Carrera de Computación

Título:

Estándares y Legislación para la protección de datos e información

Asignatura:

Seguridad de la información

Estudiantes:

Adrián Viscaino

Bryam Barrera

Pedro Illaisaca

Docente:

Ing. Jennifer Yepez

Cuenca, 26 de noviembre de 2021

• ¿Qué consecuencias trajo o puede traer el ataque informático de la ANT, para el Estado Ecuatoriano y para los usuarios de este servicio? (3 puntos)

Trajo como consecuencia la suspensión total de los servicios en línea ofrecidos por la ANT.

Agentes de tránsito aprovecharon la situación para cometer actos de corrupción detenían a los conductores verificaban los datos del permiso de conducir y al no obtener respuesta alguna del sistema los agentes daban por sentado que el permiso de conducir era invalido por consiguiente se aprovecharon de la situación pidiendo sobornos.

El ataque hacia el activo principal (datos) de la ANT y sistema en general supone un evidente riesgo a la integridad de los datos de los titulares que tienen registros en la ANT pese a que 24 horas antes se supone que se mejoró la seguridad para evitar procesos fraudulentos, según investigaciones señalan que la base de datos de respaldo no sufrió alteraciones de información

• ¿Qué leyes ecuatorianas posiblemente violó la ANT al no proteger adecuadamente sus sistemas? (Considerar únicamente las leyes ecuatorianas vigentes, seleccionar al menos 3 leyes diferentes y mencionar mínimo 1 artículo por cada ley) (3 puntos)

Según la información recolectada sobre el ataque a los sistemas de la ANT posiblemente se vulneran las siguientes leyes.

El articulo 76 “Medidas técnicas de seguridad e invulnerabilidad” de la ley orgánica de telecomunicaciones (el Pleno, 2015) dicta que a los prestadores de servicios ya sea que usen redes propias o de terceros deberán, implementar las medidas apropiadas para preservar la seguridad en sus servicios e invulnerabilidad y el secreto en las comunicaciones que se transmitan por sus redes, con el objetivo de garantizar la seguridad frente a los riesgos existentes.

Numeral 12 del artículo 66 de la constitución del Ecuador (Ecuador & Asamblea Constituyente, 2008): Se reconoce y garantiza a las personas el derecho a la protección de los datos personales, incluido el acceso y decisión sobre la información y datos de esta naturaleza, incluyendo la protección correspondiente.

El Articulo 9 “Protección de datos” de la Ley de Comercio Electrónico (Ecuador & Ley de Comercio Electrónico, 2002): Para transferir datos, obtenidos directa o indirectamente se deberá contar con el consentimiento explícito de estos propietarios, pueden elegir la información que quieren compartir con terceros. La recopilación y uso de datos personales responderá a la privacidad, intimidad y Confidencialidad garantizada por la constitución de la República y solamente se pueden usar o transferir con la autorización del propietario del titular de la información.

Art. 38.- “Medidas de seguridad en el ámbito del sector público.” De la ley de Orgánica de protección de datos personales(el Pleno, 2021): Los mecanismos gubernamentales de seguridad de la información deben incluir medidas que se deben tomar cuando los datos personales enfrente riesgos, amenazas, vulnerabilidades, acceso no autorizado, pérdida, manipulación, destrucción o comunicación accidental o ilegal, el procesamiento de datos se implementará de acuerdo con los principios de seguridad de los datos personales, el presente artículo deberá ser acatado por todas las instituciones públicas.

• Tomando en cuenta las leyes ecuatorianas vigentes, ¿qué acciones puede tomar un ciudadano cuando ocurren este tipo de incidentes en las empresas estatales? (1 punto)

La acción que debe tomar un ciudadano cuando sus derechos han sido vulnerados es presentar la respectiva denuncia en la fiscalía acompañado de asesoramiento por parte de un abogado. En el caso ANT el ciudadano podría presentar una denuncia especificando que se vulnera el artículo 68 de la ley de protección de datos personales "Infracciones graves del responsable de protección de datos" (el Pleno, 2021) citando que el numeral 6 dicta que será sancionado por no implementar las debidas seguridades para proteger los datos personales de vulnerabilidades identificadas.

