sabotaje requiere:

- Una selección rigurosa del personal.
- Buena administración de los recursos humanos
- Buenos controles administrativos
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.

- Asignar a una persona la responsabilidad de la protección de los equipos en cada área.

Problema 6. Clase de riesgo: fenómenos naturales

- Grado de Negatividad: Grave
- Frecuencia de Evento: Aleatorio
- Grado de Impacto: Grave
- Grado de Certidumbre: Probable
- Situación actual Acción Preventiva

Problema

Terremoto e inundación. Para evitar problemas con inundaciones o terremotos es necesario ubicar los servidores a un promedio de 50 cm de altura. En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura.

Identificación de la solución

Cuando el daño del edificio ha sido mayor, se necesita evaluar el traslado a un nuevo local Alterno, hasta considerar la posibilidad del traslado.

Cuando el daño ha sido menor se procede:

- Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable encargado de Soporte y Mantenimiento.
- Recoger los respaldos de datos, programas, manuales y claves. Responsable encargado de Redes.
- Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento
- Restaurar la información de las bases de datos y programas. Responsable encargado de Desarrollo.
- Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo.

ESTRATEGIAS DE PROTECCIÓN TECNOLÓGICAS

Proporcionan mayor seguridad a la información y a los activos críticos, en caso de necesitar una solución inmediata en respuesta a un evento imprevisto. Las áreas en las que se deben definir estrategias de protección son:

- Manejo de la información.
- Obtención de respaldos de información.
- Seguridad en la red.

- Seguridad física.
- Controles contra códigos maliciosos.
- Mantenimiento de los equipos.
- Sabotaje o daño accidental.

1. Manejo de la información

Para las estrategias de protección para el manejo de la información en el plan de Contingencia del Consejo Nacional Electoral, se ha realizado en base a las Normas Técnicas Ecuatorianas (NTE) para Tecnologías de la Información (TI) como es la Norma NTE INEN-ISO/IEC 27002:2009.

1. Restringir el acceso al personal no autorizado a las instalaciones donde se almacena información sensible o critica.
2. Realizar pruebas a los respaldos de información para verificar que se encuentra en buen estado.
3. Debe estar debidamente etiquetada en todos los medios almacenados y su nivel de sensibilidad.
4. Debe contar con procedimientos de protección al momento de intercambiarla a través de la red pública.
5. Uso de técnicas de encriptación para proteger la confidencialidad, la integridad y la autenticidad de la información.
6. Responsabilidades a los empleados de no comprometer a la organización a través de difamación acoso suplantación de identidad etc.
7. Implementar precauciones sobre métodos de robo de información con ingeniería social.
8. Procedimientos y policías para la protección de la información en los sistemas que usan información.

2. Obtención de copias de seguridad de la información

Para las estrategias de protección en la obtención de copias de seguridad de la información en el plan de Contingencia del Consejo Nacional Electoral, se ha realizado en base a las Normas Técnicas Ecuatorianas (NTE) para Tecnologías de la Información (TI) como es la Norma NTE INEN- ISO/IEC 27002:2009.

1. Implementación de políticas y proceso de copias de respaldo de la información y software.
2. Realizar registros exactos y completos de las copias de respaldo.

3. Contar con procedimientos de restauración pruebas que funcionen de la información.
4. La información de respaldo debe ser almacenada en un lugar externo a las instalaciones principales para evitar ser afectada por cualquier desastre que pueda presentarse.

3. Seguridad en redes

Para las estrategias de protección para la seguridad en redes en el plan de Contingencia del Consejo Nacional Electoral, se ha realizado en base a las Normas Técnicas Ecuatorianas (NTE) para Tecnologías de la Información (TI) como es la Norma NTE INEN-ISO/IEC 27002:2009.

