SAGRADO
Universidad del Sagrado Corazón

Política para la Seguridad de la Información

Efectivo: 2019.07.01

Propósito

Sagrado (también conocido como "Universidad") establece esta política para crear y establecer controles que incluyendo:

- Asegurar la protección, confidencialidad, integridad y disponibilidad de información sensitiva incluyendo información electrónica protegida.
- Asegurar la prevención de cualquier actividad inusual y/o anormal que envuelve recursos tecnológicos de información.
- Asegurar la protección de los sistemas de información de la Universidad con el fin de mitigar vulnerabilidades, riesgos y amenazas.

Aplicabilidad

Esta política aplica a todos los estudiantes universitarios, facultad, empleados y a toda entidad (“usuarios”) que se les otorgue acceso y uso de los recursos de tecnología de tecnología e información (“IT”) de Sagrado.

Principios de Seguridad de Información

El propósito de la seguridad de información es proteger los recursos de tecnología de información y la información de sistemas de la Universidad de accesos no autorizados o daños.

Todo miembro de la comunidad universitaria es responsable de proteger la seguridad de la tecnología de información de la Universidad, así como de sus sistemas de información. Cada miembro se responsabiliza adhiriéndose a los objetivos y requisitos establecidos en las políticas universitarias.

Todo usuario de los recursos de IT de Sagrado tiene algún tipo de responsabilidad hacia la protección de la tecnología de información y la información de sistemas de la Universidad. Esta política hace referencia a todos los recursos IT ya sean controlados individualmente o compartidos, independientes o en red. Aplica a todas las facilidades de computadoras y comunicación alquiladas, arrendadas, operadas o contratadas por la Universidad, o de la cual la misma sea dueña. Esto incluye: dispositivos en red,

asistentes personales digitales, teléfonos móviles, dispositivos inalámbricos, computadoras personales, estaciones de trabajo, ordenadores centrales (*mainframes*), mini-computadoras y cualquier dispositivo y/o programa asociado. Aplica independientemente de si se usa para propósitos administrativos, investigativos, pedagógicos u otros propósitos.

1. Recursos de Tecnología de Información (IT)

El término recursos de tecnología de tecnología e información ("IT") significa la red, los equipos, los programas, las facilidades, la infraestructura y cualquier otro recurso, están disponibles para apoyar los roles de enseñanza, aprendizaje, investigación y administrativos para los cuales están designados.

2. Integridad de la Información

La información utilizada en el transcurso de manejar, enseñar, aprender, investigar o en el proceso administrativo se puede confiar que refleja correctamente la realidad con que se representa.

3. Confidencialidad de la Información

La capacidad de acceder o modificar información está provista solo para usuarios autorizados y para propósitos autorizados.

4. Apoyo de Desarrollo Académico, Operaciones Administrativas y de Servicios Estudiantiles

Los requisitos para salvaguardar recursos de información deben estar balanceados entre la necesidad de apoyar el desarrollo legítimo académico y las operaciones administrativas y de servicios estudiantiles.

5. Acceso a la Información

El valor de la información como recurso institucional aumenta a través del uso apropiado y disminuye por el mal uso, la mala interpretación o restricciones innecesarias al acceso de la misma. La información perteneciente a Sagrado será utilizada para propósitos universitarios apropiados. Todos lo miembros de la comunidad universitaria deben estar conscientes de su obligación de proteger la información de la Universidad, en particular:

- El acceso a la información se provee basado en la necesidad de saber, la necesidad del usuario llevar a cabo ciertas actividades para la Universidad y provisto que el usuario tenga la autorización apropiada.

- Un usuario autorizado con acceso a información es responsable de almacenar correctamente la misma y asegurarla de accesos no autorizados por medio de, pero no limitado a, cifrado de datos, asegurar y proteger contraseñas, entre otros métodos de control de acceso.
- Un usuario autorizado con acceso a información es responsable de informar sobre cualquier situación real o potencial que se preste para una violación de seguridad de información al Principal Oficial de Información ("CIO") al 787.728.1515, ext. 35871, o por correo electrónico a luis.gotelli@sagrado.edu.
- Los dueños de información que otorgaron acceso a un usuario son responsables de asegurar que ese acceso particular sea asignado, modificado y revocado apropiadamente si el usuario autorizado es transferido o asignado a una nueva actividad o posición donde no necesite del acceso. Igualmente son responsables si el usuario termina su relación con la Universidad.

