Política de seguridad de aplicaciones UTREEE

1. Visión general

Este documento describe una configuración de seguridad mínima requerida para enrutadores y conmutadores que se conectan a la red de producción UTREEE o se utilizan en una capacidad de producción dentro de UTREEE.

2. Propósito

El propósito de la Política de seguridad de aplicaciones es evitar la divulgación inadvertida de información confidencial o sensible, minimizar los riesgos para los usuarios y la Universidad y garantizar la disponibilidad de aplicaciones críticas. UTREEE centra sus esfuerzos en aplicaciones de seguridad que contienen o utilizan conjuntos de datos que contienen información / registros de estudiantes, información de identificación personal como números de seguro social o números de tarjetas de crédito y otras categorías de datos que están protegidos por leyes o regulaciones federales o estatales. En última instancia, para garantizar la disponibilidad y confiabilidad de las aplicaciones, todas las aplicaciones deben protegerse independientemente del tipo de información que utilicen.

3. Alcance

La Política de Seguridad de Aplicaciones se aplica tanto a las aplicaciones desarrolladas por el personal de la universidad como a las adquiridas de proveedores externos. Todas las aplicaciones están sujetas a esta política, independientemente de si la aplicación está alojada en equipos universitarios o en otro lugar.

4. Declaración de política

Para mantener el riesgo a un nivel aceptable, UTREEE se asegurará de que se implementen los controles de seguridad adecuados para cada aplicación. Se espera que los propietarios de datos, custodios, administradores de sistemas y desarrolladores de aplicaciones utilicen su juicio profesional para administrar los riesgos de la información, los sistemas y las aplicaciones que usan y respaldan. Todos los controles de seguridad deben ser proporcionales a los requisitos de confidencialidad, integridad y disponibilidad de los datos procesados por el sistema.

1. UTREEE IT, los departamentos individuales y los contratistas deben implementar estándares de seguridad de aplicaciones para tener controles efectivos sobre los sistemas que administran directamente.
    1. Si UTREEE IT administra un entorno o aplicación, UTREEE IT será responsable de implementar los controles de seguridad de la aplicación.

2. Si un departamento administra un entorno o una aplicación, ese departamento será responsable de implementar los controles de seguridad de la aplicación.
3. Si un contratista subcontratado administra un entorno o aplicación UTREEE para un departamento individual, el departamento debe asegurarse de que el contratista implemente los controles de seguridad de la aplicación.
4. El personal de UTREEE que contrate servicios de alojamiento de terceros (como servicios en la nube, SaaS o alojamiento administrado) para fines de investigación o aprobados debe:
    1. obtener la aprobación previa del Gerente de Recursos de Información o de la persona designada.
    2. no confíe a ese proveedor datos empresariales sensibles o confidenciales tal y como se define en la directiva de clasificación de datos.
    3. Los acuerdos de disponibilidad y soporte (por ejemplo, 24X7, 8-5, solo días laborables) deben estar en un nivel acorde con la disponibilidad esperada de las aplicaciones y deben comunicarse a UTREEE IT.

2. Las aplicaciones instaladas o que se están modificando deben seguir el ciclo de vida de la aplicación estandarizado establecido por el ciclo de vida del proyecto de TI de UTREEE.
3. Cada usuario individual (ya sea un desarrollador, administrador o usuario) debe tener un conjunto único de credenciales para acceder a una aplicación informática.
4. Los usuarios autenticados deben tener acceso a una aplicación informática y solo se les debe permitir acceder a la información que necesitan (principio de privilegio mínimo).
5. El propietario de los datos de la aplicación debe aprobar el establecimiento y cambio del acceso para un usuario o grupo.
6. Los desarrolladores deben seguir las mejores prácticas para crear aplicaciones seguras con la intención de minimizar el impacto de los ataques.
7. Los desarrolladores no deben desarrollar ni probar una aplicación con orígenes de datos de producción.
8. Los registros del servidor, la aplicación y los servicios web deben recopilarse y mantenerse en un formato visible durante un período de tiempo especificado por las regulaciones estatales aplicables.

9. Mantenga un inventario completo de todas las aplicaciones, para incluir los sistemas de autenticación y autorización, la clasificación de datos y el nivel de criticidad de cada aplicación.
10. Documente reglas y procesos claros para revisar, eliminar y otorgar autorizaciones.
11. Eliminar las autorizaciones críticas para el acceso a las solicitudes de las personas que han dejado la universidad, se han transferido a otro departamento o han asumido nuevas funciones laborales.

5. Distribución

Esta política se distribuirá a todo el personal de UTREEE responsable de la configuración, ingeniería y soporte del hardware de red.

6. Historial de versiones de directivas

Versión	Fecha	Descripción	Aprobado por
1.0	4/6/2019	Comenzó la política inicial	
1.1	5/12/2020	Revisión	
1.2	1/2/2022	Revisión	