1. Los sistemas la red eléctrica y de telecomunicaciones deben estar protegidos contra interceptaciones o daños.
2. El cableado debe estar debidamente protegido para evitar posibles daños o interceptaciones no autorizadas.
3. Tanto equipos como cables deben estar debidamente etiquetados para evitar errores en el manejo, o conexiones erróneas en la red.
4. Contar con un plano del cableado de la red para ubicar rápidamente algún segmento de la red que se encuentre afectado.
5. Realizar un reconocimiento en las instalaciones físicas en busca de dispositivos conectados sin autorización.
6. Solo el personal autorizado y capacitado puede realizar el mantenimiento de los equipos de red.
7. Llevar un registro del manteamiento preventivo y correctivo realizado a los equipos.
8. Definir los controles necesarios para salvaguardar la confidencialidad e integridad de los datos través de las redes públicas e inalámbricas.
9. Se recomienda el uso de herramientas para implementar algoritmos de encriptación para proteger las comunicaciones por correo electrónico donde se envíe información confidencial.
10. Crear políticas para la protección contra riesgos con la obtención de archivos y software desde o a través de redes externas.
11. Deshabilitar de los equipos los servicios que no sean necesarios y verificar los posibles puertos que se encuentren abiertos y no se estén utilizando para cerrarlos.
12. Gestionar y optimizar la distribución apropiada del ancho de banda para la red cableada y la red inalámbrica.
13. Realizar un monitoreo de la red, detectar y corregir vulnerabilidades para proteger la infraestructura y la red de ataques.
14. Solicitar permisos de autentificación al momento de conectarse a la red ya sea inalámbrica o cableada médiate claves de acceso.

15. Identificar las seguridades necesarias para el acceso a servicios niveles de seguridad.
16. Para la protección del acceso no autorizado a nivel lógico se sugiere la habilitación de un firewall y proxy que impida el ingreso desde redes externas hacia la red interna de la empresa.

4. Seguridad física

Para las estrategias de protección para la seguridad física en el plan de Contingencia del Consejo Nacional Electoral, se ha realizado en base a las Normas Técnicas Ecuatorianas (NTE) para Tecnologías de la Información (TI) como es la Norma NTE INEN-ISO/IEC 27002:2009.

1. Restringir el acceso al departamento de sistemas mediante la utilización de llaves, tarjetas de identificación y sistemas biométricos.
2. El acceso al departamento de sistemas debe ser únicamente por el personal autorizado.
3. Controlar el acceso a las áreas donde se procesa o almacena la información sensible, se debería implementar un registro con fecha y hora de ingreso y salida a los visitantes, los mismos que siempre deben ser supervisados por el personal encargado.
4. Cuando se cuenta con servicios de soporte de terceros se debe tener el acceso restringido y solo si es necesario se debe autorizar el acceso y llevar el respectivo monitoreo.
5. Contar con vigilancia para realizar un constante monitoreo de posibles sospechosos que quieran atentar con la integridad de los equipos, infraestructura.
6. Se recomienda la contratación o implementación de oficinas alternas y procedimientos de protección en casos de desastres naturales o manifestaciones sociales.
7. Evitar el uso de equipos de grabaciones de videos, fotográficas sin la respectiva autorización.
8. Evitar que la información sensible se encuentre a simple vista de forma de reducir el riesgo por visualización de la información por personas no autorizadas.
9. Realizar un monitoreo constante de las condiciones ambientales dentro del centro de datos para evitar fallas ocasionadas estos equipos que afectaría al procesamiento de la información.
10. Procedimientos de revisión en los de iluminación electricidad agua, ventilación para garantizar el adecuado funcionamiento.
11. Debe contar con un UPS para el cierre ordenado de los equipos o el funcionamiento continuo de las operaciones críticas.

5. Códigos maliciosos

Para las estrategias de protección para los códigos maliciosos en el plan de Contingencia del Consejo Nacional Electoral, se ha realizado en base a las Normas Técnicas Ecuatorianas (NTE) para Tecnologías de la Información (TI) como es la Norma NTE INEN-ISO/IEC 27002:2009.

