UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y MECÁNICA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Informe N°1 - Tercer Parcial:

"Métricas"

DOCENTE: ROXANA LISETTE QUINTANILLA PORTUGAL

ALUMNOS:

- Cordova Castro, Marko Leugim 160890
- Guevara Ferro Cristian Luis 171061
- Luna Ccasani, Charlie Joel 161368
- Mallqui Apaza, Nadiabeth Diana 171063
- Quispe Leon,Widmar Raul 171259
- Rojas Cahuana Etson Ronaldao 124821
- Sullca Peralta, Melanie Indira 171070
- Rodriguez Hancco, Rudy Rodrigo 171068

CUSCO – PERÚ
2021

TABLA 1. RELACIÓN ENTRE EL OBJETIVO DE SEGURIDAD DEL SOFTWARE, LAS CLÁUSULAS ISO/IEC 17799:2005 Y LOS REQUISITOS DE SEGURIDAD.

Software **Objetivo de seguridad**	**ISO / IEC** **17799: cláusulas 2005** **para el control**	**Requisito de seguridad.**
Confidencialidad Autenticidad	Control de acceso (A.11) Hombre de acceso de usuario.(A.11.2) Resolución de usuario (A.11.3) Control de acceso a aplicaciones e información (A.11.6)	Identificación,autenticación y autorización requeridas. Privacidad Requisitos
Confidencialidad Integridad Autenticidad	Requisito de seguridad. de IS (A.12.1) Procesamiento correcto en la aplicación (A.12.2) Controles criptográficos (A.12.3) Seguridad de los archivos del sistema (A.12.4) Servicios de comercio electrónico (A.10.9)	Requerimiento de identificación, autenticación y autorización. Requisitos de privacidad Requisito de Integridad. Requerimiento de Servicio disponible.
Monitor No repudio	Protección contra código móvil y malicioso (A.10.4) Seguimiento. (A.10.10) Informe de debilidad de eventos de S.I. (A.13.1) Gestión de incidentes y mejoras de S.I. (A.13.2) Cumplimiento de los requisitos legales (A.15.1)	Requisitos de detección de actividades maliciosas. Requisitos de auditoría de seguridad. Requisitos de no repudio.
Disponibilidad	Copia de seguridad (A.10.5)	Requiere copia de seguridad y recuperación. Requiere disponibilidad del servicio.

TABLA 2. MÉTRICAS PARA REQUISITOS DE IDENTIFICACIÓN, AUTENTICACIÓN Y AUTORIZACIÓN

G1=SR1 Objetivo Asunto Punto de vista	Garantizar Identificación, autenticación y autorización Usuario, organización	1 : cumplimiento total 0.5 : cumplimiento promedio 0 : cumplimiento débil
Preguntas (Q) = SR1.Q	**Métricas(M) = SR1.M**	**Puntaje**
¿Cómo se identifican los usuarios?	Evaluación subjetiva por parte del usuario de todos los niveles identificado de manera única para usar el sistema	1 (cumplimiento total por identificación y nombre de usuario)
¿Como son los usuarios identificando?	Nombre, contraseña, token, ID, biométrico (huella dactilar, voz)	1 (Cumplimiento total de acceso con token)
¿Cómo se gestiona la sesión de usuarios?	Tiempo máximo por autenticación, tiempo máximo que la sesión continúa sin interacción activa del usuario.	0.5 (Cumplimiento promedio con el tiempo de sesión, se tiene 30 minutos de acceso no continua de interacción)
¿No ha fallado el intento de bloquear la cuenta de usuario?	Total de intentos fallidos de inicio de sesión para un usuario específico.	0 (Cumplimiento débil, no tiene actualmente)
¿Cómo otorgar autorización al usuario?	Personal o basado en roles o grupo con principio de privilegio mínimo u otros medios	1 (Cumplimiento total, cada usuario que es autorizado tiene un rol específico)
¿Cuántos recursos y nivel de uso se otorgan para un solo usuario?	Sin acceso a recursos y nivel de uso como perfil de acceso para cada usuario	1 (Cumplimiento total, cada usuario tiene niveles de accesos según los roles)
¿Cuántas capas de verificación de autenticación / autorización?	No de autenticación / autorización check por uso.	1 (Cumplimiento total, se realiza una comprobación de acceso con el rol y token)
Puntaje total = 100 * (1+1+ 0.5+0+1+1+1) / 7 = 78.57%		Por lo tanto, los requisitos de identificación, autenticación y autorización pueden alcanzar el 78.57% de cumplimiento en el sistema.

