Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente



SEGURIDAD DE LA

INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento, así como hacer obras derivadas, siempre y cuando tenga en cuenta citar la obra de forma específica.

Política de Separación de entornos

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 2.0 | **Categoría** | Política |
| **Última actualización** | 11/07/2022 | **Estado** |  |

# Objetivo

Reducir el riesgo de cambios o accesos no autorizados en el ambiente de producción.

# Alcance

Todas las aplicaciones informáticas, sean o no desarrollados por la organización, que requieran o sufran cambios a lo largo de su ciclo de vida. Incluye, sin ser taxativo, herramientas para la administración de la red, seguridad, incidentes, antivirus, gestión de parches, etc.

# Responsabilidades

**Responsable de seguridad de la información** debe velar por el cumplimiento de la presente política.

**Responsable de tecnología de la información** es el responsable de la gestión técnica que requiera el cumplimiento de la presente política. Es responsable por la validación final de los cambios realizados en las herramientas informáticas que no son aplicaciones del negocio, junto con los **responsables técnicos** de las áreas involucradas.

**Dirección** es responsable por otorgar los recursos necesarios para el cumplimiento de la presente política.

**Gerencias** son responsables por la validación final de los cambios funcionales en las aplicaciones informáticas del negocio.

El **personal y proveedores** deben cumplir con lo establecido en la presente política.

# Políticas relacionadas

Política de Gestión de cambios

# Descripción

La organización debe:

1. Definir un procedimiento formal de pasaje a producción y uno o más responsables de los pasajes a producción. Los pasajes a producción deben ser formalmente documentados según se establezca en el procedimiento.
2. Contar con ambientes separados para desarrollo, pruebas y producción.
3. Definir, en el marco de la política de gestión de cambios, un procedimiento formal para la gestión de los mismos. Los pasajes a producción deben estar alineados con la política y procedimiento de gestión de cambios. Los cambios siempre deben ser probados y aceptados previamente por personal de la organización designado por las gerencias.

Los sistemas o herramientas provistas por terceras partes también deben existir en dichos ambientes, al menos en ambiente de pruebas y producción, para que la organización pueda realizar los controles pertinentes antes de cualquier instalación, actualización y aplicación de cambios.

El ambiente de pruebas debe estar adecuadamente identificado de forma tal de diferenciarlo del ambiente de producción.

El personal que realiza las pruebas debe utilizar cuentas de usuario diferentes a las que posee en producción para la realización de éstas.

# Cumplimiento

Se destaca que el incumplimiento de la presente política aumenta la exposición de la información y el riesgo de tener un incidente de seguridad de la información. Ante la verificación de un incumplimiento la Dirección podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

# Historial de revisiones

|  |  |  |
| --- | --- | --- |
| **Fecha de revisión** | **Responsable** | **Resumen de cambios** |
|  |  |  |