1. Realizar procesos de concientización a usuarios sobre códigos maliciosos y la importancia de la seguridad de la información dentro de la empresa.
2. Llevar a cabo revisiones regulares de software y el contenido de datos de los sistemas, se debe investigar la presencia de archivos no aprobados o modificaciones no autorizadas.
3. Usar software de fuentes conocidas y de confianza, de tal forma que se evite copias falsificadas que puedan ser objetivos de un atacante al no contar con las debidas garantías que provee un software oficial.
4. Para la detección de códigos maliciosos se recomienda la utilización de un software que permita detectarlos y en caso de ser necesario reparar archivos que se vean afectados por estos códigos maliciosos, este software debe estar en continua actualización.
5. Para mayor eficiencia se considera contar con un antivirus para los equipos de usuario y otro para los servidores, de esta manera es más difícil la propagación de los virus al contar con la diversificación de antivirus, es importante que estos dos software escogidos sean compatibles para evitar fallas dentro del sistema operativo.
6. A fin de evitar que códigos maliciosos ingresen al sistema se prohíbe la instalación de programas sin el permiso del administrador de red.
7. La instalación de software debe ser realizada únicamente por el personal del departamento de sistemas y tecnología, se recomienda contar con una lista del software, este será seleccionado por la gerencia y del departamento de sistemas y tecnologías.
8. Contar con información actualizada sobre seguridad de la información y acerca de los nuevos códigos maliciosos.
9. Procedimientos y responsabilidades para la gestión y verificación de códigos maliciosos en medios extraíbles, correos electrónicos páginas web, archivos enviados por la red.

6. Fallas en hardware o software

Para las estrategias de protección para las fallas en hardware o software en el plan de Contingencia del Consejo Nacional Electoral, se ha realizado en base a las Normas Técnicas

Ecuatorianas (NTE) para Tecnologías de la Información (TI) como es la Norma NTE INEN-ISO/IEC 27002:2009.

1. Se recomienda que al menos dos veces al año se realice el mantenimiento preventivo de todos los equipos tanto de redes como Computadoras, y llevar un control de los daños encontrados, y el desgaste de los mismos
2. Se sugiere contar con uno o más empleados debidamente capacitados que brinden el mantenimiento preventivo y correctivo a todos los equipos de la organización.
3. Los equipos de computación deben tener un regulador de voltaje para evitar daños por variaciones de voltaje.
4. Implementar herramientas sistematizadas para controlar el inventario de Hardware y Software de la empresa.
5. Realizar actualizaciones de seguridad para los sistemas operativos.

7. Sabotaje o daños accidentales

Para las estrategias de protección para el sabotaje o daños accidentales en el plan de Contingencia del Consejo Nacional Electoral, se ha realizado en base a las Normas Técnicas Ecuatorianas (NTE) para Tecnologías de la Información (TI) como es la Norma NTE INEN-ISO/IEC 27002:2009.

Aunque no existe protección absoluta contra el robo de la información se puede minimizar el impacto haciendo uso de algunas herramientas:

1. Contar con políticas de seguridad de información dentro de la organización.
2. Designar responsabilidades a cada uno de los empleados.
3. Solicitar la debida autentificación y permisos por parte del administrador para el acceso y modificación de datos.
4. Solicitar permisos de administrador para la copia de información en cualquier tipo de dispositivo extraíble por parte de las estaciones de trabajo.
5. Establecer medidas drásticas con empleados que atentan con la integridad de la empresa.

8. Tiempo de Recuperación e impacto generado si fallan los activos críticos

Hay que tomar en cuenta que existen varias amenazas como desastres naturales, fallas en los equipos, daños provocados por terceros, etc., por las que la información e infraestructura de

red se verían comprometidas en integridad y disponibilidad.

En el caso de que suscite algún tipo de daño debido a desastres naturales el impacto producto de la materialización de estas amenazas seria crítico, generando pérdidas económicas.

Si la materialización de amenazas se presenta en los sistemas principales o en los equipos críticos, el impacto para la empresa seria alto, se suspenderían las actividades diarias, generaría pérdidas económicas y molestias en los usuarios.

Cuando los daños se producen en los equipos de usuario final el impacto sería normal pues no interrumpiría con las actividades de la empresa y el costo de recuperación sería menor.

9. **Documentación del Proceso**

A continuación se presenta un manual de procedimientos que permita la pronta reanudación de las operaciones en el menor tiempo posible luego de haberse presentado un evento que dificulte el desarrollo normal de las actividades en la empresa.

