Universidad Autónoma de Zacatecas

UAZ

Política de Seguridad de la Universidad Autónoma de Zacatecas (UAZ)

Índice

Propósito

Esta política tiene como objetivo proteger la integridad, confidencialidad y disponibilidad de la información y los datos de todos los usuarios que interactúan con los servicios informáticos y telecomunicaciones de la Universidad Autónoma de Zacatecas (UAZ). La política se aplica a todos los administradores, docentes, estudiantes, proveedores y visitantes que utilizan los servicios informáticos y telecomunicaciones ofrecidos por la UAZ. La información que incluye, pero no se limita a, números de identificación personal, registros académicos, información de salud, datos financieros y credenciales de inicio de sesión. El proceso de verificación de la identidad de un usuario mediante el uso de credenciales, como nombres de usuario y contraseñas.

Responsabilidades

Usuarios: Deben proteger sus credenciales de acceso, utilizar contraseñas seguras, y reportar cualquier actividad sospechosa o potencial violación de seguridad al equipo de seguridad de la UAZ.
Administradores de Sistemas y Sitios Web: Son responsables de implementar, mantener y monitorear las medidas de seguridad necesarias para proteger la integridad y disponibilidad de los servicios web, telecomunicaciones y los datos que contiene. Esto incluye la instalación de parches de seguridad, la configuración segura de sistemas y la supervisión continua de las actividades del sistema, así como el respaldo de la información.

Control de Acceso

Autenticación: Se requiere que los usuarios se autentiquen mediante el uso de nombres de usuario y contraseñas seguras. La UAZ recomienda la utilización de autenticación de dos factores (2FA) para acceder a áreas sensibles de los servicios web y telecomunicaciones.
Autorización: Los permisos de acceso se basan en roles y responsabilidades. Solo el personal autorizado tiene acceso a información confidencial y a funciones administrativas del sistema.

Protección de datos

Confidencialidad: Los datos sensibles se encriptan tanto en reposo como en tránsito. Esto asegura que la información esté protegida contra accesos no autorizados y posibles filtraciones.
Integridad: Se implementan controles de integridad, como el uso de sumas de verificación y criptografía, para asegurar que los datos no sean alterados de manera no autorizada.
Disponibilidad: La infraestructura tecnológica se diseña para garantizar una alta disponibilidad, con medidas como balanceo de carga y sistemas redundantes, para minimizar el tiempo de inactividad de acuerdo a las limitantes tecnológicas que cuenta con la universidad.

Mantenimiento y Actualización

Actualizaciones de Software: El software del servidor y de la página web se actualiza regularmente para aplicar parches de seguridad y corregir vulnerabilidades conocidas. Esto incluye tanto el sistema operativo como las aplicaciones web y los plugins.
Monitoreo: Se implementan sistemas de monitoreo continuo para detectar actividades sospechosas o anómalas. Los administradores reciben alertas en tiempo real para poder responder rápidamente a posibles incidentes de seguridad.

Gestión de Incidentes

Detección y Respuesta: La UAZ tiene implementados sistemas de detección de intrusiones (IDS) y prevención de intrusiones (IPS) para identificar y mitigar amenazas de seguridad. Los incidentes de seguridad se gestionan de acuerdo con un plan de respuesta a incidentes que incluye la identificación, contención, erradicación, recuperación y análisis post-incidente.
Notificación: En caso de una violación de seguridad que afecte datos personales de los usuarios, la UAZ notificará a los afectados en un plazo de 72 horas desde la detección del incidente, conforme a las regulaciones aplicables.

Incumplimiento de la Política

Consecuencias del Incumplimiento: El incumplimiento de esta política de seguridad puede resultar en sanciones disciplinarias para los administradores, docentes, estudiantes y proveedores, que pueden incluir, pero no se limitan a, advertencias, suspensión de privilegios de acceso y acción legal, dependiendo de la gravedad de la violación.
Medidas Correctivas: En caso de un incumplimiento de la política, se tomarán medidas correctivas apropiadas para mitigar los efectos del incumplimiento, resolver las vulnerabilidades de seguridad que se hayan identificado y prevenir futuros incidentes. Estas medidas pueden incluir revisiones adicionales de seguridad, actualización de políticas y procedimientos, y capacitación adicional para los involucrados.
Notificación: Cualquier violación de la política debe ser reportada inmediatamente al equipo de seguridad de la información de la UAZ. El equipo de seguridad llevará a cabo una investigación completa del incidente y determinará las acciones correctivas necesarias.

Revisión y Actualización de la Política

Frecuencia de Revisión: Esta política se revisará y actualizará anualmente para reflejar cambios en la tecnología, las amenazas de seguridad y las regulaciones aplicables.
Proceso de Revisión: La revisión será realizada por el Comité de Seguridad Informática de la Coordinación de Evaluación e Información Institucional de la UAZ y aprobada por el Coordinador. Los cambios significativos se comunicarán a toda la comunidad universitaria.