Bases fundamentales para la ciberseguridad en un startup

Jean Michael Wong Díaz
Guía: Roque Hernández

Presentado como parte de los requisitos para el Título de Magíster en Ciberseguridad. CES: RPC-SE-01-N°.014-2020. Cohort2 2022 - 2023.
Correo electrónico del autor: jean.wong.diaz@gmail.com Guayaquil, 3 de abril de 2023.

Bases fundamentales para la ciberseguridad en un startup

Introducción

Este documento describe como la maestría de Ciberseguridad en la Universidad Casa Grande ha ayudado, a identificar los cimientos o bases principales en términos de Ciberseguridad y Seguridad de la Información a implementar dentro de un startup, desde el uso de las buenas prácticas, hasta los diferentes métodos para proteger información valiosa.

En el transcurso de la maestría, las materias de esta, ayudaron a mejorar procesos en el previo lugar de trabajo del autor, tales como la implementación de la certificación de la Norma ISO 27001 – 2013. La Norma Internacional de Organización para la Estandarización (ISO) publicó en el año 2013 la norma ISO/IEC 27001, la cual establece los requisitos para un sistema de gestión de seguridad de la información (ISO, 2013). Adicionalmente se mejoró la protección de las bases de datos de un aplicativo web que manejaba información sensible de sus clientes.

El giro de negocio de la empresa actual del maestrante, la cual es considerada como un startup, por su tamaño y tiempo, se basa en un aplicativo web y móvil, los cuales tienen la función de directorio de servicios masivos, en donde usuarios con perfiles de negocio, profesionales e independientes pueden registrarse, reclamar su perfil y empezar a transaccionar sus servicios. Bajo este contexto, en donde al autor debe cumplir los roles de "jefe de Ciberseguridad y "desarrollador tecnológico", se han identificado oportunidades de implementación las cuales, gracias a materias específicas dentro de la maestría de Ciberseguridad, han aportado contenido de valor para poder realizar una propuesta de proyecto que formalice las bases de ciberseguridad y seguridad de la información en dicho startup.

Una de las principales materias identificadas es "Seguridad de Aplicaciones y Bases de Datos", debido a que el aplicativo web previamente mencionado, se encuentra en constante

evolución y por ende se necesita un desarrollo continuo, el cual es realizado por un equipo interno, en paralelo con el desarrollo de su versión móvil, por lo que se considera necesaria la implementación de un "Framework de Desarrollo de Software Seguro". Uno de los objetivos principales es implementar de manera eficiente los requerimientos solicitados por los diferentes departamentos dentro de la empresa, detallando un "Ciclo de Vida de Desarrollo de Software" (SDLC por sus siglas en inglés), el cual permite según la publicación de NIST 800-218, establecer ya sea una metodología formal o informal para el diseño, creación y mantenimiento de software e incluso a nivel de hardware, existen varios modelos de desarrollo para SDLCs, como los pueden ser waterfall, spiral, agile; en particular metodologías agile combinadas con software de desarrollo y operaciones de TI, llamadas prácticas DevOps (Souppaya, Scarfone, & Dodson, 2022).

Otra de las asignaturas que destacan para ser consideradas dentro de la propuesta es "Estrategias y Políticas Multilaterales para la Ciberseguridad", materia que ha ayudado a reconocer el inicio del camino que se debe tomar en términos de la Seguridad de la Información, al identificar los riesgos que pueden afectar a cualquier empresa o proyecto. Una de las acciones a implementar es el SGSI, "El Sistema de Gestión de Seguridad de la Información es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional" (Ecuador, 2020). Esto llevado de la mano con aspectos tratados en la materia de "Gestión Económica y Auditorías en la Seguridad de la Información", identificando inversiones que prevengan potenciales pérdidas dentro de la empresa según el riesgo que representen.

Por último y no menos importante se seleccionó la materia de "Continuidad de Negocio", la cual potencia la importancia sobre los factores que integran un "Sistema de Gestión de Continuidad de Negocio".

> La capacidad de una empresa para gestionar eventos disruptivos se está volviendo fundamental para su supervivencia. La variedad de amenazas que pueden causar interrupciones comerciales es cada vez mayor. Desde ciberataques y pandemias globales hasta desastres naturales, una organización necesita un conjunto de herramientas para administrarse a sí misma en tiempos de incertidumbre (nqa., 2019).

