POLITICAS DE SEGURIDAD DE LA INFORMACION

INTRODUCCION.-

La Universidad del Azuay, para garantizar principios fundamentales de la seguridad de información, i) la integridad que hace referencia a que la información debe estar libre de alteraciones o modificaciones no planificadas, ii) la disponibilidad que indica que la información debe ser utilizable cuando se la requiera, y iii) la confidencial para que la información pueda ser accedida solo por los que lo requieren, se norma mediante las siguientes políticas de Seguridad de Información:

OBJETIVOS DE DESARROLLO SOSTENIBLE.-

La Universidad del Azuay como una comunidad comprometida con su entorno y el tejido social, así genera estas políticas que apoyan a las acciones que la Universidad realiza hacia alcanzar los objetivos de desarrollo sostenible promovidos por la Organización de Naciones Unidas, en específico con los objetivos 4. "Educación de calidad" y 11. "Ciudades y comunidades sostenibles".

OBJETIVOS.-

Para la Universidad del Azuay, en base a lo que sugiere la norma 27001:2013, los objetivos a alcanzar en la implementación de un Sistema de Gestión de Seguridad Integral (SGSI), pretende:

- Asegurar la confidencialidad, seguridad y correcto uso de los sistemas de la Institución, además de la información de la misma.
- Asegurar de forma adecuada la información y tecnologías empleadas en la Institución, aumentando así la confianza en cuanto al uso y la confidencialidad.
- Garantizar el compromiso de la dirección de la Universidad con la seguridad de la información.
- Establecer los canales adecuados para poder garantizar la seguridad de la información en todos los procesos institucionales.
- Identificar los riesgos que puedan afectar a los procesos de la Universidad, minimizando las amenazas que pudieren impactar sobre las mismas y provocando a su vez una disminución de los riesgos asociados a todos los activos de información.
- Mejorar y crear nuevos controles para garantizar el cumplimiento de los niveles de riesgo que acepta la Universidad.

Universidad del Azuay | Av. 24 de mayo 7-77 y Hernán Malo | Teléfono: (593) 7 409 1000, Fax: (593) 7 281 5997 | Apartado 981 | www.uazuay.edu.ec | Cuenca, Ecuador

- Establecer la forma de poder controlar y cuantificar el estado actual y futuro de los sistemas de la Seguridad de la Información mediante el uso de auditorías internas, provocando de esta forma una mejora continua y detección de nuevas amenazas contra los activos.
- Aumentar la concienciación sobre la seguridad y gestión de la información para asegurar la continuidad de las operaciones en condiciones críticas.
- Mejorar las inversiones realizadas por la Institución en la gestión de los sistemas de Seguridad de la Información, mediante la implantación de nuevos sistemas, evolución de los mismos o mejora de procedimientos.

Las alcances descritos en este documento, norman las responsabilidades del Departamento de Tecnologías de Información, entidad encargada de la implementación de las políticas de seguridad aquí establecidas, en los ámbitos de gestión de datos, redes y telecomunicaciones e infraestructura, servicios Web.

Políticas de seguridad sobre la gestión de bases de datos. Responsable: Subdirecciones de Desarrollo y Producción.-

- El Departamento de Tecnologías de Información, tiene la responsabilidad, de estructurar las bases de información, desarrollar las aplicaciones requeridas para los procesos administrativos y académicos, optimizar el funcionamiento y entregar a las áreas interesadas, con la debida capacitación y documentación de uso, dar mantenimiento y apoyo a las aplicaciones en base a los requerimientos.

- El desarrollo de software se efectuará en las herramientas autorizadas por la Dirección de Tecnologías de Información de la Universidad, las mismas que contarán con el respectivo licenciamiento, en caso que las requieran.

- Se mantendrá activo tres ambientes informáticos para los procesos de implementación, siendo estos: Desarrollo, Certificación y Producción, con los respectivos protocolos de gestión, para el traslado de aplicaciones y datos entre ambientes.

- Se alojarán las bases de datos, manteniéndolas activas con una garantía de operación del 99,95% del tiempo (uptime).

- Se deberá usar las herramientas necesarias para mantener copias diarias de todas sus bases de datos y ambientes, las mismas que deberán almacenarse en unidades independientes tipo NAS (Network Attached Storage), autónomas de los almacenamientos utilizados por los servidores de Producción, Desarrollo y Certificación.

- Se debe mantener una réplica ON-LINE (espejo) de las bases transaccionales en el ambiente de Producción, en el sitio alterno de la Institución, con un desfase transaccional no mayor a 30 segundos entre los sitios.

- Se mantendrá una política de control de accesos, en los niveles de administrador (super-usuario), desarrollador, usuario final, los mismos que deberán manejarse de forma encriptada e integrada con servicios de terceros.

