TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MARCOS NORMATIVOS)

Unidad I – caso practico

Profesor: Lic. Juan Pablo Villalba

Alumno: Balbuena Atar Dante Gabriel

Tucumán, Tafí Viejo – septiembre 2024

Contenido

1. Introducción

TecnoData S.A., una empresa de desarrollo de software y consultoría en IT, se enfrenta a importantes desafíos en términos de seguridad de la información. Con una infraestructura híbrida que incluye tanto servidores físicos como servicios en la nube, y una base de 150 empleados que trabajan en diversos proyectos locales e internacionales, la empresa ha experimentado incidentes de seguridad que han puesto en riesgo información sensible. Estos incidentes han evidenciado la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con las Normas ISO 27000 e ISO 27001.
El objetivo de este trabajo es proponer un enfoque sistemático para gestionar y proteger los activos de información de la empresa. Para ello, se evaluarán los riesgos críticos, se definirán políticas y procedimientos de seguridad, y se diseñará un plan de continuidad del negocio que garantice la operatividad de la organización ante cualquier incidente. Además, se revisarán las obligaciones legales que TecnoData S.A. debe cumplir tanto en el contexto del **GDPR** como de la legislación argentina de protección de datos.
La implementación de estas normas no solo permitirá mitigar los riesgos de seguridad, sino también mejorar la competitividad de TecnoData S.A. en un mercado cada vez más exigente en términos de ciberseguridad y privacidad de la información.

2. Desarrollo

1) Evaluación de riesgos

1. En el Incidente de Phishing que considero al mismo como un riesgo critico, aplicaría de los 114 controles provenientes del anexo A el control A.7.2 Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. en el control A.7.2.2 Concienciación, educación y formación en seguridad de la información.
2. Para mitigar los problemas con el acceso No Autorizado a Servidores aplicaría el control A.9.2.6 que implica el Retiro o ajuste de los derechos de acceso.
3. Con respecto a la Pérdida de Datos en la Nube el control A.12.1.4 es el mas adecuado para mitigar el riesgo lo que implica que se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
4. En cuanto a las Fallas en la Gestión de Backups, la mejor solución es aplicar el control A.12.3.1, este control implica que se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
5. Para mitigar el riesgo por el uso No Autorizado de Software aplicaría el control A.12.6.1 ya que este control dice que se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

2) Política de seguridad propuesta:

Las computadoras siempre deben estar bloqueadas durante el tiempo que no se estén usando, cada empleado debe tener sus datos de acceso a las herramientas y no deben ser compartidas bajo ningún aspecto, el empleado al ingresar a operaciones debe tener su tarjeta de acceso propia y llevarla con su credencial visible durante su jornada laboral, no revelar información confidencial (clientes, contratos etc) como por ejemplo en redes sociales, ante cualquier sospecha de fraude o actitud sospechosa reportar el caso a la línea de reporte brindado por la empresa.

3) Análisis de Cumplimiento:

Para cumplir con el GDPR y la Ley de Protección de Datos Personales de Argentina, TecnoData S.A. debe obtener consentimiento explícito para procesar datos, garantizar el derecho de acceso, rectificación y eliminación de los mismos, implementar medidas de seguridad como cifrado y controles de acceso, y notificar rápidamente cualquier brecha de seguridad. Además, debe registrar sus bases de datos y asegurarse de cumplir con los requisitos de protección de datos tanto a nivel local como internacional.

4) La siguiente tabla explica tanto el BCP y DRP de manera resumida para tener un panorama global.

BCP	DRP
Evaluación de Impacto en el Negocio (BIA)	Escenarios de desastres considerados
Identificación de recursos y dependencias críticas	Acciones y procedimientos de recuperación
Planificación de la continuidad	Comunicación durante una crisis
Mantenimiento y monitoreo continuo	Evaluación post - desastre
Capacitación del personal y simulacros	Pruebas y simulaciones del DRP
Actualización y revisión periódica del BCP	

5) Capacitación y concienciación:

Para desarrollar un programa de capacitación a empleados (phishing, usb, contraseñas, software) iré enumerando las medidas a tomar, esta enumeración no implica el nivel de importancia ya que solamente es para ordenar la información: 1) una plataforma de E-learning. 2) capacitación especifica para cada nueva herramienta de software que use la empresa o que piensa incorporar. 3) control de acceso a las instalaciones físicas de modo que no pueda filtrase dispositivos que puedan fugar información (celulares, usb etc). 4) resaltar la importancia critica de no divulgar información como por ejemplo las claves de acceso y la actualización de la misma de manera regular. 5) distribución de los programas de concienciación según el requerimiento (nueva herramienta, mal manejo de una herramienta etc) y de manera regular.

6) Gestión de Incidentes:
Implementación de un SOC con un área de monitoreo, lo cual inmediatamente reporta los incidentes a un sector de respuestas (analistas etc).

7) Revisión de Proveedores:
Implementación de un sistema de carga de formularios, lo cual este formulario incluye Información General del Proveedor, Prácticas de Seguridad, Manejo de Incidentes, Cumplimiento Normativo, Auditorías y Evaluaciones. Una vez que el proveedor complete el formulario, los datos se envían automáticamente a los especialistas de seguridad (SIEM) seguido de un Reporte y Seguimiento.

8) Implementación de 2FA:
Se implementará un 2FA a las aplicaciones críticas de "TecnoData S.A." como son:
Aplicaciones de Autenticación (TOTP), Notificaciones Push, Correo Electrónico (recibe un código de autenticación en su correo electrónico), biometría para el acceso a los servidores físicos, Certificados Digitales.

9) Controles de Acceso y Gestión de Identidades:
Se implementará IAM (Identity and Access Management) para las computadoras, notebooks, servidores y la infraestructura cloud. Utilizará la autenticación multifactor (MFA) para acceso a G Suite, AWS, y recursos internos. Asegurarse de que los accesos estén basados en roles y que se realicen auditorías periódicas de los permisos para garantizar que los usuarios solo tengan acceso a la información necesaria para sus funciones.

10) Gestión de Backups:
Frecuencia de Backup: diarios (datos críticos), Semanal (datos no críticos), mensual (archivos históricos)
Ubicación: local (servidores locales), Remoto (servicios de almacenamiento en la nube)
Cifrado: En tránsito (Uso de protocolos seguros), En reposo (algoritmos robustos)
Pruebas Periódicas de Restauración: Mensual (datos críticos), Anual (restauración completa del sistema)

3. Conclusiones

Se logra observar que las actividades propuestas en su conjunto dan una perspectiva muy amplia sobre diferentes aspectos en la seguridad de la empresa, decir que tiene una mirada holística seria lo mas acertado ya que nos permite abordar de manera mucho más fácil el método en la que encaramos la vida laboral en el futuro es decir que esta mas orientado a la realidad. Aporta seguridad al estudiante a la hora de organizar la implementación de las normas ISO 27001. En resumen, este trabajo logro aumentar mi conocimiento en marcos de trabajo y normativas y como implementarlos de manera eficiente en una empresa.

4. Referencias

ISO/IEC. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*. International Organization for Standardization. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

European Parliament and Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

National Institute of Standards and Technology (NIST). (2012). *Computer Security Incident Handling Guide: SP 800-61 Rev 2*. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/61/r2/final

National Institute of Standards and Technology (NIST). (2017). *Digital Identity Guidelines: SP 800-63-3*. National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-63-3/final

TechRadar. (2023). *Best backup software of 2023*. https://www.techradar.com/best/best-backup-software

Este documento sigue las normas de citación y referencias de la *Publication Manual of the American Psychological Association* (7ª ed.).