Estas son las materias que nutren este ensayo, y forman parte de las bases que puede implementar una entidad la cual no ha formalizado un esquema de Ciberseguridad y Seguridad de la Información, abriendo paso a proyectos que mejoren diferentes aspectos en términos de calidad y seguridad en el transcurso del tiempo.

Desarrollo

Estos pilares, representados por las materias, "Seguridad de Aplicaciones y Bases de Datos", "Estrategias y Políticas Multilaterales", "Gestión Económica y Auditorías en la Seguridad de la Información", y "Continuidad de Negocio"; han brindado lineamientos que sirven como base para la implementación de medidas y controles de la Ciberseguridad y Seguridad de la Información en este startup, las cuales se materializan en forma de propuesta, que ayuda a formalizar y sistematizar la Ciberseguridad y Seguridad de la Información de este startup.

Seguridad de Aplicaciones y Bases de Datos

Esta materia transmitió la importancia que tienen los activos digitales, como los pueden ser servidores que alojen aplicativos o bases de datos, ya que, según el giro de negocio de cada empresa, puede ser el factor principal de dicha compañía. Dentro del startup del autor, se trabaja en el desarrollo de un aplicativo web y móvil, los cuales evolucionan acorde al plan de negocio que se dicte o se mantenga. En el transcurso de dicha materia, se explicó la importancia de

mantener un aplicativo que esté alineado a ciertos parámetros de seguridad, logrando esto con diferentes tipos de pruebas de penetración periódicas, ya sea a nivel de código fuente o mediante el uso del mismo, como lo son las pruebas de caja blanca, caja negra y caja gris.

White box testing o pruebas de caja blanca: El auditor involucrado debe conocer todas las tecnologías internas y subyacentes utilizadas por el entorno objetivo cuando realiza este tipo de prueba de penetración. Por lo tanto, abre una puerta para que un pentester vea y evalúe críticamente las vulnerabilidades de seguridad con el mínimo esfuerzo posible y la máxima precisión. Este proceso aporta más valor a la organización, en comparación con el enfoque de caja negra debido a que eliminará cualquier problema de seguridad interna que se encuentre en el entorno de la infraestructura de destino, lo que hace más difícil que un adversario malintencionado se infiltre desde el exterior (Castro, 2019).

Black box testing o pruebas de Caja negra: El auditor de seguridad evaluará la infraestructura de la red y no estará al tanto de ninguna tecnología interna implementada por la organización objetivo. Al emplear una serie de técnicas de hackers del mundo real y atravesar fases de pruebas organizadas, las vulnerabilidades pueden revelarse y potencialmente explotarse. Es importante que un pentester entienda, clasifique y priorice estas vulnerabilidades de acuerdo con su nivel de riesgo (bajo, medio o alto), el cual puede medirse según la amenaza impuesta por la vulnerabilidad en general (Castro, 2019).

Una auditoría de caja gris pone a prueba las habilidades del analista. La naturaleza de la prueba es la eficiencia; la amplitud y profundidad dependen de la calidad de la información proporcionada al Analista antes de la prueba, así como de su

> conocimiento aplicable. Este tipo de prueba a menudo se denomina prueba de vulnerabilidad y la mayoría de las veces es iniciada por el objetivo como una autoevaluación (Castro, 2019).

Adicionalmente, se implementaron talleres que reflejaban como es el desarrollo de estas pruebas de penetración con varias herramientas recomendadas como “SonarQube”, herramienta que permite realizar una prueba de penetración de tipo caja blanca, la cual permitió analizar el código fuente del aplicativo web, el cual el maestrante desarrolló en su anterior lugar de trabajo, mostrando un informe en el cual se enlistan las recomendaciones de seguridad en fragmentos específicos del código, así como los ataques y vulnerabilidades a los que se están expuestos.

No solamente se trataron temas de seguridad a nivel del código de software, también se dieron recomendaciones de un control de calidad en temas de desarrollo interno, tema el cual aporta un gran valor a la propuesta del maestrante, ya que, al mantener un equipo de desarrollo activo, es importante implementar una o varias metologías que se adapten de manera óptima a los requerimientos entrantes sobre el aplicativo web y móvil, estableciendo un Framework de Desarrollo Seguro, con un ciclo de vida del desarrollo, dando lugar a “Devops”, el cual es un conjunto de prácticas con la intención de reducir el tiempo entre realizar cambios en el sistema y efectuar estos cambios en un ambiente de producción de una manera en la que se asegure un alto control de calidad (Bass, Weber, & Zhu, 2015). De esta manera se logra un mejor manejo y control de los requerimientos solicitados, evitando bugs y vulnerabilidades dentro del código fuente, a su vez que se mantienen intactas las operaciones comerciales u operativas acorde al giro de negocio de la empresa, un factor crítico en este startup, ya que se cuenta con el equipo de operaciones – comercial, y sus requerimientos necesitan una atención rápida para una mayor captación de usuarios.