MÉTODOS PARA REALIZACIÓN DE PRUEBAS Y VALIDACIÓN

1. **Pruebas específicas**

En una actividad específica se trata de probar al personal, utilizando los procesos definidos en el plan, de esta manera el personal tendrá, tareas específicas y desarrollará la habilidad para cumplirla.

2. **Pruebas de escritorio**

Se realizarán las pruebas a través de un conjunto de preguntas típicas las mismas que se caracterizan por tener:

- Un formato prestablecido
- Va dirigido a los equipos de trabajo
- Permite probar las habilidades de diligénciales de los líderes de equipos

Los ejercicios son realizados de una forma hipotética, las preguntas que se generan serán resueltas por cada uno de los equipos responsables de los riesgos que se encuentren a cargo

3. **Pruebas en tiempo real**

Las pruebas en tiempo real se las realiza a cualquier clase de riesgo por un periodo de tiempo determinado, las mismas que pueden ser de la siguiente manera:

- Se lo utilizará para comprobar ciertas partes importantes del plan en tiempo real.
- Permitirá verificar las habilidades de coordinación entre los equipos de trabajo y las relaciones de coordinación interna y externas los mismos que se encuentran asignados para afrontar cada uno de los riesgos a suscitarse.
- Esta prueba se las debe ejecutar en el momento en que se están realizando las actividades normales en la empresa sin que estas afecten el funcionamiento de la misma.
- Estas pruebas como se menciona anteriormente no deben afectar a las actividades de la empresa, ni comprometer ninguno de los servicios que la misma ofrece, esta debe estar dirigida o a cargo de cada uno de los jefes de grupos de trabajo y enlazadas con cada una de las relaciones de coordinación, dependiendo el riesgo que se desea comprobar.

4. Preparación de la Pre-prueba

- ✓ Trata de una serie de pasos que hay que seguir antes de realizar las pruebas del plan de contingencias
- ✓ Repasar cada uno de los riesgos citados en el plan
- ✓ Confirmar que existan responsables para cada uno de los riesgos
- ✓ Confirmar que el plan se encuentre aprobado por la autoridad máxima de la Empresa
- ✓ Preparar a todo el personal involucrado en el plan
- ✓ Establecer fechas y horas para la ejecución del plan
- ✓ Documentar cada uno de los ensayos que se le realicen al plan informático
- ✓ Designar días específicos para la prueba sin que estas afecten al normal desarrollo de las actividades de la empresa
- ✓ Al iniciar las pruebas se orientará en preparar a los equipos que ejecutaran con éxito el plan de contingencias
- ✓ Enfocar los problemas en los servicios que dependen de sistemas específicos o dependen de compañías externas donde se asume que haya problemas
- ✓ Definir lo lugares en los que se realizara las reuniones de los equipos de plan de contingencias
- ✓ Entregar a cada uno de los departamentos de la empresa una copia del plan de contingencias para el personal se encuentre al tanto en caso de que se presentara alguna emergencia.

COMPROBACIÓN DEL PLAN Y MONITOREO

- ✓ La fase de Monitoreo del Plan de Contingencia en el Consejo Nacional Electoral nos dará la seguridad de que podamos reaccionar en el tiempo preciso y con la acción

correcta. Esta fase es de mantenimiento. Cada vez que se da un cambio en la infraestructura, debemos de realizar un mantenimiento correctivo o de adaptación.

- ✓ La comprobación del plan y monitoreo debe ser un ensayo en el cual encierre cada uno de los riesgos que se citan en el plan, que involucre a cada una de las relaciones coordinación tanto interna como externa y que integre cada uno de los puntos críticos, de cada uno de los riesgos.

- ✓ El éxito del plan de contingencias reside en tanto que nos acerquemos más a las medidas a tomar de la prueba, con cada una de los resultados que deseamos obtener.

- ✓ Para hacer la comprobación y monitoreo del plan de contingencia se lo realiza a través de una lista de chequeo las mismas que se encuentran acorde a cada uno de los riesgos que se ha estimado en el plan.

