Organización que tiene un equipo de desarrollo de proyectos tecnológicos, desarrollando varios proyectos/softwares, estos se comunican a través de APIS de comunicación, también se comunican con BD externas, de la misma organización, a través de APIS. Hay equipo de QA y de desarrollo, cada proyecto de SW tiene su equipo de desarrollo, están implementando prácticas de desarrollo de SW, gestionan requerimientos a través de la plataforma JIRA, trabajan con SCRUM, código de SW en repositorios privados de GitHub, los SPRING se componen de mas o menos tres semanas, donde la última semana es de QA, con un equipo separado de revisores, los revisores son estudiantes con becas de trabajo, y los desarrolladores están full time.

Unidad de desarrollo de proyectos tecnológicos para la facultad de ingeniería, generación de varios desarrollos y proyectos tanto para el decanato de la facultad de ingeniería y los departamentos académicos. La facultad de ing. Se compone del decanato, dptos. Académicos, centros de investigación y otras subunidades. El decano es la autoridad mayor, en los departamentos son los directores de departamentos. Hay un consejo que reúne tanto al decano como a los directores de departamento, donde se deciden cosas transversales a nivel de facultad, además de consejeros, los temas al interior del departamento se deciden al interior.

El desarrollo de proyectos es parte del decanato, deben tener cierta seguridad. Actualmente han desarrollado los proyectos con ciertos resguardos, manejan gestor de versiones en GitHub modalidad privada, montan los desarrollos en un entorno al interior de la universidad, en un servidor de pruebas y producción, BD de prueba y producción por separado, los desarrolladores no tienen acceso directo a estos entornos, solo manejan sus entornos de desarrollo. También existe un área de QA que prueban estos desarrollos antes de pasar a los usuarios, se preocupan del tema funcional y algunos temas de seguridad, por ejemplo, GitHub avisa cuando hay versiones vulnerables de dependencias y componentes, RoR como framework de desarrollo, con sus respectivas gemas. Sistema de versión de requerimientos, tareas e incidentes, llamado JIRA, se encuentra los desarrolladores y el equipo de QA, donde se gestionan los requerimientos de los diferentes usuarios. Separan los incidentes con la gestión de requerimientos. Trabajan con metodología SCRUM, al planificar un SPRINT se revisan las incidencias, se pasan al sistema requerimientos a medida de su prioridad, desde GitHub. Los requerimientos hechos por usuarios. Existen requerimientos de seguridad respecto a la autenticación de las apps, al desarrollo, los estándares, donde están los datos, las codificaciones, la replicación de datos. Han tratado de revisar buenas practicas de seguridad de desarrollo de SW, herramientas automáticas. Ya tienen un par de aplicaciones en línea, estas están requiriendo interconectarse con otras aplicaciones, por ejemplo LOA, a través de APIS de comunicación.

Principales activos que proteger en estos momentos:

1. El código fuente
2. Las BD de desarrollo tanto de pruebas como de producción, la de prueba replica a la de producción cada cierto tiempo y la de producción contiene datos de los usuarios.
3. Los servidores donde todo esto está montado.
4. Servicios de Google, gestión de archivos, formularios, documentos.

Codigo fuente disponible en GitHub, los desarrolladores los bajan a sus equipos de desarrollo, por lo tanto, se deben proteger estos equipos.

Servidores se encuentran en la red de la universidad, solo se pueden acceder a través de servicios de VPN, con un usuario autorizado. Hay una persona que se encarga de meterse a los servidores con su usuario VPN para actualizar el código y la BD, sin embargo, la BD no depende del departamento, es antigua, permite gestionar una gran cantidad de datos de forma rápida, sin embargo, es administrada por otra área dentro de la unidad informática de la facultad.

Entorno empresarial: relación con unidad de vicerrectoría de investigación y desarrollo, que provee datos de investigaciones y proyectos que realizan los académicos. También se relacionan con la unidad de datos, los diferentes vice decanatos, con las oficinas de recursos humanos al interior, y con los departamentos académicos.

SW que se están desarrollando que son activos a proteger (datos de estudiantes/profesores):

* Sistemas de gestión de la actividad académica.
* Sistema de solicitudes.
* Sistema de gestión de programas de asignaturas.
  + Seguimiento de asignaturas.

