|  |
| --- |
| **Título del Proyecto:** |
| **Granja sostenible usquito** |
| **Meta, Alcance y Objetivos:** |
| **Meta:**  Crear un proyecto de calidad, que logre satisfacer los requerimientos y logre cumplir con las peticiones de la granja experimental auto sostenible de la universidad Surcolombiana.  **Alcance:**  El alcance del proyecto es tener una página para dar a conocer todos los servicios y productos que produce la granja experimental a toda la comunidad, vinculando de manera directa, a la web oficial de la universidad, diseñando una interfaz amigable para que sea más grata su visita a la página web de la granja.  **Objetivos generales:**  Dar a conocer a la comunidad, todos los productos y servicios que ofrece la granja experimental autosostenible usquito por medio de una página web.  **Objetivos específicos:**   * Consolidar la información necesaria para dar una perspectiva tanto global como específica de la granja a toda la comunidad. * Diseñar una interfaz amigable con la comunidad para que sea más grata su visita a la página web de la granja. * Vincular de manera directa la página web a la página oficial de la Universidad Surcolombiana con el objetivo de aprovechar los recursos que ofrece la institución. |
| **Definición de Condiciones, Restricciones y Supuestos del Proyecto:** |
| El proyecto debe ofrecer como resultado final un producto de calidad y totalmente operable.  Se asumirá que el cliente contará con la infraestructura que se requiere para poner el sistema en ambiente de producción para la fecha en la cual se establezca la entrega del producto.  La solución deberá poderse instalar en los servidores propios de la universidad y deberá vinculada en la página oficial de la universidad surcolombiana.  La plataforma estará alojada en un servidor local de la universidad.  El sistema debe estar en capacidad de soportar hasta 1000 usuarios concurrentes.  **Leyes y decretos los cuales restringer el software:**  La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos. De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado De la Protección de la información y de los datos que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”. El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):  - Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.  - Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.  - Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.  - Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.  - Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.  - Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.  Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.  - Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS  PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.  En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.  La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.  Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006  Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:  1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.  2. Por servidor público en ejercicio de sus funciones  3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.  4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.  5. Obteniendo provecho para sí o para un tercero.  6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.  7. Utilizando como instrumento a un tercero de buena fe.  8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales. Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos, así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”. Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal. Por su parte, el capítulo segundo establece:  - Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.  - Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.  La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos ó telemáticos. Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea. En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información. Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información. Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información. Así mismo, resulta conveniente dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes del nuevo rol que les corresponde en el nuevo mundo de la informática. Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas. Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales. |
| **Miembros del Equipo:** |
| * Patrocinador: Universidad Surcolombiana * Líder del proyecto: Natalia Tapias Heredia * Representantes de los usuarios: Representante de la usco |
| **Reglas de Juego para el equipo:** |
| Se definieron las siguientes reglas para el grupo:   1. **Reuniones**: Se realizará una reunión semanal de forma virtual: Los lunes de 9:00 pm a 11:00 pm por google meet en una reunión la cual será preestablecida. 2. **Reunión de seguimiento del proyecto:** La reunión de seguimiento del proyecto se realizará los jueves de 6:00 pm a 6:30 pm,por medio virtual. La asistencia a esta reunión es obligatoria, por tanto, en caso de NO asistencia la persona aportará 10.000 pesos para la próxima fiesta u otro evento sin ánimo de trabajo que se haga. 3. **Comunicación:** La comunicación oficial se hará por un tablero de trello, predefinido por el equipo, si se necesita de una mayor comunicación se hara a través del grupo de telegram el cual creará el líder del proyecto. 4. **Mecanismo de toma de decisiones:** Algunas decisiones se toman entre todos, por medio de un consenso de grupo. Si un integrante NO se encuentra en el momento de una reunión en donde hay consenso, se aprobará la decisión tomada, deberá aceptar y cumplir las decisiones que allí se hayan tomado. 