• Diseñar un programa de clasificación de datos para su institución basándose en el contenido presentado en la Unidad 1. Por lo tanto, el programa debe cumplir con los 14 pasos presentados.

1. Determinar los objetivos del proyecto de clasificación de datos (al menos 3). (3 puntos)

- Implementar una rutina de respaldo en las bases de datos de la Organización, para prevenir la perdida de información en caso de sufrir ataques que destruyan datos.
- Informar al personal que trabaja directamente con información confidencial mediante capacitaciones para dar a conocer las consecuencias que conlleva realizar un mal uso de los permisos otorgados.
- Ejecutar un plan de acción que permita conocer realmente qué tipo de información debe ser considerada confidencial, para enfocar de mejor manera los recursos hacia los datos que la organización considera importantes su resguardo.

2. Establecer apoyo organizacional: describir cómo se lograría ese apoyo. (1 punto)

Aplicar aspectos referentes a inteligencia de negocios para generar interés en altos mandos de la organización, el personal al notar el interés por parte de la gerencia refleja interés hacia sus roles asignados.

3. Desarrollar una política de clasificación de datos: presentar una política con al menos 4 reglas. (2 puntos)

La presente política establece 4 reglas acerca del manejo de los datos las cuales están descritas en un alto nivel.

Regla 1: Conocer detalladamente el tipo de información disponible y quien es el colaborador responsable de dichos datos, del mismo modo los datos disponibles deben contar con un formato legible ya que comúnmente las personas no profesionales en informática no suelen comprender correctamente información resultante de una consulta de base de datos.

Regla 2: Toda la información disponible en la Organización será clasificada según un nivel de confidencialidad establecida en 4 niveles:

- **Confidencial:** Es toda la información que al ser manipulada por personal no autorizado representa un riesgo hacia los activos de la organización.
- **Semiconfidencial:** Representa a toda la información con niveles medios de confidencialidad.
- **Uso interno:** Información que solamente está autorizada a personal administrativo en la organización.
- **Publica:** Esta no considera un riesgo para la organización de modo que puede ser accedida por el público en general.

Regla 3: Establecer un formato de etiquetado a la información clasificada, todo el documento descrito en papel se procederá a escanearlos y adicionar una marca de agua que informe el nivel de confidencialidad, por otra parte, a la información almacenada en bases de datos se procederá a desarrollar un módulo seguridad que consiste en un panel de control general donde se podrá visualizar la información y asignar el nivel de confidencialidad.