CONCLUSIONES

A partir del análisis técnico, normativo y estratégico de la seguridad digital, se pueden establecer las siguientes conclusiones claves:

10. **La ciberseguridad es una condición estructural para la gobernanza digital.** La protección de sistemas y redes no solo previene ataques, sino que garantiza derechos fundamentales como la privacidad, la integridad informativa y la seguridad jurídica. Su implementación debe ser transversal en todas las instituciones.
11. **El manejo de datos requiere responsabilidad legal, ética y organizaciona.** El tratamiento de datos informáticos debe cumplir con principios como finalidad, proporcionalidad y consentimiento informado, tal como lo establece la **Ley Orgánica de Protección de Datos Personales (LOPDP)** en Ecuador. La trazabilidad y clasificación de datos son esenciales para evitar vulneraciones.
12. **Los planes de contingencia fortalecen la resiliencia institucional.** Contar con protocolos de prevención, respuesta y recuperación ante incidentes permite minimizar el impacto de ciberataques, fallos técnicos o desastres naturales. La planificación debe incluir simulacros, respaldo de información y comunicación estratégica.
13. **La articulación entre normativa y estándares técnicos es indispensable.** La integración de marcos como **ISO/IEC 27001**, **NIST SP 800-34** y la LOPDP permite construir sistemas robustos y contextualizados. Esta articulación favorece la interoperabilidad, la auditoría y el cumplimiento regulatorio.
14. **La ciberseguridad es también una cuestión de justicia digital e inclusión.** Las brechas tecnológicas y la falta de capacitación pueden convertir la seguridad digital en un privilegio. Es necesario promover una cultura organizacional inclusiva, con formación continua y acceso equitativo a herramientas de protección.

RECOMENDACIONES

A partir de los desafíos actuales y las mejores prácticas internacionales, estas recomendaciones buscan fortalecer la resiliencia institucional y proteger los activos digitales frente a amenazas cada vez más sofisticadas:

1. **Adoptar el modelo de confianza cero (Zero Trust)**

   - ✓ Verificar continuamente la identidad de usuarios y dispositivos.
   - ✓ Implementar autenticación multifactor (MFA) en cuentas críticas.
   - ✓ Aplicar el principio de mínimos privilegios para limitar accesos innecesarios.

2. **Proteger integralmente los datos y la infraestructura en la nube**

   - ✓ Cifrar los datos sensibles en tránsito y en reposo.

- ✓ Implementar estrategias de prevención de pérdida de datos (DLP).
- ✓ Realizar auditorías periódicas con herramientas de protección nativa en la nube (CNAPP).

3. Automatizar la respuesta a incidentes

- ✓ Integrar soluciones de detección y respuesta ampliada (XDR).
- ✓ Usar herramientas de automatización (SOAR) para reducir tiempos de reacción.
- ✓ Realizar simulaciones periódicas de ciberataques para evaluar la eficacia del plan de contingencia.

4. Fortalecer la seguridad en la cadena de suministro

- ✓ Exigir estándares de ciberseguridad a proveedores y socios.
- ✓ Aplicar segmentación de red y controles de acceso basados en Zero Trust.
- ✓ Monitorear riesgos en tiempo real con herramientas avanzadas.

5. Desarrollar una cultura organizacional de ciberseguridad

- ✓ Capacitar al personal en prevención de phishing y técnicas de ingeniería social.
- ✓ Fomentar el uso de gestores de contraseñas y buenas prácticas digitales.
- ✓ Incluir métricas de seguridad en la evaluación institucional.

Bibliografía consultada:

