SAGRADO
Universidad del Sagrado Corazón

Política sobre el Uso de Contraseñas ("*Passwords*") para el Acceso a los Recursos de Información y Tecnología

Efectivo: 2019.07.01

Propósito

Sagrado (también conocido como "Universidad") establece esta Política que describe los requisitos de la Universidad para la selección y el mantenimiento aceptable de una contraseña para maximizar la seguridad y minimizar el mal uso o el robo de las mismas. Las contraseñas son el método utilizado para la autenticación para el acceso a los recursos de tecnología e información ("IT") de Sagrado. Dado al uso de contraseñas débiles, la proliferación de programas que descifran contraseñas y la actividad de "hackers" y "spammers" maliciosos, las contraseñas también tienden a ser el método mas débil en asegurar data.

Aplicabilidad

Esta Política aplica a todos los estudiantes universitarios, facultad regular y parcial, empleados administrativos y de propuestas y a otros ("usuarios") con acceso y uso de los recursos de información y tecnología ("IT") de Sagrado.

Estándares de Contraseñas

1. En general, la fortaleza de las contraseñas aumenta dependiendo de su longitud y complejidad.

2. Contraseñas más complejas y reforzadas con medidas de seguridad adicionales deben ser utilizadas para situaciones de mayor riesgo que requieren de un nivel de protección elevado. Sistemas de alto riesgo incluyen, pero no están limitados a, sistemas que proveen: acceso a información sensitiva o crítica, control de acceso a datos compartidos, un sistema o aplicación con seguridad más frágil y las cuentas de administrador que mantienen el acceso de otras cuentas o proveen acceso a la infraestructura de seguridad.

3. Generalmente, las contraseñas deben satisfacer como mínimo los siguientes estándares:

- ❖ Ser de al menos diez (10) caracteres en longitud (para contraseñas de redes, 6 caracteres para correo de Google);
- ❖ Utilizar al menos una (1) letra minúscula;
- ❖ Utilizar al menos un (1) número;
- ❖ Utilizar al menos un (1) caracter especial (¡ @ # $ %);
- ❖ Utilizar al menos una (1) letra mayúscula;
- ❖ No debe incluir el primer nombre o el apellido del usuario;
- ❖ No debe ser similar a las últimas tres (3) contraseñas.

4. El número de Seguro Social y los números de tarjetas de crédito no pueden ser usados como nombre de usuario ("*username*") o contraseña para ayudar a prevenir el robo de identidad.

5. Las contraseñas son consideradas información sensitiva y por lo tanto nunca deberán ser escritas o almacenadas en línea al menos que estén adecuadamente seguras.

6. Las contraseñas no deberán ser incluidas en mensajes en correos electrónicos ni en otras formas de comunicación electrónica sin la autorización previa y por escrito del Principal Oficial de Información ("CIO").

7. Las contraseñas que se puedan usar para el acceso a información restricta o confidencial deben ser encriptas.

8. La misma contraseña no se puede utilizar para accesos externos a la Universidad.

9. Se recomienda que las contraseñas se cambien al menos cada sesenta (60) días calendario.

10. Las contraseñas individuales no se deben compartir con nadie incluyendo a los asistentes administrativos o el personal de la Unidad de Información y Tecnología Integrada ("ITI") sin la autorización previa y por escrito del CIO.

11. Las contraseñas compartidas que se utilizan para proteger dispositivos en red de conexión o en archivos compartidos tienen que tener una persona responsable del mantenimiento de esas contraseñas quien se asegurará que solo empleados autorizados tengan acceso a esas contraseñas.

12. Si una persona sospecha que una contraseña ha sido utilizada por alguien sin la autorización previa y por escrito del CIO, la contraseña tiene que ser cambiada de inmediato y notificar el incidente al CIO.

13. El CIO o la persona designada realizará periódicamente un monitoreo aleatorio para verificar la seguridad de las contraseñas. Si la contraseña es decodificada o adivinada durante las verificaciones, el dueño de la contraseña tendrá que cambiar la misma de inmediato.

Estándares de Computadoras de Oficina

En el caso de las contraseñas de las computadoras en las facilidades de Sagrado, también aplica lo siguiente.

1. Las contraseñas deben ser cambiadas al menos cada sesenta (60) días calendario.

2. El usuario tendrá hasta cinco (5) intentos para acceder a los recursos de IT.

3. Luego de cinco intentos fallidos, se bloqueará el sistema y será necesario que personal de ITI intervenga. Los intentos fallidos de acceso quedarán documentados y se retendrán por un mínimo de treinta (30) días calendario.

4. El personal de ITI tiene que inspeccionar regularmente las anotaciones de intentos fallidos e informar al CIO inmediatamente si hubiera una sospecha de una posible irregularidad.

Estándares de Cuentas Compartidas

En el caso de las contraseñas de los servidores, también aplica lo siguiente.

1. Las contraseñas de los servidores tienen que cambiarse cada vez que se cambie de personal de ITI.

2. Si se sospecha que una cuenta o contraseña ha sido utilizada por alguien sin autorización previa y por escrito del CIO, la contraseña tiene que ser cambiada de inmediato y notificar el incidente al CIO y las contraseñas que pudiesen potencialmente verse afectadas tienen que ser cambiadas inmediatamente.

3. El personal de ITI tendrá hasta cinco (5) intentos para acceder al servidor. Luego de cinco intentos fallidos, se bloqueará el sistema y será necesario que el CIO intervenga.

Los intentos fallidos de acceso quedarán documentados y se retendrán por un mínimo de treinta (30) días calendario.

4. El personal de ITI tiene que inspeccionar regularmente las anotaciones de intentos fallidos e informar al CIO inmediatamente si hubiera una sospecha de un posible ataque o una irregularidad.

Informar el Uso Indebido de las Contraseñas

Los usuarios tienen la responsabilidad de reportar sospechas de incidentes de uso indebido de las contraseñas y el acceso a la información electrónica 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 y Procedimientos. 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

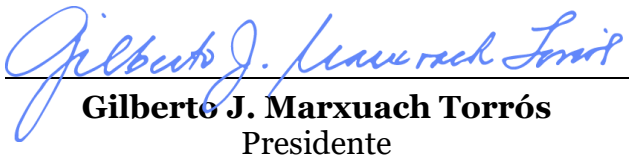
Las violaciones a esta Política deben dirigirse al Asesor Jurídico al 787.728.1515, ext. 1221, o por correo electrónico a cameliac.fernandez@sagrado.edu, o al Oficial de Cumplimiento e Integridad.

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