Estrategias y Políticas Multilaterales para la Ciberseguridad

La siguiente materia, se describe como un punto de encuentro con las demás, ya que enfatiza la importancia sobre la Seguridad de la Información, lo cual es el tema de partida en las demás materias, explicando la importancia de un Sistema de Gestión de Información (SGSI).

> Según Arlenys se entiende como información, todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, etc.), de su origen (propia o externa), o de la fecha de elaboración (Arlenys, 2017).
>
> La seguridad de la información, según ISO 27001 - 2013, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:
>
> - Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
> - Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
> - Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
>
> (Arlenys, 2017).

Se realizaron prácticas simulando entornos reales, donde las actividades realizadas ayudaron a identificar riesgos y probabilidades, estableciendo controles que los mitiguen, denotando la importancia de establecer un control "jerárquico" sobre las decisiones a tomar, esto bajo el término de "Comité de Seguridad de la Información", encajando perfectamente con el desarrollo de la propuesta del maestrante, ya que brinda los lineamientos acorde a la ISO 27001-2013 sobre cómo tratar la información tratada en los diferentes procesos.

Gestión Económica y Auditorías en la Seguridad de la Información

De la mano con la sección anterior (Estrategias y Políticas Multilaterales para la Ciberseguridad), esta materia denota la importancia de mantener y proyectar presupuestos para diferentes factores dentro de los riesgos de una empresa, ya que cada giro de negocio o institución en particular cuentan con diferentes ingresos y presupuesto a aplicar, en donde el objetivo es proyectar la menor pérdida financiera posible a consecuencia de potenciales riesgos, como lo pueden ser un secuestro de un servidor con la base de datos o accesos sensibles de la empresa, se priorizan las inversiones en contra de estas consecuencias como inversiones de prevención a mediano y largo plazo.

Similar a la materia de Estrategias y Políticas Multilaterales, se desarrollaron simulaciones materializadas en matrices de riesgos, plantilla que identifica potenciales riesgos sobre la empresa, estableciendo controles y procesos que mitiguen el nivel de impacto o consecuencia sobre la misma, con la diferencia en que se trataban a los riesgos proyectados en pérdidas financieras o ahorros a mediano o largo plazo, dando un enfoque más financiero al criterio sobre la Seguridad de la Información, ya que el presupuesto de las empresas nunca es infinito, estableciendo límites aceptables e incluso de pérdida.

Continuidad de Negocio

Esta materia ayudó a desarrollar partes de un Comité de Continuidad de Negocio, estructura la cual unifica diferentes elementos que mantienen la continuidad y operaciones de la empresa, aunque ésta haya sufrido algún tipo de incidente. Se identificó al personal que se adapta adecuadamente a los roles del Gobierno de Continuidad de Negocio, estableciendo las funciones a realizar en casos de emergencia. Adicionalmente se implementaron las matrices BIA Y RIA, matrices que ayudan a calcular el tiempo que una empresa puede detener sus operaciones tomando en cuenta las consecuencias en términos de finanzas, los últimos puntos de respaldo o retorno y el tiempo que se necesita para la recuperación de las operaciones en casos emergentes. Dichos factores demostraron la importancia de un Plan de Continuidad de Negocio. Según Oneto, "Un plan de continuidad de negocio es principalmente operativo y debe contemplar todas las medidas preventivas y acciones necesarias para mantener la operatividad de la organización a un nivel mínimo aceptable durante una contingencia" (Latina, 2020). De esta manera el maestrante identificó que otros elementos se necesitan implementar en su lugar de trabajo, tales como un Plan de Recuperación de Desastres, el cual no solo abarcan los respaldos de servidores, sino el procedimiento en general a tomar acorde a las diferentes áreas de la empresa.

Estas materias previamente mencionadas, conforman los puntos de partida que permiten el desarrollo de propuesta con nombre "Ciberseguridad - Essentials" para este startup, propuesta que consta de 5 fases en el transcurso de un tiempo determinado.