- Se asignará el acceso a cada usuario, a la información de cada función de los usuarios, basado en la definición previa de perfiles

- Se activará de forma permanente los elementos de auditoría, para todas las bases de datos transaccionales en el ambiente de Producción, que permitan determinar todas las transacciones y/o actualizaciones de información, manteniendo la información mínima de fecha-hora, usuario, máquina, contenido pre y post modificación.

- Se efectuará las coordinaciones necesarias, con las áreas de Software, Web, Soporte con la Dirección del Departamento de Tecnologías de Información, cuando se requieran soluciones que integren varios componentes de diferentes áreas.

Todo el personal del área firmará un convenio de confidencialidad y buen uso de la información, dentro del ámbito de su responsabilidad, solo la Dirección de Tecnologías de Información autorizará usos no contemplados dentro de su función.

Políticas de infraestructura, redes y telecomunicaciones. Responsable:

Subdirección de Infraestructura.-

- Es responsabilidad del área de Tecnologías de Información por medio de la Subdirección de Infraestructura, el diseño, implementación, operación y mantenimiento de la infraestructura de hardware, redes LAN, Wifi, Internet, propias de la Universidad, así como servicios entregados por terceros que sugieran la utilización de medios digitales, o infraestructura de la Institución.

- Mantendrá activos los 2 centros de datos (principal y alterno), respetando el modelo activo-pasivo para todos los servicios, con plataformas de servidores y arquitecturas de red del mismo tipo, que garanticen integración entre los centros de datos, actualmente ubicados en los Campus Principal y Bicentenario.

- Los centros de datos mantendrán los protocolos de diseño construcción y gestión para los Centros de Datos, basados en el estándar TIA-942 (ANSI-TIA) para el tipo TIER-2 . La

Universidad del Azuay | Av. 24 de mayo 7-77 y Hernán Malo | Teléfono: (593) 7 409 1000, Fax: (593) 7 281 5997 | Apartado 981 | www.uazuay.edu.ec | Cuenca, Ecuador

adopción de una norma superior, deberá ser aprobada previamente por las autoridades de la Institución.

- Los centros de datos estarán interconectados de forma permanente con enlaces de alta capacidad (principal y backup), e integrados en una red de capa 2.

- El centro de datos alterno, contendrá una copia de todos los servicios del centro de datos principal.

- Se contará con la normativa de replicación, backups, y protocolos de activación de servicios desde el sitio alterno desarrollada por la subdirección de Producción

- La Institución contará con una red física basada en normas y estándares vigentes en el mercado, debiendo acogerse a las recomendaciones, buenas prácticas y estándares internacionales, acordes a la necesidad institucional.

- El Departamento de Tecnologías de Información: diseñará, construirá nuevos requerimientos, basados en las capacidades e infraestructura actual que dispone la Institución, tanto para los Campus Central, Bicentenario y otras sedes u oficinas que sean parte de la Institución.

- Todas las dependencias locales y remotas, deberán estar interconectadas con capacidades de transmisión de datos que soporten los servicios internos y provistos por terceros, con una capacidad de al menos 1.5 veces el promedio de consumo del último semestre.

- El hardware de soporte de las redes deberán tener la capacidad de gestión de datos, servicios de comunicación (correo, video conferencia), transferencia de archivos, telefonía IP y todos aquellos servicios que se incorporen a la Institución.

- Se implementará soluciones de hardware de red, con equipamiento necesario para cubrir una arquitectura de 3 niveles: core, distribución y acceso.

- El equipamiento de core, y de distribución, deberá ser redundante, para garantizar una operación de 99,95% (uptime)

- Se contará con una red inalámbrica (Wifi) de acceso libre en todas las sedes, la misma que deberá gestionarse de forma centralizada con capacidad de soporte para los estándares vigentes.

- La cobertura de la señal Wifi, deberá ser superior al 95% de las áreas físicas, para ello se efectuará mediciones en todas las área, al menos una vez cada año, o cuando existan modificaciones a la red.

- Tanto el tráfico en redes físicas como inalámbricas, serán de forma encriptada, utilizando la tecnología y equipamiento que garantice la que la transmisión entre el origen y destino no pueda ser decodificada por terceros.

- Se utilizarán las herramientas de gestión y monitoreo permanente de estado de los componentes de la red ethernet, red wifi, estado de salud de servidores, estado de los servicios publicados en la página Web de la Universidad, uso de los enlaces lan y wan.

- La integración con servicios de terceros, tales como proveedores de Internet, proveedores de telefonía, servicios de transacciones con tarjetas de crédito/débito, servicios de video conferencia, u otros servicios que se integren con empresas públicas o privadas, deberá cumplirse con la normativa específica de contratos, tanto en los requerimientos de hardware, software, gestión y seguridad, específicos de cada servicio. De ser necesario se implementará políticas específicas de gestión y control en los casos que ameriten.

- Mediante la utilización de software y hardware específico, se controlará el acceso no autorizado a equipos servidores de bases de datos, de aplicaciones, equipos de red, equipos de seguridad, y demás implementos sensibles que presten uno o varios servicios a la Institución.

