

Manual de políticas de seguridad de la información

De Wiki Ceibal

COPIA NO CONTROLADA

Cualquier copia impresa de este documento se considera **no controlada**, por lo que está prohibida la reproducción total o parcial sin la autorización del Responsable de Calidad.

Datos SGC	
Código	65344
Tipo	Normativa interna (NI)
Nombre	Manual de políticas de seguridad de la información
Revisión	98106 (2024-12) - 20230805
	Ubicación
Proceso	Gestión de la Seguridad de la Información
Subproceso	

Contenido

- 1 Objetivo
- 2 Alcance
- 3 Fundamento legal
- 4 Responsabilidades
- 5 Descripción
 - 5.1 Política de seguridad de la información
 - 5.2 Política de gestión de activos de información
 - 5.3 Política de uso aceptable de los sistemas de información e infraestructura
 - 5.4 Política de uso aceptable de Internet
 - 5.5 Política de teletrabajo
 - 5.6 Política de seguridad de la información para proveedores
 - 5.7 Política de control de acceso
 - 5.8 Política sobre el uso de controles criptográficos
 - 5.9 Política de gestión de claves de cifrado y certificados SSL
 - 5.10 Política de intercambio de información
 - 5.11 Política de desarrollo seguro
 - 5.12 Política de gestión de software de base y aplicaciones
 - 5.13 Política de clasificación de activos de información
 - 5.14 Política de gestión de incidentes
 - 5.15 Política de continuidad del negocio y recuperación ante desastres
 - 5.16 Política de respaldos
 - 5.17 Política de gestión de ambientes
 - 5.18 Política de seguridad en la nube
 - 5.19 Política de destrucción de la información
 - 5.20 Política de escritorio y pantallas limpias
- 6 Glosario y abreviaturas
- 7 Vigencia
- 8 Cómo se realiza la regulación

Objetivo

El objetivo del presente Manual de Políticas de Seguridad de la Información es establecer los lineamientos y el marco de referencia para la exitosa implementación del SGSI en Centro Ceibal.

Alcance

El Manual de Políticas de Seguridad de la Información establece el marco para el correcto desarrollo de todos los procedimientos, instructivos y demás documentación asociados a la implementación del SGSI. Alcanza a todos los/as funcionarios/as de Centro Ceibal sin importar la modalidad de contratación, los proveedores y demás partes involucradas que interactúan con activos de información de Centro Ceibal.

Fundamento legal

El Manual de Políticas de Seguridad de la Información sigue las recomendaciones establecidas en el MCA (Marco de Ciberseguridad de AGESIC) (<https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad>)

A su vez, está alineado a las buenas prácticas internacionales recomendadas por:

- NIST CSF
- ISO 27001
- ISO 55000
- ISO 22300

El Manual de Políticas de Seguridad de la Información también cumple con la normativa nacional en materia de ciberseguridad, que incluye entre otros:

- Ley 18331 (Protección de Datos Personales)
- Ley 18381 (Derecho al Acceso de la Información Pública)
- Decreto 451/009 (Centro Nacional de Respuesta a Incidentes de Seguridad Informática, Funcionamiento y Organización)
- Decreto 452/009 (Administración Pública - Política de Seguridad de la Información)
- Decreto 178/013 (Intercambio de Información)

Responsabilidades

Los roles y responsabilidades en el Marco del SGSI (Sistema de Gestión de Seguridad de la Información) se encuentran en el Manual de Gestión Integrado

En relación a las políticas de Seguridad de la Información, se detallan las siguientes responsabilidades:

Directorio

Aprueba la Política General de Seguridad de la Información y vela por el cumplimiento de la normativa y legislación vigente al respecto, poniendo a disposición para ello los recursos necesarios para dar cumplimiento a lo establecido. Delega en el Comité de Seguridad de la Información (CSI) la aprobación del presente Manual de Políticas de Seguridad de la Información.

Comité de Seguridad de la Información

Aprueba el presente Manual de Políticas de Seguridad de la Información. Establece las responsabilidades específicas para su ejecución, control, monitoreo y mejora.

Jefe de Seguridad de la Información

Colabora en la elaboración del presente Manual de Políticas de Seguridad de la Información. Elabora la documentación necesaria para la correcta implementación de las políticas y vela por el cumplimiento de las mismas.