Propuesta de proyecto – "Ciberseguridad Essentials"

A inicios de la maestría, varias de estas materias fueron clave para el desarrollo y soporte de ciertos procesos en el anterior lugar de trabajo del autor, en donde destacaron los siguientes puntos:

Evidencias previo lugar de trabajo (Ver anexo A)

- Asistencia de implementación de la norma ISO 27001 – 2013, brindando asistencia a las matrices de riesgo que elaboraban los encargados de cada departamento.
- Desarrollo de aplicativo web el cual debía cumplir requisitos de seguridad, pasando por pruebas de caja negra, donde se reforzó la seguridad por headers del servidor del aplicativo y control de accesos a la base de datos por código, finalmente aprobado y adoptado por varios clientes de renombre.
- Asistencia en auditorías de TI a empresa de seguros, tomando responsabilidad en temas de control de accesos, infraestructura de redes, continuidad de negocio, protección de datos personales, todo esto mediante las indicaciones estándares de las políticas internacionales y locales de esta aseguradora.

Actualmente, dentro de este startup que consta principalmente de tres departamentos clave (desarrollo – técnico, comercial y marketing), el autor ha implementado las siguientes medidas desde su entrada a dicho startup:

Evidencias actual lugar de trabajo (Ver anexo B)

- Jobs que realizan el respaldo de las instancias que se encuentran alojadas en Amazon Web Services del servidor del aplicativo web y bases de datos del ambiente de producción.
- Implementación de buckets s3 para subida de imágenes en el aplicativo, evitando cross site scripting.
- Identificación de activos físicos y lógicos mapeados con su importancia.
- Elaboración general de matriz de riesgos por departamentos.
- Identificación de procesos críticos del startup.

- Capacitaciones sobre buenas prácticas de seguridad, donde se abordaron temas de uso de credenciales, amenazas (phishing - malwares), importancia de vpn.
- Implementación de vpn mediante servidor en Google Cloud.
- Encriptación del equipo de trabajo del personal remoto mediante BitLocker.
- Uso de gestor de contraseñas con Norton Password Manager.
- Conformación del gobierno de Continuidad de Negocio.
- Elaboración de matriz BIA y RIA según los procesos críticos.
- Uso de sistema CRM para el manejo de leads o clientes en vez de mantener bases en hojas de cálculo.
- Control de accesos por roles al dashboard de administrador del aplicativo web y demás plataformas.
- Accesos a servidores de producción y staging mediante clave ssh y validación ip (vpn).

Tomando estos puntos previamente mencionados, los cuales son los que se han implementado en este startup, se busca formalizar y sistematizar dichas acciones mediante políticas, controles y procesos; adicionalmente identificar y profundizar en las potenciales vulnerabilidades presentes, materializándose en forma de propuesta que ramifique en diferentes proyectos en el transcurso del tiempo.

Dentro de la siguiente propuesta, se tomaron las bases de las materias previamente descritas, las cuales se seccionan en diferentes fases de esta propuesta de proyecto con nombre “Ciberseguridad - Essentials”. Esta propuesta tiene como objetivo establecer los cimientos en términos de Ciberseguridad y Seguridad de la Información, para el actual lugar de trabajo del autor, startup que brinda soluciones tecnológicas para mejorar el desarrollo de la sociedad. Estos “cimientos” o “pilares” desarrollarán las bases que cualquier empresa o entidad pueda implementar

dentro de sus procesos, activos, finanzas y operaciones en general, mitigando el riesgo de cualquier tipo de amenaza o situación emergente, esta propuesta se compone en 5 fases:

Fase #1 – SGSI

Dentro de la primera fase la cual constará de 5 semanas, se desarrollarán los siguientes puntos a conformar para establecer un Sistema de Gestión de la Seguridad de la Información:

- Primera semana, conformación del comité de Seguridad de la Información e identificación de procesos generales en los diferentes departamentos de la empresa.
- Segunda semana, desarrollo de matriz de riegos por departamento.
- Tercera semana y Cuarta semana, desarrollo de políticas, procedimientos y protocolos a partir de la matriz de riesgos.
- Quinta semana, capacitación general al personal sobre las políticas, procedimientos y protocolos.

Fase #2 – Seguridad de Aplicativos y Bases de Datos

La segunda fase se en enfoca en la seguridad a nivel de activos lógicos o tecnológicos, como los son el código del aplicativo, servidores y bases de datos, teniendo una duración de 4 semanas:

- Primera semana, se analizará el código a nivel de prueba de caja blanca, prueba cual entregará un informe presentando las vulnerabilidades actuales del aplicativo web y móvil, las cuales serán solventadas ya en función de los tiempos del equipo de desarrollo.
- Segunda semana, se realizará el análisis de los servidores del aplicativo y bases de datos, para tomar medidas preventivas ya sean de resolución o parchado según las vulnerabilidades presentes.