- Los laboratorios Informáticos, computadoras, impresoras, cámaras video-vigilancia, etc, están a cargo, serán de responsabilidad de la subdirección de Infraestructura de T.I., tanto en su funcionamiento, actualización y mantenimiento.

- La configuración, implementación de políticas de seguridad, gestión de accesos a los servicios, serán controlados de forma centralizada, en servidores de Active Directory o LDAP.

- Llevará registro del inventario de hardware, software, licencias de productos que fueren utilizados por la institución, así como gestionará las renovaciones y actualizaciones requeridas.

- Efectuará las coordinaciones necesarias, con las áreas de Software, Web, soporte con la Dirección del Departamento de Tecnologías de Información, cuando se requieran soluciones que integren varios componentes de diferentes áreas.

- Todo el personal del área firmará un convenio de confidencialidad y buen uso de la información a su cargo, la misma que incluye arquitecturas de red, detalles de configuraciones de equipos, productos utilizadas y otras que pudieren ser utilizadas en contra de la Institución y su gestión. Solo la Dirección de Tecnologías de Información autorizará la entrega de información a terceros.

Universidad del Azuay | Av. 24 de mayo 7-77 y Hernán Malo | Teléfono: (593) 7 409 1000, Fax: (593) 7 281 5997 | Apartado 981 | www.uazuay.edu.ec | Cuenca, Ecuador

De la publicación de servicios en la página web de la Universidad del Azuay.- Responsable: Subdirección web.-

- El diseño, desarrollo, gestión de contenidos, publicación de servicios, mantenimiento y otras actividades relacionadas con la página Web de la de la Universidad del Azuay, serán administrados y gestionado por la subdirección web.

- La subdirección web debe coordinar con las diferentes unidades académicas y administrativas, en el análisis, diseño, implementación, publicación y mantenimiento de los productos que se incorporen dentro del dominio uazuay.edu.ec.

- Los desarrollos, modificaciones, mejoras, cambios de versiones de software, se efectuarán en ambientes de desarrollo, en los que se realizarán las pruebas funcionales y de seguridad, previo paso al ambiente de producción.

- Todas las aplicaciones y servicios publicados, deberán someterse a pruebas de seguridad, previa la puesta en marcha en los ambientes de producción

- Es responsabilidad del área mantener los servicios activos, funcionalmente eficientes con una garantía de operación del 99,95% (uptime).

- La subdirección web será la responsable de manejar e implementar una política de backups y recuperación, para el caso de fallos de hardware, software u otros eventos que afecten el ambiente de producción.

- Definirá y gestionará en coordinación con la Dirección de Tecnologías de Información, las plataformas de software, adquisición de herramientas, gestión de licencias, etc, necesarias para cubrir los requerimientos institucionales.

- Coordinará con las subdirecciones del departamento de Tecnologías de Información, cuando requiera asistencias de infraestructura, telecomunicaciones o información para publicación.

De la gestión y seguridad de usuarios finales.-

- La Universidad del Azuay, proveerá de los equipos informáticos, necesarios para el cumplimiento de las funciones, el personal administrativo los recibirá con actas de entrega-recepción.

- El departamento de Tecnologías de Información, será el único encargado de instalar las herramientas de software, antivirus, aplicaciones de gestión y demás

herramientas para el personal administrativo, los mismos que tendrán el respectivo licenciamiento en las que fueren necesarias.

- Cada usuario será el responsable del control y privacidad que debe dar a las claves de acceso a su equipo, cuentas de correo electrónico, y acceso a las aplicaciones definidas para su función.

- El uso de los equipos, software, aplicaciones, cuentas e información, serán de responsabilidad de los usuarios y servirán para el cumplimiento de sus tareas asignadas por la Universidad del Azuay.

- El personal Docente accederá a las aplicaciones que provee la Institución, según su función, para la gestión académica y administrativa. Será responsabilidad del docente las claves de acceso, la gestión de información, y la oportunidad de efectuar los registros, en función de su rol en la Institución.

Políticas generales.-

- Todas las personas relacionadas con las diferentes funciones descritas en el presente documento, deberán cumplir las políticas indicadas.

- Las presentes políticas serán revisadas de forma periódica, una vez al año o cuando se detecte oportunidades de mejora a alguno de los principios de seguridad de información, en los ámbitos de confidencialidad, disponibilidad e integridad.

Estas políticas serán publicadas en la página web de la Universidad del Azuay, para su difusión y conocimiento por parte de la comunidad universitaria

Cuenca, octubre de 2021

Francisco Salgado

Prof. Francisco Salgado Arteaga, Ph.D.
Rector

Universidad del Azuay | Av. 24 de mayo 7-77 y Hernán Malo | Teléfono: (593) 7 409 1000, Fax: (593) 7 281 5997 | Apartado 981 | www.uazuay.edu.ec | Cuenca, Ecuador