Descripción

Política de seguridad de la información

La Dirección de Centro Ceibal reconoce la importancia de identificar y proteger los activos de información del Centro. Para ello sigue lo establecido en la Política de Seguridad de la Información

Política de gestión de activos de información

Esta política establece las pautas para la gestión de los activos de información claves para el desempeño de la institución, ya que estos contienen datos que pueden representar una ventaja competitiva y que requieren ser protegidos.

Para el buen desempeño de su gestión, es imperativo que la organización los identifique, clasifique, controle, resguarde y determine su disposición final, según la normativa aplicable en la materia.

La gestión de los activos de información requiere implementar acciones concretas en todo el ciclo de vida de estos, tales como:

- Generar y mantener actualizado periódicamente un inventario de los activos de información de la institución.
- Definir los propietarios y custodios de los activos de información.
- Establecer los criterios de clasificación de los activos de información.
- Clasificar los activos de información de acuerdo a su relevancia.
- Establecer e implementar procedimientos de protección de los activos de información de acuerdo a su clasificación, independientemente del soporte de estos.
- Establecer e implementar procedimientos de protección y control específicos para aquellos activos que sean transportados o transmitidos a terceras partes.
- Establecer e implementar procedimientos de devolución y destrucción segura de los activos de información.
- Regular el acceso y la utilización de todos los activos de información.
- Cumplir con la normativa interna y de los organismos reguladores y de control.

Política de uso aceptable de los sistemas de información e infraestructura

Esta política establece los criterios generales que permiten el uso aceptable de los sistemas de información e infraestructura y regula la utilización apropiada de sus componentes, así como la implantación de aquellas medidas necesarias para resguardar la confidencialidad, integridad y disponibilidad de la información.

Esta política comprende el uso de los sistemas de información e infraestructura utilizados por Centro Ceibal, sean o no propiedad de este e independientemente de su localización física.

Para un apropiado desarrollo de la política, se debe:

- Definir los procedimientos que establezcan un uso adecuado de los sistemas de información y la infraestructura informática, de manera que estén alineados con los cometidos institucionales de Centro Ceibal, sus objetivos, sus políticas y la normativa vigente.
- Establecer las medidas de seguridad necesarias para permitir la correcta autenticación y autorización de las personas usuarias a los sistemas de información e infraestructura informática y denegar el acceso a personas u organizaciones no habilitadas.
- Otorgar a las personas usuarias el acceso a los sistemas de información e infraestructura informática de Centro Ceibal en los casos donde exista una necesidad fundamentada y bajo los mínimos privilegios necesarios para el desarrollo de su función actual y futura.
- Establecer procedimientos para el acceso remoto a los sistemas, velando por el mantenimiento de estándares mínimos de seguridad.
- Establecer que todo el personal vinculado a Centro Ceibal debe asumir un compromiso de confidencialidad respecto a la información a la que por su relación con Centro Ceibal tenga acceso.
- Establecer que solo el personal habilitado puede instalar, configurar, mantener y dar de baja los sistemas de información e infraestructura informática de Centro Ceibal.
- Velar porque las actividades desarrolladas por las personas usuarias no comprometan la confidencialidad, disponibilidad o integridad de los sistemas de información o infraestructura de Centro Ceibal.
- Establecer que la tecnología de Centro Ceibal no puede utilizarse para fines ilegales o prohibidos por la normativa interna o externa.
- Cumplir con la normativa interna y de los organismos reguladores y de control.

Política de uso aceptable de Internet

Esta política establece aspectos específicos adicionales a la Política de uso aceptable de los sistemas de información e infraestructura que regulen el uso de Internet y los sistemas que lo componen, entre los que se encuentran el correo institucional, las redes sociales y la mensajería instantánea, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la institución.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Monitorear e identificar el acceso y uso de los sistemas informáticos que componen los servicios de Internet y proceder a su habilitación o bloqueo.
- Establecer las pautas que debe cumplir la información entrante y saliente de Centro Ceibal a través de Internet e implementar los controles y medidas necesarios a nivel de infraestructura y sistemas de información para cumplir con dichas pautas.
- Formular un Código de uso de sistemas informáticos que incluya los criterios adecuados para el uso de Internet de acuerdo a las buenas prácticas y estándares de la industria.
- Establecer que las personas usuarias de los servicios de Internet deben respetar el Código de uso de sistemas informáticos y el marco normativo vigente, utilizando estos servicios sin afectar la operativa ni la seguridad de la información de Centro Ceibal.
- Elaborar y difundir los documentos necesarios para que las personas usuarias de Internet puedan cumplir con lo establecido en la presente política.