TABLA 3. MÉTRICAS PARA LOS REQUISITOS DE INTEGRIDAD

G2=SR2 Objetivo Asunto Punto de vista	Mejorar y garantizar Integridad Parte interesada, usuario, organización	1 : cumplimiento total 0.5 : cumplimiento promedio 0 : cumplimiento débil
Preguntas (Q) = SR2.Q	**Métricas(M) = SR2.M**	**Puntaje**
¿Cuántas comprobaciones de validación para un conjunto de entrada?	Número de comprobaciones de validación (V) por cada entrada total del usuario (Tu) o entrada total de fuentes externas (Tes) para un propósito específico (aplicación o interfaz). Una relación mayor de V/Tu o V/Tes proporciona una validación fuerte	0.5 (cumplimiento promedio de comprobación de la cuenta)
¿Cuántos puntos específicos toma el módulo para validar la entrada?	Número de puntos (Pi) del módulo de entrada, número de puntos del módulo de validación (Pv). La relación Pv/Pi =1 indica que todos los puntos de entrada tienen al menos un control de validación.	0.5 (cumplimiento promedio de validación mediante una cuenta que posee correo electrónico y contraseña, se verifica que la cuenta exista en la base de datos)
¿Cómo el programa de aplicación asegura la integridad?	Subjetivo, garantizar una aplicación inmune a fallos de funcionamiento	1 (cumplimiento total a fallos, si existe algún fallo el sistema no se detendrá)
¿Cómo se gestiona la comprobación de errores y las excepciones durante el funcionamiento normal?	Subjetivo, basado en las técnicas de comprobación de errores y gestión de excepciones, características del lenguaje de programación, número total de llamadas a funciones que no comprueban el valor de retorno para un módulo específico	0.5 (cumplimiento promedio, el sistema no se detiene si existiera algún fallo)
¿Cuáles son las cifras de clase crítica o módulo que procesan datos?	El número total de clases o módulos, determina su ubicación donde se almacenan, su responsabilidad en la	1 (cumplimiento total, poca cantidad de clases críticas)

	modificación de datos críticos o que ofrecen una funcionalidad crítica, su valor en el software como activo, la probabilidad de ser objetivo de un ataque	
¿Cómo se manejan las condiciones de carrera cuando más de un usuario intenta al mismo tiempo utilizar los datos compartidos?	Evaluación subjetiva mediante técnicas apropiadas para asegurar la sincronización.	0.5 (cumplimiento promedio permite a una cantidad limitada el uso del sistema al mismo tiempo)
Puntaje total = 100 * (1+1+1+0.5+1+0.5) / 6 = 66.66%		Por lo tanto, los requisitos de integridad pueden alcanzar el 66.66% de cumplimiento en el sistema.

TABLA 4. MÉTRICAS PARA LOS REQUISITOS DE PRIVACIDAD

G3 = SR3 Propósito asunto punto de vista relacionado con	Privacidad Usuario, organización, proveedor legal, identificación, no repudio	1 : cumplimiento total 0.5 : cumplimiento promedio 0 : cumplimiento débil
Question(Q)=SR3.Q	**Metrics(M)=SR3.M**	**Puntaje**
¿Qué tan seguro es la transmisión de datos?	Algoritmo criptográfico, algoritmo para generar clave, longitud de clave.	1 (Cumplimiento completo, se utiliza una librería criptográfica)
¿Qué tan fuerte es la contraseña de usuario?	Longitud de la contraseña, combinación mínima de letras, números y otros caracteres, restricción de palabras comunes para la selección de contraseña, duración de la contraseña.	0.5 (Cumplimiento promedio, el usuario tiene la libertad de elegir el tamaño de la contraseña sin restricción)
¿Cómo se almacenan las contraseñas?	Cifrado, código hash, texto sin formato.	0.5 (Cumplimiento promedio, la contraseña es almacenada como un texto plano con formato)
¿Cómo se clasifican los datos?	En función de su valor, ubicación donde se almacena, valor por cualquier brecha de	0.5 (Cumplimiento promedio, los datos están almacenados en la misma estructura de la base de