Clasificación de la Información

Toda la información de la Universidad está clasificada en tres (3) niveles basados en sensibilidad y riesgo. Estas clasificaciones toman en consideración protecciones legales, acuerdos contractuales, consideraciones éticas, asuntos de privacidad, y valor estratégico o propietario. El nivel determina la rigurosidad en las protecciones de seguridad y los mecanismos de autorización de acceso sobre la información. Los niveles de clasificación son los siguientes:

1. Información Restricta

La información se clasifica como "Información Restricta" si la misma requiere protección por ley, por regulación gubernamental o por políticas de Sagrado y si dicha información fuera inapropiadamente divulgada al público pudiera exponer a la Universidad a obligaciones legales o financieras. Usualmente, información con impacto operacional, impacto a los activos o a individuos, de nivel severo o catastrófico, se clasifica como "Información Restricta". Ejemplos de Información Restricta:

- La información sobre la salud de un individuo bajo leyes federales y estatales y regulaciones gubernamentales incluyendo la Ley de Transferencia y Responsabilidad de Seguro Médico (Health Insurance Portability and Accountability Act, HIPPA por sus siglas en ingles) del 1996.
- Archivos estudiantiles bajo leyes federales y estatales y regulaciones gubernamentales incluyendo la Ley de Derechos Educacionales de la Privacidad de la Familia (Family Educational Right and Privacy Act, FERPA por sus siglas en ingles) del 1974.

- Participantes en investigaciones bajo leyes federales y estatales y regulaciones gubernamentales incluyendo la Política Federal para la Protección de Seres Humanos (conocida como "Common Rule").
- Número de Seguro Social
- Número de la licencia de conducir
- Número de tarjetas de crédito
- Número de contabilidad financiera (cuentas de cheque, ahorro, inversión y otras cuentas)
- Archivos personales

2. Información Confidencial

La información se clasifica como "Información Confidencial" si la misma no es considerada Información Restricta y generalmente no está disponible al público. Ejemplos de Información Confidencial:

- Contratos con proveedores, suplidores y contratistas
- Estados Financieros
- Planes de mercadeo y comunicación
- Subvenciones privadas, federales o estatales
- Donaciones
- Información interna financiera, operacional e inteligencia.

3. Información Pública

Toda información que no es restricta o confidencial es considerada "información pública". Ejemplos de Información Pública:

- Anuncios
- Materiales promocionales
- Información en el dominio público.

Responsabilidades

1. Principal Oficial de Información ("CIO")

El Principal Oficial de Información tiene la responsabilidad por la seguridad de los recursos de IT incluyendo redactar, implantar e interpretar todas las políticas relacionadas a la seguridad de la tecnología y de la información y de diseminar información relacionada.

2. Dueños de la Información

Los dueños de la información en el sistema se encargan de poner en función políticas relacionadas al sistema, la información y otros recursos de información bajo su cuidado o control. Algunos de los propietarios son:

- Vicepresidencia de Finanzas y Operaciones
- Vicepresidencia de Desarrollo Organizacional y Recursos Humanos
- Oficina del Registrador
- Oficina de Asistencia Económica Estudiantil
- Vicepresidencia de Asuntos Académicos
- Oficina de Admisiones
- Vicepresidencia de Asuntos Estudiantiles.

3. Administrador de Sistema

Los administradores de sistema son responsables de monitorear la red de Sagrado con el fin de salvaguardar la información al igual son responsables de realizar modificaciones de acceso o revocación a los sistemas de información e instalaciones físicas a solicitud del personal autorizado de Sagrado.

4. Desarrolladores e Integradores de Sistemas

Los desarrolladores e integradores de sistemas están encargados de la implementación de las aplicaciones en la red de Sagrado y que a su vez estén alineadas con las necesidades de la Universidad.