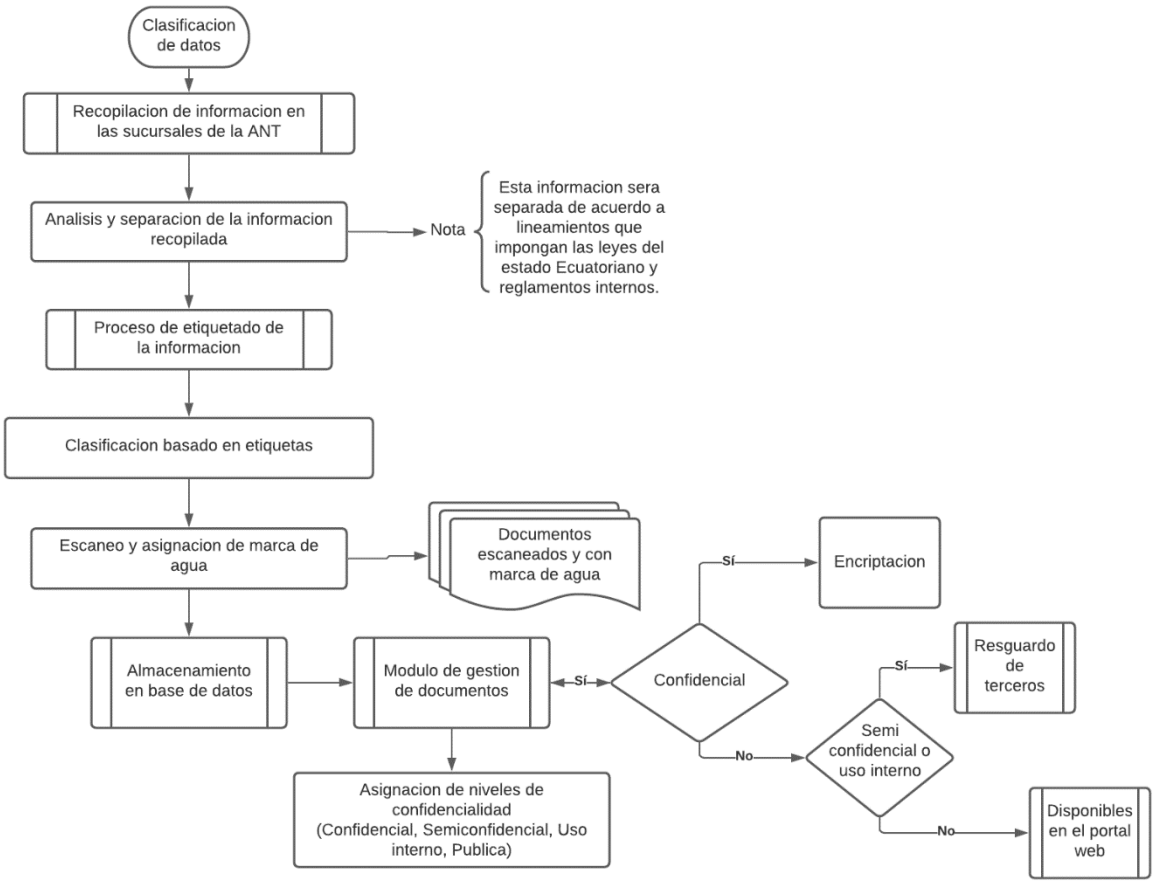
Regla 4: Establecer un protocolo de manejo de información: en el caso de información que tengan una etiqueta confidencial dicha información será cifrada en base a herramientas de Ciberseguridad, en el caso de información semiconfidencial y de uso interno será manejada mediante resguardo de un tercer colaborador, y en los casos de información pública esta puede estar disponible en los portales web de la Organización.

4. Desarrollar un estándar de clasificación de datos: deberá detallar la implementación de la política en situaciones específicas. (2 puntos)

Hace referencia a cómo será aplicada la regla de una política de una manera detallada en este caso elegimos la regla número 4 de la política presentada en la pregunta anterior:

Como ya está especificado en la regla toda información sensible estará cifrada en base a herramientas que dispone los lenguajes de programación en los que están desarrollados los sistemas de la organización, dicho cifrado es aplicado a documentos y como a la información que se encuentra en bases de datos. En los casos que sea necesario enviar determinada información por la red de internet se aplicaran técnicas de cifrado, si se desea enviar información de nivel confidencial el actor que recibe la información por medio de internet deberá contar con una clave de descifrado dicha clave será obtenida por medio de un canal seguro, con ello una vez que el actor obtenga la información por el canal inseguro (internet) no tendrá problema en interpretar la información que se transportó de manera cifrada. La clave de cifrado deberá ser actualizada después de un mes.

5. Desarrollar procedimientos y flujo de procesos de clasificación de datos: realizar un diagrama de flujo que permita interpretar cómo se realiza el proceso de clasificación. (3 puntos)



6. Desarrollar herramientas que apoyen el proceso: generar al menos una plantilla para facilitar el proceso de recolección de datos. (3 puntos)

AGENCIA NACIONAL DE TRANSITO						
Plantilla de regisro de documentacion e informacion de usuario						
Digitador:						
Cedula:				**Tipo de Sangre:**		
Nombres:				**Lentes:**	SI	NO
Apellidos:						
Fecha de Nacimiento:				**Dispositvos auditivos:**	SI	NO
Sexo:	M|	F|				
Direccion:				**Correo electronico**		
Tipo de tramite:						
Departamento Encargado:	Licencias Nuevas y Renovaciones					
Fecha de solicitud:						
Escuela de conduccion						
Nª Certificado de Aprobacion:						
Documentos anexos						
Recibos de pagos	SI|	NO|		**Copia Cedula**	SI|	NO|
	Codigo:				Codigo:	
Certificado de escuela de conduccion	SI|	NO|		**Examenes medicos**	SI|	NO|
	Codigo:				Codigo:	
Certificado de tipo de sangre	SI|	NO|				
	Codigo:					