Identificar:

**¿Cuál es la planificación que posee la organización en términos de ciberseguridad?**

Existen planes operativos dentro de la organización, donde se definen todos los proyectos que se van a realizar durante el año y se les realiza seguimiento. Entre esos proyectos, algunos están relacionados con temas de seguridad, los últimos años se han hecho temas relacionados con políticas, que se pueden hacer internamente y no se debe hacer tanta inversión de recursos. Gestión de riesgos se hizo una vez y no está formalizado y adquirido en la organización. Personal dedicado al tema de seguridad no hay. Las jefaturas de las áreas tecnológicas tienen preparación en temas de seguridad. Las políticas que se han desarrollado son: seguridad de información, clasificación de la información, protección de datos sensibles.

**¿Cuáles son los puestos de seguridad y qué responsabilidades tiene?**

No existen los puestos de seguridad, si existe la función de seguridad que se agrega al personal tecnológico.

**¿Cuáles son las herramientas de software utilizadas para la ciberseguridad?**

No existen SW de seguridad, por ejemplo controles para protegerse de ataques DDos o un cloudflare.

**¿Cómo y qué tan seguido se mantienen las implementaciones de la seguridad?**

Respecto a los controles tecnológicos: firewall, IDS basado en firmas de ataque, se compran de forma externa, mantienen ciertas actualizaciones constantes pagadas.

A nivel de equipos de trabajo, a nivel de universidad existen convenios y contratos a nivel de antivirus.

Gestión de seguridad en redes dominio de una empresa externa.

Gestión de seguridad de servidores se preocupa el administrador de sistemas de manera constante.

**¿Cuáles son los recursos más importantes que tiene el departamento de TI?**

**Recursos externos:**

Recursos y servicios de Google. Aún no están en la nube. Bases de desarrollo. RoR como parte de la cadena de suministro. Librerías de autenticación de Google drive.

**¿Qué recursos externos utiliza la institución?**

La institución externaliza la parte informática en cuanto al uso de equipamiento de escritorio, también otras relaciones, por ejemplo el tema de las redes, a nivel de universidad se tiene un enlace de internet internacional. Servicios dedicados o accesos a internet dedicados a ciertos servicios de manera internacional, con un enlace puente.

Algunos SW que maneja la universidad.

**¿Cuáles departamentos de la institución dependen del departamento de TI?**

Dependen de la secretaría académica, la cual depende del decano. Decano -> Vicedecanos (investigación/desarrollo/posgrado/docencia/vinculación por el medio) -> Secretario académico (gestión administrativa/transversal)

**¿Cómo se asignan los roles de seguridad y responsabilidad de información?**

A nivel general, nivel de funciones, descritas en los cargos funcionarios. No hay gobierno de los datos. El sistema de gestión académica abarca mucha información de toda la facultad, van a tener que asignar roles de seguridad. Hay áreas nuevas de la facultad y no tienen bien definidas sus responsabilidades.

En la gestión de activos hay que mantener un inventario, identificar que se tiene, que parte de los activos se quiere proteger y que no.

Entorno empresarial, como se organiza la facultad.

Gobernanza: Gobierno de seguridad de la información. Órgano que se compone por el decano, los vicedecanos y secretarios académicos, decisiones transversales. Se definen, presentan y priorizan los proyectos del año. Lo mismo con las políticas.

Evaluación y Gestión de riesgo baja. Generalmente es algo transversal. Se ha hecho poco a nivel de universidad, y a nivel de facultad nada.

Gestión del riesgo de la cadena de suministro. Se preocupan de cuales son los suministros, por ejemplo, librerías de SW desarrolladas por terceros, actualizadas y que no tengan vulnerabilidades.

**¿Cómo son los procesos de evaluación de riesgo? Basado en vulnerabilidades y amenazas.**

No hay. Cambios en seguridad de la información por dos factores: factor normativo, te obligan a implementar seguridad de la información. En instituciones del estado han avanzado en temas de seguridad. El otro factor es incidental, las organizaciones no invierten en seguridad de la información hasta que pasa algo, en la universidad no hay política de protección de datos personales, definida en la facultad, pero no en la universidad. No hay una política de privacidad. Los procesos se están definiendo. Dependen de las personas y tienen riesgo. Nivel bien básico.