5. Usuario de la Información

Se conoce como usuario un individuo, una aplicación automatizada o un proceso que este autorizado a crear, ingresar, editar o corregir y acceder la información de acuerdo con políticas y procedimientos estipulados. Todo usuario de los recursos de IT de Sagrado es responsable de poner en función las políticas adecuadas y relacionadas a los sistemas, la información y otros recursos de información que utilizan, acceden, transmiten o almacenan. Los usuarios tienen la responsabilidad de:

- Mantener la seguridad de las contraseñas, números de identificación personal (PINs), autenticación de fichas o certificados; los usuarios serán responsabilizados por las actividades vinculadas a sus cuentas
- Manejar toda forma de autenticación y controles de seguridad para los sistemas de procesamiento de información
- Utilizar la información solo para el propósito específico autorizado
- Prevenir la divulgación de la información confidencial o sensitiva

- Reportar cualquier sospecha de incidentes que potencialmente vulnerarán la confidencialidad de la información al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

6. Individuos utilizando computadores personales u otros dispositivos en red

Los estudiantes, facultad y empleados que utilicen sistemas personales para acceder recursos universitarios son responsables por sus computadoras personales y otros dispositivos personales en red. Estarán sujetos a todas las guías de IT, a las políticas y procedimientos para el uso de las facilidades de computación y redes de la Universidad, así como todas las otras leyes, regulaciones o políticas dirigidas al usuario individual.

7. Proveedores Externos

Todos los socios, consultores y proveedores, tales como como consultores de IT, auditores entre otros, trabajando en el campus o remoto, están sujetos a las políticas de seguridad de la Universidad y será requisito que se haga presente en acuerdos contractuales. Los proveedores están sujetos al mismo requisito de evaluación de auditoría y riesgo establecido por las políticas de seguridad y privacidad de información de Sagrado. De haber necesidad de divulgar información no-pública a los proveedores externos, los mismos deberán estar obligados por contrato a acatar las políticas de seguridad y privacidad de información de Sagrado.

Informar el Uso Indebido del Uso de la Información

Los usuarios tienen la responsabilidad de reportar sospechas de incidentes que potencialmente vulnerarán la confidencialidad de la información incluyendo, pero sin limitarse a, sospechas de actividades ilícitas o impropias al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

Inspección y monitoreo la información y los recursos de IT pueden ser necesarios para cumplir con esta Política, realizar investigaciones o auditorías, garantizar la seguridad de una persona o de la Universidad, cumplir con la ley o garantizar el funcionamiento adecuado de los recursos de IT. Solo el CIO (o designado) puede autorizar esta inspección y monitoreo.

Se espera que los usuarios de los recursos de IT cooperen con cualquier investigación de abuso de Políticas. La falta de cooperación puede ser motivo de cancelación de privilegios de acceso u otras medidas disciplinarias.

Consultas sobre esta Política

Las consultas sobre el alcance y la interpretación y las de esta Política deben dirigirse al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

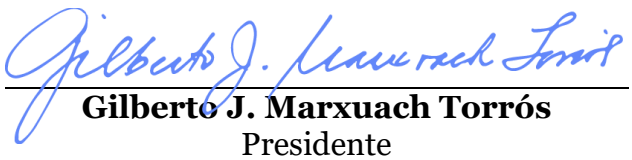
Denuncias de Violaciones a la Política

Las violaciones a esta Política deben dirigirse al Asesor Jurídico al 787.728.1515, ext. 1221, o por correo electrónico a cameliac.fernandez@sagrado.edu, o al Oficial de Cumplimiento e Integridad.

Violaciones a esta Política

La Universidad del Sagrado Corazón se reserva el derecho de interpretar esta Política en su administración, implementación y aplicación. Cualquier violación de esta Política por parte de un estudiante, profesorado o personal o cualquier otra persona puede resultar en una acción disciplinaria que puede incluir la expulsión de la Universidad (estudiantes) o la terminación de la relación laboral (personal docente y administrativo) u otras acciones legales apropiadas.

Si existe alguna ambigüedad en cualquier disposición de esta Política, la Universidad se reserva la discreción de interpretarla de acuerdo con el propósito para el cual fue establecida, el impacto en las operaciones de la Universidad y la buena fe, a menos que cualquier ley establezca lo contrario.



Gilberto J. Marxuach Torrós
Presidente