7. Identificar a los propietarios de la aplicación: describir los sistemas o tecnologías con los que cuenta su empresa e identificar a los propietarios (pueden ser roles como gerente general, encuestadores, técnicos de datos, etc.) (3 puntos)

- **Sistema de registro de datos licencias**, Este sistema será en donde los empleados de cada agencia harán el registro de la información de los usuarios y el registro de documentos físicos de acuerdo a un código único.
- **Sistema de registro de datos matriculas**, Este sistema usaran cada cantón o centro de matriculación vehicular.
- **Sistema de gestión de nivel de confidencialidad**, Este sistema tendrá un panel de toda la información receptada por los empleados de cada agencia, de acuerdo al código de asignación de cada documento el sistema automáticamente le asigna un nivel de confidencialidad. Sin embargo, el administrador puede cambiarlo de ser necesario.
- **Sistema de bases de datos**, dentro de este sistema se encuentra toda la información registrada del sistema de la Agencia Nacional de Transito, tiene accesos controlados por roles.
- **Sistema de gestión de procesos**, Este sistema es el utilizado por los funcionarios para realizar procesos como habilitaciones, importaciones, casos apartados, etc.
- **Portal web**, es el sistema que está destinado al público, únicamente presentara información que no sea confidencial ni de uso interno.

SISTEMA	Propietario
Registro de licencias	Departamento (Encargado) del registro y control de licencias
Registro de matriculas	Departamento (Encargado) del registro y gestión de matriculación vehicular
Gestión de nivel de confidencialidad	Departamento de la seguridad de la información de la agencia
Gestión de procesos ANT	Funcionarios o digitadores de las sucursales de la ANT
Bases de datos	Departamento de tics, de acuerdo a sus roles
Portal web	Usuarios en general

8. Identificar a los propietarios de los datos y sus delegados: deben estar en base a los sistemas o tecnologías identificadas en el paso previo. (3 puntos)

Tipo de información	Sistema	Propietario	Delegado
Información de usuario y licencias	Registro de licencias	Gerente de ANT	• Encargado del registro y control de licencias. • Recepcionistas de las sucursales de la ANT
Información de usuarios y vehículos	Sistema de matriculas	Gerente de la ANT	• Encargado del departamento de control de matriculación vehicular • Digitadores de cada cantón que matricule vehículos
Documentos digitalizados con un nivel de confidencialidad asignado	Gestión de nivel de confidencialidad	Director de seguridad de la información	• Delegado del departamento de Tics
Información de toda la ANT	Sistemas de bases de datos	Gerente de la ANT	• Departamento de Tics • Técnicos de seguridad informática.
Información de clasificación publica como datos de multas, información de vehículos, etc.	Portal web de la ANT	Departamento de Tics	

9. Distribuir las plantillas estándar: detallar cómo se realizará la distribución de dichas plantillas. (1 punto)

1. Cada empleado de la ANT tiene un rol asignado, con ello se puede identificar qué nivel de acceso tienen dentro del sistema de información.
2. Al tener todo dentro de un sistema informático, la asignación de roles se hace con un usuario y contraseña, con un nivel de seguridad alto como un proceso de doble verificación.
3. Las plantillas estándar se distribuirán dentro del sistema informático, de acuerdo a cada departamento y sus usuarios. Es decir, el formulario de registro de matriculación vehicular estará disponible únicamente para los centros de revisión vehicular autorizados, y dentro de este cada empleado tendrá un usuario y contraseña que al ingresar al sistema tendrá acceso a su formulario designado únicamente.
4. Para el control de asignaciones se llevará una auditoria semestral para verificar la correcta asignación de las plantillas.

