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 Finalización o cambio en la relación laboral

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 3.0 | **Categoría** | Política |
| **Última actualización** | 24/05/2022 | **Estado** |  |

# Objetivo

Establecer los lineamientos vinculados a seguridad de la información que se deberán seguir cuando el vínculo laboral de una persona con la organización finalice o si existe algún cambio en la relación funcional o contractual de la misma.

# Alcance

Todo el personal. independientemente de su rol funcional o su relación contractual.

# Responsabilidades

**Dirección** es responsable por difundir la presente política a todo el personal, independientemente del cargo que desempeñe.

**Responsable de seguridad de la información** debe velar por la difusión y cumplimiento de la política, siendo el Director, el responsable principal y último sobre dicho cumplimiento.

**Gestión Humana,** será responsable de comunicar en tiempo y forma las finalizaciones o cambios en los vínculos a la Unidad de Sistemas de Información y al Servicio de Seguridad del edificio, para que se deshabiliten los accesos lógicos y físicos que correspondan.

## Descripción

Deberán retirarse los permisos de accesos lógicos y físicos, y niveles de autorización a toda persona que finalice o cambie su relación funcional o contractual. Todo usuario de servicios que posean claves de acceso o niveles de autorización y que finalizan su relación laboral ya sea en forma definitiva o transitoria (ej. destitución, renuncia, licencia sin goce de sueldo por periodos prolongados, finalización de contrato); así como aquellos que cambien su relación funcional (ej. pase en comisión, comisión de servicio “permanente”, traslados en el inciso o entre incisos según artículos 57 y 58 de la ley 19121.) se le deberán retirar los permisos y niveles de autorización que ostenten hasta ese momento.

Este retiro deberá incluir:

1. Correo Institucional: se dará de baja o deshabilitar la cuenta de correo que a los fines institucionales se le otorgó oportunamente
2. Se eliminará el usuario de las listas de distribución de correo electrónico y grupos de trabajo.
3. Otras aplicaciones: el usuario será dado de baja de todos los accesos a las diferentes aplicaciones en las que se encuentre activo
4. Acceso a la red institucional: se bloqueará el acceso a NAS, cloud institucional, y toda otra forma de acceso a archivos, carpetas y otra información compartida.
5. Ingreso Físico: se le quitará a la persona el acceso a las diferentes áreas físicas a las que estaba autorizado a acceder.

La inhabilitación (ya sea temporal o definitiva) debe realizarse en el momento del cese, por lo cual las comunicaciones deberán efectuarse oportunamente, siendo responsables las áreas intervinientes.

Se debe definir un procedimiento específico que garantice el cumplimiento de la presente política.

# Cumplimiento

Se destaca que 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** |
|  |  |  |