5. **Asignación de tareas:** Cargas iguales de trabajo para cada miembro del equipo y cada persona elige qué quiere hacer, debido a que unas personas tienen más experiencia en ciertos temas que otros. Si existen tareas que no las quiere nadie se hace por consenso del grupo. 6. **Resolución de conflictos:** Si se presentan conflictos entre dos o más personas se podrán escalar al líder del equipo el cual podrá personalmente intentar solucionarlo, o podrá ponerlo como un punto de la agenda de la reunión semanal. 7. **Igualdad en el equipo de trabajo:** Todos los integrantes del equipo del trabajo, tendrá una opinión válida, y sin importar su rol en el proyecto esa opinión pesará de igual manera a la decisión de los demás. 8. **Organización de grupo de trabajo y óseo:** se creará un grupo de telegram para hablar solamente del proyecto, y otro grupo para hablar de cosas cotidianas o fuera del proyecto, para poder tener un lugar, para desestresarse y tener una mejor comunicación fuera de lo laboral con el equipo de trabajo. |
| **Organigrama y definición de Roles y Responsabilidades:** |
| Los miembros del equipo han asumido un rol cuyas funciones están claramente establecidas y se dividen de la siguiente manera:    Figura 1. Organigrama equipo de trabajo SAYA |
| **Requerimientos del Proyecto:** |
| .  **Funcional**  La plataforma web de la granja de usquito me permitirá consultar toda la información acerca de está sin necesidad de ir al establecimiento. Además, obtendré la información si la granja se encuentra disponible para poder realizar visitar a esta.  Este sitio web se tiene previsto realizarse en ocho meses, según el cronograma trabajando fuertemente las cuatro semanas.  **Ambiente Físico**  La plataforma estará alojada en un servidor local de la universidad. El control ambiental, tanto de temperatura como de humedad, contando así mismo con detectores de inundación. La temperatura debería ser constante en un arco de 20 a 22 grados centígrados, y la humedad no debería ser entre 40 y un 50%.  **Seguridad**  Acceso controlado, ya sea mediante llave, o algún dispositivo de clave. Ambas cosas, llave o clave sólo la deben conocer personal autorizado.  **Generadores**  Sistemas de alimentación ininterrumpida (SAI o UPS), que además realice funciones de protección ante electricidad ‘sucia’, es decir, picos de corriente que pueden dañar a los servidores.  **Requerimientos Funcionales**   1. El usuario deberá tener la posibilidad de ver la disponibilidad en que se encuentra el establecimiento físico. Para saber si puede o no visitarlo 2. El sistema deberá proporcionar toda la información de interés a sus visitantes   **Requerimientos No funcionales**   1. El sistema debe ser capaz de operar adecuadamente con hasta 1000 usuarios con sesiones concurrentes. 2. El tiempo de aprendizaje del sistema por un usuario deberá ser menor a 4 horas. 3. El sistema debe proporcionar mensajes de error que sean informativos y orientados a usuario final. 4. El sistema debe contar con un módulo de ayuda en línea. 5. La aplicación web debe poseer un diseño “Responsive” a fin de garantizar la adecuada visualización en múltiples computadores personales, dispositivos tableta y teléfonos inteligentes |
| **Matriz de Riesgos:** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RIESGO | PRIORIDAD | IMPACTO | PROBABILIDAD | DESCRIPCIÓN | PLANES DE CONTINGENCIA |
| No obtención de alogamiento por parte de la USCO | 1 | Bajo | Media | Es posible que en los servidores de la usco no blinden un espacio en sus servidores para la montura de la página web | Se procederá a conseguir un hosting y un dominio para montar la pagina web y pedir a la usco el agregamiento del link en la plataforma de la usco. |
| **Falta de equidad en cuanto al conocimiento de los lenguajes y herramientas utilizadas** | 3 | Medio | Alta | Es posible que todos los miembros del grupo no cuenten con la misma experiencia y conocimiento de los lenguajes y herramientas utilizadas. Si esto sucede, el tiempo de desarrollo en general puede incrementarse significativamente. | Se le preguntará a cada miembro que tanta experiencia y conocimiento tiene en los diferentes lenguajes utilizados, con el fin de asignar tareas de acuerdo a los conocimientos, destrezas y habilidades de cada persona. Si alguno de los integrantes tiene un alto conocimiento de alguna de las herramientas, el líder evaluará la conveniencia de programar sesiones de entrenamiento de las herramientas. |
| **Problemas técnicos** | 4 | Medio | Baja | Se debe considerar la posibilidad de que se presenten problemas técnicos como fallas en los equipos de cómputo, pérdida de información, cortes de energía,etc | Instalar un repositorio de código, datos y documentos, con los niveles de seguridad adecuados, política de permisos y backup definidas. |
| **Problemas de Comunicación** | 2 | Alto | Baja | Los problemas de comunicación dentro del grupo, pueden provocar una baja en la productividad e incumplimiento de las tareas del proyecto y por ende de los objetivos del grupo. | El líder del grupo debe dar participación a los miembros del grupo en cada reunión, con el fin de conocer los diferentes puntos de vista de cada persona y que se establezca un diálogo sano y amigable. Los acuerdos y responsabilidades deben ser comunicadas a todos los integrantes del grupo, con el fin de evitar malos entendidos. Si el líder detecta que un integrante del grupo tiene alguna dificultad o existe alguna rivalidad, se debe hablar con cada persona y tratar de resolver los conflictos en el menor tiempo posible. |