10. Clasificar la información y las aplicaciones: detallar los niveles definidos y las características que deben tener los datos de cada nivel. Para diseñar esta clasificación pueden encontrar información adicional en el documento (2 puntos)

NIVEL	CRITERIOS
Bajo	Información de carácter público, accesible a cualquier persona dentro del portal web. Datos públicos de una persona, citaciones, multas, información general de la organización, información para procesos comunes como consulta de puntos, renovaciones, matriculas, etc. Si se compromete esta información no es mucha perdida, los servicios al público son los afectados pero la organización seguiría funcionando internamente
Moderado	Información de uso interno y accesible solo para el usuario propietario y el funcionario encargado, información como datos para procesos personales, habilitaciones de vehículos, chatarrización o procesos específicos. Si esta información se compromete las consecuencias podrían ser de perdida de funciones internas, generando costes económicos, pérdida de recursos humanos al no tenerlos en trabajo, afectaría a la parte financiera y la credibilidad de la organización.
Alto	Información confidencial, como las finanzas de la organización, además de los enfoques de negocios, información delicada de los usuarios, información como claves y contraseñar de los usuarios del sistema, si esta información y sistemas son comprometidos pueden afectar gravemente a la organización y dejarla sin funcionar, afectando económicamente, públicamente y con posibles demandas.

Clasificación de la información y las aplicaciones		
Nivel	**Información**	**Aplicación**
Bajo	- Noticias de la organización - Datos de la licencia - Datos de la matricula - Multas pendientes - Datos de propietario de un vehículo	- Portal web Sistemas de turnos y tramites de licencias
Moderado	- Datos de solicitud de licencias nuevas y renovaciones - Datos de matriculación vehicular - Datos de procesos de la ANT como habilitaciones de vehículos importaciones, etc. - Datos de funcionarios de la ANT	- Sistema de registro de licencias - Sistema de registro de matriculas - Sistema de gestión de procesos ANT Sistema de certificados
Alto	- Finanzas de la ANT - Organización interna de la ANT - Documentos oficiales - Datos de los usuarios de los sistemas (usuarios y contraseñas) - Bases de datos - Datos de multas	- Bases de datos - Gestión de confidencialidad

11. Desarrollar procesos de auditoría: establecer cada cuánto tiempo se deberá realizar los procesos de auditorías y el tipo de auditoría que se realizará. Justificar la respuesta. (2 puntos)

Tomando en cuenta que existen dos tipos de auditoría interna y externa cada una cuenta con aciertos y desventajas, al realizar una auditoría interna un empleado de la empresa lleva a cabo tal proceso por lo tanto se corre el riesgo de que el auditor tenga afinidad con determinado personal y que no realice correctamente los procesos la ventaja de este tipo de auditoria es que se conoce completamente los procesos de la empresa, por otra parte, al realizar una auditoría externa un auditor ajeno a la empresa se encarga en realizar los procesos lo cual la afinidad con el personal no existe y se los evalúa correctamente y la desventaja es que como es un auditor ajeno no conoce el giro del negocio y el proceso llevara más tiempo.

El tipo de auditoría que se deberá aplicar en este caso sería una auditoría interna donde los procesos deberían realizarse al menos una vez por 6 meses, con el objetivo de conocer que datos que esta maneja pueden estar en alta amenaza o indebidamente protegidos, esto con el fin de verificar que toda la información y que sus procesos no se encuentren afectados además de conocer que medidas de seguridad se necesita mejorar o implementar para protegerlas.

12. Almacenar información en un repositorio central: detallar la ubicación física del repositorio y por qué se escogió dicha ubicación. (1 punto)

El repositorio contara con una estructura similar a los data center donde accederá mediante la red de alta velocidad en la cual todos los usuarios que tengan acceso a ella sean mediante autenticación

Las características que debe ofrecer el repositorio seran:

- Obtener un mejor rendimiento y seguridad en el uso de datos.
- Gran escalabilidad y la posibilidad de reducir costos en infraestructura.
- Los datos pueden ser muy accesibles.
- Aumento de la seguridad de la información.

La ubicación física donde será ubicado el repositorio será el sector cebollar en la ciudad de cuenca, se escoge este lugar porque cuenta con una ubicación geográfica idónea ya las condiciones del sector impiden que existan inundaciones y fallas geológicas.

