DGTIC UNAM

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

FUNDAMENTACIÓN

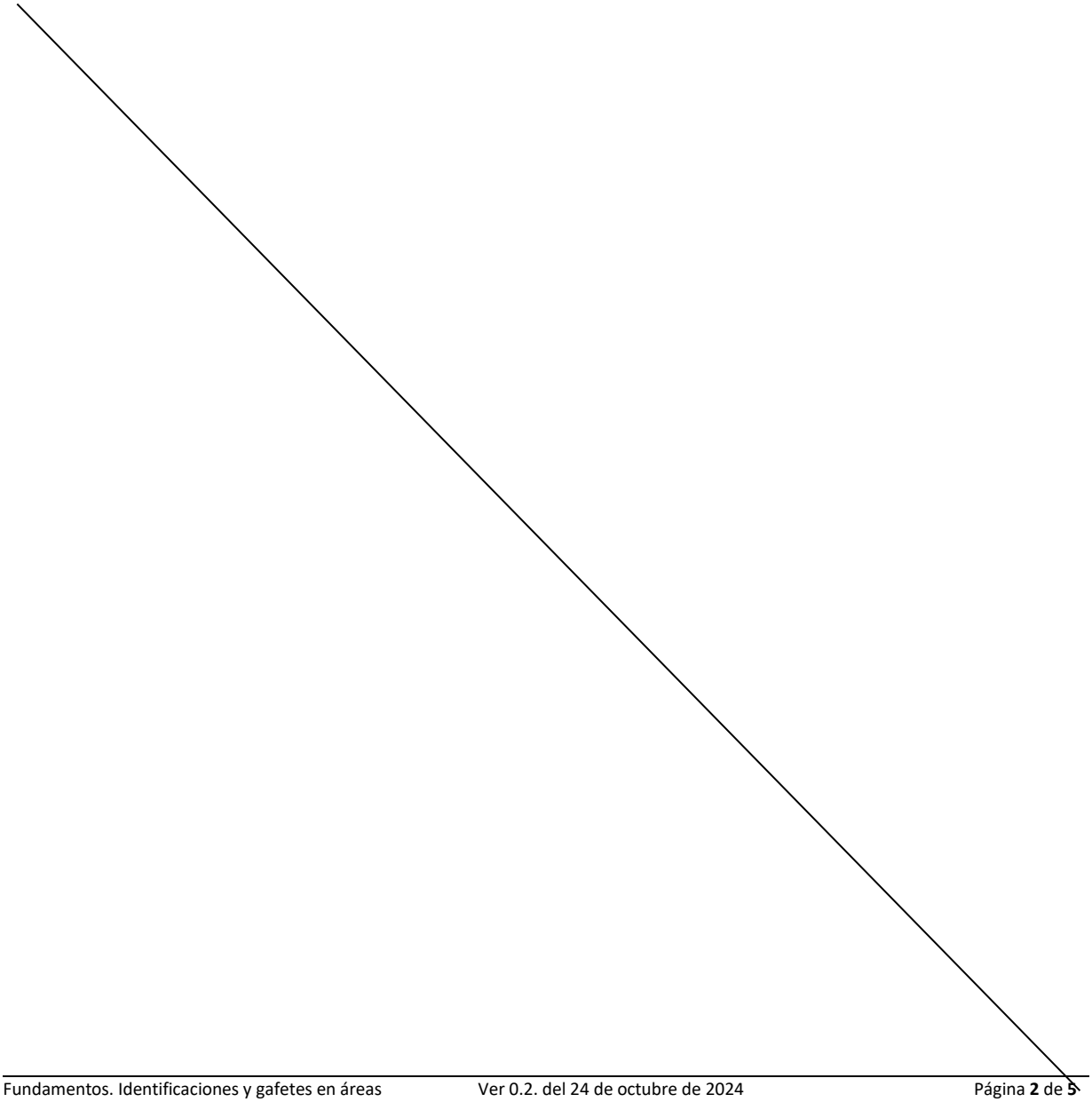
USO DE IDENTIFICACIONES Y GAFETES EN ÁREAS SEGURAS

Código:	20241024-DSSI-Presentación-Lineamientos-GafetesZonasSeguras		
Versión	0.2	**Fecha:**	24 de octubre de 2024
Vigencia	**Ciclo 1. 2022-2024**		
Creado / redactado por:	Fabián Romo Zamudio (FRZ)		
Edición / corrección:	Célica Martínez Aponte (CMA), Fabián Romo Zamudio (FRZ)		
Revisión / comentarios:	Lourdes Velázquez Pastrana (LVP)		
Aprobación:	Comité de Seguridad de la Información Comisión Local de Seguridad		
Del conocimiento de:	Dirección General de Cómputo y de Tecnologías de Información y Comunicación		
Nivel de confidencialidad:	2. Uso interno exclusivamente		

© 2021 - 2024. Universidad Nacional Autónoma de México.

Histórico de versiones

Fecha	Versión	Creado por	Descripción de cambios
7 octubre 2024	0.1	DSSI (CMA, FRZ)	Creación de documento a partir de la de la Política y los Procedimientos de Áreas Seguras para el Centro de Datos en el marco de la certificación ISO 27001:2022
24 octubre 2024	0.2	DSSI (CMA, FRZ)	Ajustes en áreas de uso y portabilidad de gafetes. Cuadrillas y áreas de alta seguridad.



© 2021 - 2024. Universidad Nacional Autónoma de México.
Dirección General de Cómputo y de Tecnologías de Información y Comunicación www.tic.unam.mx.

Fundamentación

En este documento se proponen las normas y procedimientos para el uso de identificaciones y gafetes dentro de las instalaciones de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).

Dado que la DGTIC proporciona servicios de misión crítica a la comunidad de la UNAM, así como resguarda y mantiene en operación activos informáticos que son indispensables para el adecuado cumplimiento de los objetivos institucionales, es indispensable garantizar los niveles adecuados de seguridad en las diversas áreas que componen la dependencia.