	seguridad, etc. clasificado como sensible, confidencial, público.	datos relacional)
¿Cómo se manejan, almacenan y acceden los datos críticos?	Mediante aplicación o por otros medios, ubicación con texto cifrado o sin formato para almacenar, mecanismo de control de acceso adecuado.	1 (Cumplimiento total, se tienen gestores de acceso a datos con implementación segura)
¿Qué tan importante es el almacenamiento y el acceso del módulo?	Ubicación donde se almacena y técnica de control de acceso.	1 (Cumplimiento total, se tienen bien definidos las técnicas de acceso)
¿Algún dato requiere el cumplimiento de algún requisito legal?	Sí o no y evaluación subjetiva de cómo se realiza el cumplimiento.	1 (Cumplimiento total, los datos ya cumplen con el requisito legal de legitimidad)
¿Qué número aleatorio se considera para claves criptográficas o para otros fines?	Fuente de números aleatorios, tamaño de semilla y entropía por número de bits.	1 (Cumplimiento total, se tiene métricas fiables con la libreria bcrypt)
Puntaje total = 100 * (1+0.5+0.5+ 0.5+1+1+1+1) / 8 = 81.25%		Por lo tanto, los requisitos de privacidad pueden alcanzar el 81.25% de cumplimiento en el sistema.

TABLA 5. MÉTRICAS PARA LOS REQUISITOS DE DISPONIBILIDAD DEL SERVICIO

G4=SR4 Objetivo tema punto de vista relacionar con	Garantizar la disponibilidad del servicio Partes interesadas, usuarios copia de seguridad y recuperación	1 : cumplimiento total 0.5 : cumplimiento promedio 0 : cumplimiento débil
Preguntas (Q) = SR4.Q	**Métricas(M) = SR4.M**	**Puntaje**
¿Cuánto tiempo estará disponible un servicio específico para su funcionamiento normal?	Porcentaje de tiempo (Ta) de los servicios por software disponibles durante un periodo de tiempo determinado (Tt). Ta/Tt =1 implica que el servicio está disponible durante todo el periodo determinado.	1 (cumplimiento total, los servicios estarán disponibles durante todo el tiempo que se determinó)

¿Qué tan rápido puede recuperarse un servicio específico?	Diferencia entre el tiempo de recuperación (Tr) y el tiempo de fallo (Tf). Un valor pequeño de (Tr-Tf) dan más impresión de disponibilidad	0.5 (cumplimiento promedio de recuperación de un servicio específico, si ocurriera un fallo)
¿Identificar el posible punto de un fallo del servicio?	Calcular el punto total mediante parámetros como el número de dependencias con otras funcionalidades internas o externas, la dependencia del hardware, etc.	0.5 (cumplimiento promedio al identificar la causa del fallo)
¿Cómo interactúan los servicios críticos entre sí y mantienen una relación de confianza?	Evaluación subjetiva por métodos de interacción y relación de confianza entre los servicios.	0.5 (cumplimiento promedio, existe relación de confianza entre los servicios críticos)
Puntaje total = 100 * (1+0.5+0.5+0.5) / 4 = 62.5%		Por lo tanto, los requisitos de disponibilidad del servicio pueden alcanzar el 62.5% de cumplimiento en el sistema.