- Tercera semana, se empezará con la identificación de herramientas que permitan un desarrollo de tipo “Devops” para el equipo de desarrollo en conjunto del equipo comercial.
- Cuarta semana, se volverán a realizar las pruebas de penetración hacia los activos previamente analizados la tercera semana.

Fase #3 – Gestión Económica en procesos y emergencias

Esta fase se enfoca al cálculo del presupuesto disponible hacia procesos que necesitan una inversión monetaria o en casos de emergencias, esta fase constará de dos semanas:

- La primera semana, se identificarán que procesos se mantienen en un nivel de riesgo alto y necesitan de una inversión considerable, las cuales serán tratadas con la directiva de la empresa.
- La segunda semana se realizarán las actualizaciones de las matrices RIA y BIA acorde a los procesos de la empresa y serán de igual manera presentados a la directiva.

Fase #4 – Continuidad de Negocio

Esta fase constará en 5 semanas, en las cuales se terminará de conformar el Plan de Continuidad de Negocio, en donde se terminará de implementar:

- Primera semana, Comité de Continuidad de Negocio.
- Segunda semana, Plan de Recuperación de Desastres.
- Tercera semana y Cuarta semana, Políticas y Procedimientos de Plan de Continuidad de Negocio.

- Quinta semana, simulaciones de emergencias y pruebas del Plan de Recuperación de Desastres sobre los activos actuales de la empresa.

Fase #5 – Retroalimentación - Capacitación

En esta fase final se realizarán capacitaciones al personal en general, tanto como pruebas a los mismos mediante técnicas como phishing, y se espera una retroalimentación mediante simulaciones de situaciones reales para comprobar la efectividad de las medidas de control implementadas.

Recomendaciones

Dado el transcurso para la elaboración de este documento, se han identificado ciertas pautas a seguir para establecer implementaciones o realizar cualquier tipo de acción requerida, tales como:

- Mantener reuniones estratégicas con la directiva o encargados de los departamentos o partes involucradas sobre lo que se quiere realizar, para de esta manera acaparar en el personal la atención e importancia esperada.
- No todo el personal es consciente de las amenazas existentes, por lo que es pertinente realizar campañas o capacitaciones que poco a poco concienticen al personal sobre la importancia de la seguridad en general.
- No es posible mantener un conocimiento absoluto en general, por lo que es recomendable realizar previamente un “estudio de campo” con los departamentos o personas que se requiera, para luego proceder a tomar mejores decisiones.

Conclusión

Las materias mencionadas son las que han brindado las bases para hacer posible esta propuesta y las implementaciones previamente realizadas; cabe recalcar que este ensayo funciona como guía, más no como requisitos a seguir, la Ciberseguridad es un mundo inmenso en constante evolución, por lo cual es importante mantenerse al día con las metodologías, amenazas y técnicas actuales que se presenten.

Anexos

Anexo A. Evidencias repositorio en sección "Evidencias – Previo lugar de trabajo"

https://lily-enemy-ae5.notion.site/UCG-Ciberseguridad-3c1be387e08c4d91b3ecb659c3289c6a

Anexo B. Evidencias repositorio en sección "Evidencias – Actual lugar de trabajo"

https://lily-enemy-ae5.notion.site/UCG-Ciberseguridad-3c1be387e08c4d91b3ecb659c3289c6a

Referencias

Arlenys, C. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA.* Politécnico GranColombiano.

Bass, L., Weber, I., & Zhu, L. (2015). *DevOps: A Software Architect's Perspective .* Addison-Wesley Professional.

Castro, C. (2019). *Pruebas de Penetración e Intrusión.* Universidad Piloto de Colombia.

Ecuador, G. N. (2020). *GUÍA PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN.* Gobierno Nacional del Ecuador.

ISO. (2013). *Information technology — Security techniques — Information security management systems — Requirements.* ISO.

Latina, B. d. (2020). *Oneto Andrés.* CAF.

nqa. (2019). *ISO 22301:2019 GUÍA DE IMPLEMENTACIÓN DE LA CONTINUIDAD DE NEGOCIO.* nqa.

Souppaya, M., Scarfone, K., & Dodson, D. (2022). *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.* Gaithersburg, Meryland, United Stated: National Institute of Standars and Technology.