Esta necesidad se incrementó a raíz del proceso de certificación del Centro de Datos de la dependencia en las normas ISO 27001:2022 y TIA 942B, dado que ambas establecen requerimientos específicos para asegurar que tanto los componentes físicos como los elementos lógicos, así como los servicios asociados y los espacios en los cuales operan estén protegidos y con riesgos mínimos de afectación por casusa deliberada o fortuita.

Norma ISO 27001:2022

Si bien esta norma no menciona el tipo de gafetes o identificaciones de manera explícita, si establece controles en su Anexo A, el cual detalla un conjunto de elementos que pueden ser seleccionados e implementados por una organización para gestionar sus riesgos de seguridad de la información. Los controles que sustentan el uso de gafetes e identificaciones en esa norma son:

A.9 Controles de acceso: Este control se enfoca en garantizar que la información esté accesible solo a aquellos que estén autorizados a utilizarla. Dentro de este control, se pueden establecer subcontroles relacionados con:

- **Gestión de identidades y accesos**: Este subcontrol abarca la creación, modificación y eliminación de identidades (usuarios) y la asignación de derechos de acceso.
- **Control de acceso físico**: Aquí se establecen los mecanismos para controlar el acceso físico a las instalaciones, incluyendo el uso de identificaciones, tarjetas de acceso, biometría, etc.
- **Gestión de dispositivos**: Se establecen controles para gestionar el acceso a los sistemas y datos a través de dispositivos externos.

© 2021 - 2024. Universidad Nacional Autónoma de México.
Dirección General de Cómputo y de Tecnologías de Información y Comunicación www.tic.unam.mx.