TABLA 6. MÉTRICAS PARA REQUISITOS DE NO REPUDIACIÓN

G5 = SR5 Propósito asunto punto de vista	Garantizar no repudio Interesado, usuario	1 : cumplimiento total 0.5 : cumplimiento promedio 0 : cumplimiento débil
Question(Q)=SR5.Q	**Metrics(M)=SR5.M**	**Puntaje**
¿Qué atributos se consideran como prueba de transacción y cómo se almacena?	Fecha, hora, autenticar la identidad de las partes que interactúan, almacenamiento de información o datos, reconocimiento relevante, almacenamiento automático por software como registro o archivo normal.	1 (Cumplimiento total, las operaciones guardan las fechas para las citas y registros en conjunto con el rol determinado)
¿Cómo se puede acceder al archivo de registro?	Técnica de control de acceso adecuada.	0.5 (Cumplimiento parcial, se tiene una lista de todas las citas de un tutor y estudiante, donde se reportan al coordinador o para determinado usuario)

¿Cómo comprobar todas las entradas de interacción en el registro?	Proporción entre el no de entrada en log (Ne) y el no de interacción (Ni). Ne / Ni = 1 significa toda la entrada de interacción en el registro	0.5 (Cumplimiento parcial, se tienen todas las entradas, pero aún no se tiene interacción con el registro)
Puntaje total = 100 * (1+0.5+0.5) / 3 = 66.66%		Por lo tanto, los requisitos de no repudio pueden alcanzar el 66.66% de cumplimiento en el sistema.

TABLA 7. MÉTRICAS PARA LOS REQUISITOS DE DETECCIÓN DE ACTIVIDADES MALICIOSAS

G6=SR6 Objetivo tema punto de vista relacionado con	Detectar Actividades maliciosas Organización Identificación, autenticación y autorización	1 : cumplimiento total 0.5 : cumplimiento promedio 0 : cumplimiento débil
Preguntas (Q) = SR6.Q	**Métricas(M) = SR6.M**	**Puntaje**
¿Cuáles son los contenidos del registro de seguimiento de auditoría?	Cada intento fallido de autenticación, modificación de autorización o de otras acciones ilegales hora, fecha	0.5 (cumplimiento promedio, informa las acciones fallidas o ilegales pero falta del registro de seguimiento)
¿Cuánto tiempo se tarda en informar después de cualquier violación de la seguridad?	Diferencia de tiempo entre el informe de la violación de la seguridad (Tsvr) y la violación ocurrida (Tsvo), es preferible un valor pequeño de Tsvr-Tsvo	0.5 (cumplimiento promedio, el sistema informa al usuario que no tiene las credenciales para determinada actividad)
¿Cómo se cuentan los intentos de inicio de sesión fallidos?	Número de intentos totales de inicio de sesión (Na)-Número de intentos totales de inicio de sesión con éxito (Ns) para un período de tiempo específico.	0 (cumplimiento débil, falta la implementación de conteo de intentos de inicio de sesión fallidos)
¿Cómo se detectan, denuncian y detienen los virus, gusanos u otros códigos maliciosos?	Evaluación subjetiva mediante técnicas de manejo de código malicioso.	0 (cumplimiento débil, falta la detección de virus, códigos maliciosos, etc)

Puntaje total = 100 * (0.5+0.5+0+0) / 4 = 25%	Por lo tanto, los requisitos de detección de actividades maliciosas pueden alcanzar el 25% de cumplimiento en el sistema.

TABLA 8. MÉTRICAS PARA REQUISITOS DE AUDITORÍA DE SEGURIDAD

G7 = SR7 Propósito Asunto Punto de vista Relacionado con	Mejorar. Auditoría de seguridad. Interesado, organización. Requisitos de seguridad, política, objetivo.	1 : cumplimiento total 0.5 : cumplimiento parcial 0 : cumplimiento débil
Question(Q)=SR7.Q	**Metrics(M)=SR7.M**	**Puntaje**
¿Todos los mecanismos de seguridad funcionan, se actualizan correctamente y son compatibles con las políticas y el objetivo de seguridad requeridos?	Sí o no, evaluación subjetiva si es necesario y tiempo de duración para generar el informe.	0.5 (Cumplimiento parcial desde el punto de vista en un producto mínimo viable se cumple con las expectativas de políticas de seguridad, no se tiene un examen formal)
Puntaje total = 50.00%		Por lo tanto, los requisitos de auditoría de seguridad pueden alcanzar el 50.00% de cumplimiento en el sistema.