Recuperación:

Planificación de recuperación: Datos de BD respaldados, código del github respaldado, código de servidores de producción y desarrollo respaldados. Los datos se respaldan habitualmente, especialmente antes de las actualizaciones de sistema. Los datos son probados para asegurar que funcionen correctamente con los sistemas. Sacan copia de BD, suben a otra BD.

**¿Qué actividades o planes de recuperación tiene el departamento?**

Ante cualquier amenaza, materializada o no, las BD están todas respaldadas, en un NAS (servidor de base de datos en red), disco duro externo en la casa del administrador de sistemas, y también copia de los datos en la FAE. Lo mismo con los códigos fuentes, y en GitHub.

**¿Se incorpora o actualiza las lecciones aprendidas a los procesos de recuperación?**

**No.**

**¿Cuáles son los puntos críticos internos/externos que participan en las respuestas y recuperaciones de seguridad?**

Varios servidores de respaldo, alta disponibilidad.

**¿Ante un evento de seguridad, el personal tiene la capacidad de reconocer y priorizar la protección de los recursos críticos de la organización? ¿Las tecnologías utilizadas cuentan con protocolos de reconocimiento de puntos críticos en los sistemas y las redes? ¿Pueden priorizar, apoyar y proteger otros servicios?**

Tienen un firewall protegiendo los servidores, que tiene un IDS, módulo de detección de intrusos, e IPS, módulo de protección, para bloquear los flujos. Estos son en base de firmas de ataque. Si el ataque no está en la base de datos, por ejemplo, los ataques nuevos, puede que no sean detectables. Hay controles para mitigar eso pero no se tiene, por ejemplo un sistema de detección en base a anomalías, políticas de inteligencia artificial y estados normales del sistema.

**Seguridad de los datos.**

Datos en frío o reposo o estáticos, almacenados y en frío, aparte. Datos en tránsito, de un equipo a otro en redes. Datos en caliente o dinámicos, en sistemas de producción, en actualización continua.

Los datos en tránsito, entre routers, control a nivel de capas, seguridad IP, encripta comunicación de router a router.

Dentro de la universidad, topología de anillo a nivel de switch (capa 2), los datos pueden circular por toda la universidad hasta llegar al destino, pueden estar susceptibles a ataques capa 2. Pueden atacar los switch y los equipos de la red. Algunas amenazas como man in the middle, meterse en la comunicación entre dos equipos y escucharla. ARP poison engaña a los equipos y los switch, indicando que la MAC corresponde al equipo de destino, re enviándola al equipo de destino y escuchando la comunicación, no se pueden dar cuenta porque no hay perdidas de paquetes.

Hacia afuera los datos van encriptados, se hace a través de VPN.

La segmentación de red también, la facultad tiene ciertos rangos de IP, un rango corresponde a la red de servidores que pueden ser compartidas por otros equipos en la red.

Los datos estáticos corren riesgo de filtración. Algunos datos de las personas quedan en los equipos de las personas en sus casas debido a la pandemia.

Datos en producción son los más protegidos. Sin embargo, hay ciertos accesos a la BD que son antiguos que no se han eliminado, riesgo de filtración.

**¿Cómo afrontará la pérdida de datos la institución, respecto a los afectados?**

Se recurre a los respaldos. Tienen procedimientos para ver si se corrompe un dato. Hay redundancia de datos. Están en BD y en papel. Tienen como recuperar los datos.

**¿Se implementan mecanismos para lograr requisitos de resiliencia en situaciones normales y adversas?**

Si, pero no es algo formal y recurrente, es algo ad hoc, cuando se puede hacer se hace. Si un disco duro de corrompe se arregla solo. El servicio no se pierde y tiene disponibilidad. Hay tipos de servidores y de discos que soportan cambio en caliente. Diferentes fuentes de poder, para no perder el servicio. Diferentes configuraciones en data center. Si le pasa algo al sitio caliente, puede ser trasladado a otro.