Si bien los controles específicos se encuentran en el Anexo A de la norma, las cláusulas generales de la ISO 27001 que soportan la implementación de mecanismos para el uso de gafetes e identificaciones en las zonas seguras son:

- **Cláusula 5: Liderazgo:** La alta dirección debe demostrar compromiso con la seguridad de la información y establecer una política de seguridad que defina los requisitos para el control de acceso.
- **Cláusula 6: Planificación:** En esta cláusula se deben identificar los riesgos para la seguridad de la información y seleccionar los controles adecuados para tratarlos.
- **Cláusula 7: Soporte:** Se establecen los recursos necesarios para implementar y mantener el sistema de gestión de seguridad de la información (SGSI), incluyendo el personal y los procesos para gestionar el acceso.
- **Cláusula 8: Operación:** En esta cláusula se describen los procesos para operar, monitorear y mantener el SGSI, incluyendo el control de acceso.
- **Cláusula 9: Evaluación del desempeño:** Se establecen los procesos para evaluar el desempeño del SGSI, incluyendo auditorías internas y revisiones de gestión.

Por lo anterior, en el ámbito del ISO 27001:2022 es necesario el uso de gafetes e identificaciones para garantizar ante una revisión de auditoría y la continuidad de una certificación lo siguiente:

1. **Evaluación de riesgos:** Poder identificar los riesgos asociados al acceso no autorizado a las áreas seguras.
2. **Selección de controles:** Seleccionar los controles adecuados del Anexo A para mitigar los riesgos identificados, como el control A.9 antes mencionado.
3. **Desarrollo de procedimientos:** Para desarrollar procedimientos sobre la gestión de identidades, la asignación de derechos de acceso, el control de acceso físico y la gestión de dispositivos.
4. **Documentación:** Poder documentar todos los procesos y controles relacionados con el acceso a las áreas seguras.
5. **Capacitación:** Mantener informado al personal sobre los procedimientos de control de acceso y concientizar sobre la importancia de proteger la información**.**
6. **Monitoreo y revisión:** Dar continuo seguimiento al sistema de control de acceso y realizar revisiones periódicas para garantizar su eficacia**.**

© 2021 - 2024. Universidad Nacional Autónoma de México.
Dirección General de Cómputo y de Tecnologías de Información y Comunicación www.tic.unam.mx.

Norma TIA 942B

Si bien la norma TIA 942B no establece un requisito directo para el uso de gafetes e identificaciones en áreas seguras, su cumplimiento se vincula estrechamente con la norma ISO 27001:2022 para incrementar los niveles de seguridad en áreas de misión crítica, por medio de las Consideraciones de Diseño y los Procedimientos que se indican a continuación:

Consideraciones de diseño en TIA942:

- **Áreas de seguridad:** Se debe definir claramente las diferentes zonas de seguridad dentro del centro de datos (p. ej., sala de equipos, área de almacenamiento, acceso principal).
- **Controles de acceso:** Se deben implementar múltiples capas de control de acceso, como lectores de tarjetas, biometría, vigilancia por video y guardias de seguridad.
- **Registro de actividades:** Se deben mantener registros detallados de todas las actividades de acceso, incluyendo quién ingresó, cuándo y a dónde.

Procedimientos en TIA942:

- **Política de seguridad**: Debe existir una política de seguridad que establezca los requisitos para el control de acceso, la emisión de identificaciones y los procedimientos en caso de pérdida o robo.
- **Capacitación del personal:** Se debe capacitar al personal sobre los procedimientos de seguridad y la importancia de proteger el centro de datos.
- **Revisiones periódicas:** Se deben ejecutar revisiones periódicas de los controles de seguridad para garantizar su eficacia.

Por lo anterior, la Dirección de Sistemas y Servicios Institucionales, a través de la Coordinación de Servicios de Cómputo, desarrolló la Política de Áreas Seguras y el Procedimiento de Trabajo en Áreas Seguras, a efecto de cumplir con las citadas normas y que ello derive en el incremento en la confianza y certeza de seguridad y protección a los activos de información que la DGTIC tiene a su cargo y que son propiedad y de uso frecuente de la UNAM.

Se propone a la Comisión Local de Seguridad y al Comité de Seguridad de la Información estos lineamientos, en concordancia con la Política y Procedimiento mencionados, para garantizar que los procesos de certificación se cumplan a cabalidad.

© 2021 - 2024. Universidad Nacional Autónoma de México.
Dirección General de Cómputo y de Tecnologías de Información y Comunicación www.tic.unam.mx.