TABLA 9. MÉTRICAS PARA LOS REQUISITOS DE COPIA DE SEGURIDAD Y RECUPERACIÓN

G8=SR8 Objetivo tema punto de vista	Asegurar copia de seguridad y recuperación organización disponibilidad	1 : cumplimiento total 0.5 : cumplimiento promedio 0 : cumplimiento débil
Preguntas (Q) = SR8.Q	**Métricas(M) = SR8.M**	**Puntaje**
¿Con qué frecuencia se realizan copias de seguridad de datos críticos,	Mida la frecuencia de las copias de seguridad por día, por semana o por tiempo	0 (cumplimiento débil, las copias de seguridad se

registros y pistas de auditoría?	específico y técnicas para hacer la copia de seguridad.	realizan de manera manual así que es relativo)
¿Cómo se almacenan, autentifican, localizan y conservan las copias de seguridad?	Texto plano o encriptado, control de acceso para la copia de seguridad, ubicación donde se almacena, cantidad de tiempo de retención de la copia de seguridad	0.5 (cumplimiento promedio, se almacena en la nube en una plataforma online)
¿Cuánto tiempo se tarda en recuperar la copia de seguridad y los requisitos legales para cumplimiento?	Tiempo de recuperación de la copia de seguridad	1 (cumplimiento total, se recupera en un tiempo corto)
Puntaje total = 100 * (0+0.5+1) / 3 = 50%		Por lo tanto, los requisitos de copia de seguridad y recuperación pueden alcanzar el 50% de cumplimiento en el sistema.

RESULTADOS

La medición de la calidad es, en general, un tema difícil, aunque importante. Incluso para la seguridad del atributo de calidad difícil de comprender, es importante poder medir el nivel de seguridad e identificar los puntos débiles en la implementación de la seguridad. Solo con medidas es posible tomar decisiones de gestión de proyectos sobre una base bien fundamentada.

Se utilizó un conjunto de requisitos de seguridad derivados del objetivo de seguridad del software y la norma ISO / IEC 17799: 2005 aceptada para la seguridad de la información como base para desarrollar dichas métricas de seguridad. Es obvio que no puede haber una sola medida de seguridad, ya que es un concepto multifacético. Definimos un conjunto de medidas que abarcan estas distintas facetas. Permite relacionar claramente las medidas definidas con los objetivos de seguridad originales. Esto proporciona una base bien fundada para nuestras métricas de seguridad.

RESUMEN DE MÉTRICAS

RELACIÓN ENTRE EL OBJETIVO DE SEGURIDAD DEL SOFTWARE, LAS CLÁUSULAS ISO/IEC 17799:2005 Y LOS REQUISITOS DE SEGURIDAD	RESULTADOS
MÉTRICAS PARA REQUISITOS DE IDENTIFICACIÓN, AUTENTICACIÓN Y AUTORIZACIÓN	78.57 %
MÉTRICAS PARA LOS REQUISITOS DE INTEGRIDAD	66.66 %
MÉTRICAS PARA LOS REQUISITOS DE PRIVACIDAD	81.25 %
MÉTRICAS PARA LOS REQUISITOS DE DISPONIBILIDAD DEL SERVICIO	62.50 %
MÉTRICAS PARA REQUISITOS DE NO REPUDIACIÓN	66.66 %
MÉTRICAS PARA LOS REQUISITOS DE DETECCIÓN DE ACTIVIDADES MALICIOSAS	25.00 %
MÉTRICAS PARA REQUISITOS DE AUDITORÍA DE SEGURIDAD	50.00 %
MÉTRICAS PARA LOS REQUISITOS DE COPIA DE SEGURIDAD Y RECUPERACIÓN	50.00 %
PROMEDIO FINAL	60.08 %

BIBLIOGRAFÍA

- **ISO 27001: The 14 control sets of Annex A explained,** https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained
- **Measuring Security Requirements for Software Security,** https://www.researchgate.net/profile/Paolo-Falcarin/publication/238594490_Measuring_security_requirements_for_software_security/links/00b4952fff9cbf3ca2000000/Measuring-security-requirements-for-software-security.pdf