13. Entrenar a los usuarios: describir brevemente cómo se planea entrenar a los usuarios. (1 punto)

En este caso para entrenar a los usuarios de la manera más eficiente se aplicaría un taller de fomento donde cada uno recibiría dependiendo de su rol en la institución una guía de usuario y además de capacitación con personas expertas para que así logren desenvolverse de la manera más correcta en su trabajo.

14. Revisar y actualizar periódicamente las clasificaciones de datos: detallar quién o quiénes podrán actualizar las clasificaciones de datos y cómo será el proceso. (2 puntos)

Para realizar las actualizaciones de datos existirán diferentes maneras:

1. Que el usuario actualice sus datos voluntariamente realizando una petición a la institución mediante su plataforma web, donde el usuario entregue documentos válidos para la modificación de esta.
2. Que la institución cada cierto tiempo pida al usuario verificar si su información este debidamente almacenada y que si necesita o no una actualización de esta.

• Seleccionar un estándar de seguridad de la información, que aplicaría para proteger adecuadamente los activos de información de su institución como datos, software y hardware (puede ser un estándar de los revisados en clase o incluir uno nuevo). Debe justificar por qué seleccionó dicho estándar. (3 puntos)

El estándar de seguridad de la información utilizada es la ISO/IEC 27001, ya que esta es una norma internacional la cual permite la confidencialidad, el aseguramiento, la integridad de los datos y de la información, además de los sistemas los cuales la procesan (Figueroa-Suárez,2018).

Aplicar este estándar significa sobresalir respecto a las demás ya que esta mejora los rasgos competitivos y la imagen de una institución, también permite a los procesos de seguridad estar equilibrados y se coordinen entre sí, además de esto permite la reducción de costos gracias a que se emplea con mayor eficiencia, permitiendo así un mayor seguimiento a los controles de seguridad.

• Tomando en cuenta el ataque informático que ha ocurrido en la ANT y que usted es el OSI. ¿Qué medidas aplicaría para proteger a los propietarios de los datos ante cualquier riesgo de seguridad de la información? Mencione al menos 4 medidas diferentes, indicando cómo las ejecutaría, cuándo las ejecutaría (el mismo día de la filtración, por el lapso de un mes posterior a la filtración, etc.) y por qué las considera oportunas. (4 puntos)

Para proteger la información de los usuarios tomaría las siguientes medidas:

1. Como la institución sufrió un ataque a su sistema, lo primero que se realizaría es el cambio de contraseñas actualizándolas con contraseñas robustas, es decir, con caracteres aleatorios los cuales deben incluir símbolos, letras mayúsculas y minúsculas para lograr una mayor complejidad.
2. Controlar el acceso a los datos más estrictos, esto con el fin de limitar el acceso a la información ya que cuantas menos personas accedan a esta menor será el riego de comprometerla. Por lo que se debería implementar en la institución un sistema el cual impida dar acceso a datos personales e importantes a cualquier usuario.
3. Si la información fue comprometida y alterada se debería realizar una recuperación con las copias de seguridad para así poder evitar la pérdida de estas y permitiendo preservar la información que se vio afectada.
4. Contratar software integral de seguridad, esto con el fin de proteger a la institución contratando paquetes de seguridad los cuales contengan antivirus, anti-espías, antimalware, firewall, etc. La cual permita proteger la información ante otro posible ataque.
5. Monitorización continua y respuesta inmediata, esto con el fin de monitorizar como se está gestionando los datos y detectar si existen posibles fallos o gestión incorrecta. Este sistema ayudara a actuar de manera inmediata para resolver cualquier incidencia y minimizar posibles repercusiones.

Todas estas medidas se deberían cumplir con la brevedad posible para evitar cualquier tipo de filtración o alteración de los datos lo cual es lo más importante en la actualidad.

Referencias Bibliográficas.

Ecuador, & Asamblea Constituyente. (2008). *CONSTITUCIÓN DE LA REPUBLICA DEL ECUADOR*.

Ecuador, & Ley de Comercio Electrónico. (2002). LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS. *Leyes Relativas a La PI Adopt. Por El Pod. Legis*, 1–19.

el Pleno. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. 22–22.

el Pleno. (2015). *LEY ORGÁNICA DE TELECOMUNICACIONES*.

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. Polo del conocimiento, 2(12), 145-155.