- Aguilera P. (2010). Seguridad Informatica. México: Editex. Alvarez A. (2005). Hablemos de Seguridad. Pluma de Mompox.
- Anton, G. L. (2009). Plan de Contingencia Informatico y Seguridad de Información 2009. En G. L. Anton, Plan de Contingencia Informatico y Seguridad de Información 2009. Piura: http://www.eumed.net/libros- gratis/2009c/605/indice.htm.
- Areitio J. (2008). Seguridad de la información Redes, Informática y Sistemas de Información. Madrid: Paraninfo.
- Baca G. (2016). Seguridad Informática. México: Patria. Baud, Jean Luc. (2017). Itil V3. España: Eni ediciones. Bertolín, J. A. (s.f.). E.
- Caballero C, Clavero J. (2016). Sistemas de Almacenamiento UF1466. España: Elearning S.L.
- Carlos Caballero González, J. A. (2016). Sistemas de Almacenamiento UF1466. España: Elearning S.L.
- Chicano E. (2014). Gestión de Incidentes de Seguridad Infomática. IFCT0109. Málaga: IC Editorial.
- Cisneros J. (1998). Panorama sobre Base de Datos. Baja California: Luis Enrique Medina Gómez.
- COBARSI J. (2011). SISTEMA DE INFORMACIÓN EN LA EMPRESA. BARCELONA: UOC.
- Corrales, J. (2005). Ayudante Técnicos. Opcion Informatica. Junta de Andalucia. España: MAD, S.L.
- Corrales, J. D. (2005). Ayudante Técnicos. Opcion Informatica. Junta de Andalucia. España: MAD, S.L.
- De Pablos C. (2004). Informática y Comunicaciones en la Empresa. Madrid: Esic.
- Del Peso E. (2003). Manual de Outsourcing Informático (Análisis y Contratación). España: Díaz de Santos.
- Diego, L. (2015). Auditoria Informatica. Vesprini & Vesprini, 52.
- García A, Hurtado C, Alegre M. (2011). Seguridad Informática. España: Paraninfo.
- Gómez A. (2011). Enciclopedia de la Seguridad Informática 2° edición. España: Ra-Ma.
- HERAS, I. (2011). ISO 9000, ISO 14000 Y OTROS METAS ESTÁNDARES EN PERSPECTIVA. REVISTA UNIVERSIA BUSINESS REVIEW, 72.
- Hernan, L. (2015). Fuentes de daño. Auditoria Informatica, 65-66. Julieta, D. (2015). RIESGO. vesprim & vesprim, 47.
- López P. (2010). Seguridad Informática. México: Editex.
- Marchionni E, Formoso O. (2012). Virtualizacion con VMware. Buenos Aires: Fox Andina.
- Martínez J. (2004). Planes de Contingencia la Continuidad del Negocio en las Organizaciones. España: Diaz de Santos.
- MONCADA G. (2001). Guía Práctica para el Desarrollo de Planes de Contingencia de

Sistemas de Información. LIMA: Taller Gráfico del Instituto Nacional de Estadística e Informática.OEA. (2013

Fuentes consultadas

- ManageEngine: Cómo implementar un modelo de seguridad Zero Trust
- Cloudflare: Guía para comenzar con zero trust
- Object First (Ootbi): Guía completa para implementar Zero Trust
- NIST Special Publication 800-207 (Zero Trust Architecture)
- Uso de contraseñas seguras y autenticación multifactor: TuProfeDigital.com - 10 Medidas de Seguridad
- Estrategias completas de protección y gestión en TI: Tenea.com - Seguridad Informática
- Protección integral de datos con cifrado, backups y monitoreo: Splashtop.com - Estrategias de Protección de Datos
- Cultura de seguridad y ciberseguridad organizacional: Siconta Blog

INDICE

CAPITULO I
CIBERSEGURIDAD

CAPITULO II
MANEJO DE DATOS INFORMATICOS

CAPITULO III
PLAN DE CONTIGENCIA

La Agencia ISBN Ecuador

CERTIFICA

Que Toapanta Cuascota, Martha Susana con número de identificación 1714962634 está registrado en La Agencia ISBN Ecuador y figura como Editor - autor del siguiente título:

TÍTULO	ISBN 13 DÍGITOS
Ciberseguridad y manejo de datos Informáticos [D]	978-9907-0-0891-3

Nota: [I] => Impreso [D] => Digital.

Este certificado se expide a solicitud del interesado, en la ciudad de Quito a los 27 días del mes de febrero de 2026. La presente certificación no acredita titularidad de derechos de autor sobre la obra aquí contenida.

Atentamente,

Firmado electrónicamente por: CARLOS MAURICIO MANGIA CARVAJAL

Anl. Sist. Carlos Mangia Carvajal

Agencia ISBN Ecuador

Si desea verificar la información puede ingresar aquí: https:///isbnecuador.celibro.cerlalc.org/catalogo.php