Política de teletrabajo

Esta política establece los criterios generales para realizar un teletrabajo seguro, de manera de proteger la información y los activos de Centro Ceibal. Detalla la infraestructura, procesos, controles y gestión de riesgos adecuados para poder desarrollar un teletrabajo alineado a las metas estratégicas.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Realizar una definición del trabajo permitido, los horarios correspondientes, la clasificación de la información que se puede realizar y los sistemas y servicios internos a los que el/la teletrabajador/a se encuentra autorizado/a a acceder.
- Establecer la infraestructura y procedimientos necesarios para poder brindar una conectividad segura a los/as teletrabajadores/as. Esta deberá incluir las configuraciones y soluciones necesarias para que los/as usuarios/as puedan acceder a los sistemas de manera segura.
- Establecer los requisitos de la seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a ser accedida y transmitida sobre los enlaces de comunicación y la criticidad del sistema interno.
- Establecer las medidas necesarias para mantener la seguridad física de la información en los casos que la confidencialidad de la información lo amerite.
- Establecer los controles necesarios a realizar sobre los dispositivos móviles, tomando en cuenta los riesgos asociados al uso de estos dispositivos en entornos desprotegidos. Entre los requisitos a considerar se deberían incluir:
 - El registro de los dispositivos móviles
 - Los requisitos de protección física
 - La restricción de instalación de software y los requisitos de actualizaciones
 - Los controles de acceso
 - Técnicas criptográficas
 - Protección contra software malicioso
 - Desactivación, eliminación o bloqueo a distancia
 - Copias de seguridad
- Establecer los casos en los que se permitirá el uso de equipamiento de propiedad privada y las recomendaciones que se deben seguir en el uso de este tipo de dispositivos.
- Establecer las reglas y directrices del acceso de la familia y visitas al equipamiento y la información contenida.
- Establecer las consideraciones de protección ante software malicioso y filtrados de contenidos (por ejemplo cortafuegos) en equipamiento de propiedad privada a ser usado para el teletrabajo.
- Establecer las directrices para el suministro de soporte y mantenimiento de hardware y software de los equipos usados para el teletrabajo.
- Tomar en cuenta las consideraciones legales pertinentes de cumplimiento con las leyes y regulaciones del teletrabajo y la provisión de seguros en caso de que sean necesarios.
- Considerar las posibles responsabilidades en cuanto a licencias de software en equipos de trabajo de propiedad privada de los/as teletrabajadores/as.
- Establecer los elementos de auditoría, monitoreo y control de seguridad de acuerdo a lo que se haya definido.
- Establecer los procedimientos necesarios para realizar respaldos adecuados y mantener la continuidad del negocio. Se deberán establecer también los procedimientos necesarios para asegurar el cumplimiento y desarrollo de los procesos estratégicos.
- Considerar la revocación de autoridad y de los derechos de acceso y el regreso de los equipos asociados cuando las actividades de teletrabajo finalizan.

Política de seguridad de la información para proveedores

Esta política establece los criterios generales para proteger los activos de información que son accesibles por los proveedores. Establece los requisitos y controles para mitigar los riesgos asociados con el acceso de los proveedores a la información, a través de procesos y procedimientos propios y otros que se deberán requerir al proveedor.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Identificar, documentar y clasificar los proveedores de acuerdo a la información a intercambiar, los procesos de negocios y los riesgos involucrados.
- Generar los procedimientos y estándares a cumplir por los proveedores para asegurar la seguridad de la información.
- Establecer los requisitos de seguridad de la información que se deberán cumplir en los acuerdos firmados con los proveedores, donde se deberán incluir:
 - Acuerdos de Confidencialidad que garantice los requisitos de confidencialidad de Centro Ceibal.
 - Acuerdos de Nivel de Servicio (SLA) que cumplan con los requisitos de negocio y seguridad de Centro Ceibal.
 - Descripción de la información a ser proporcionada/accedida y los métodos de proporcionar/acceder a la información.
 - Clasificación de la información de acuerdo al esquema de clasificación de Centro Ceibal y mapeo entre los esquemas de clasificación de Centro Ceibal y el proveedor en caso de ser necesario.
 - Requisitos legales y reglamentarios a cumplir, como por ejemplo la protección de datos personales, los derechos de autor y la propiedad intelectual.
 - Controles de común acuerdo entre las partes, como por ejemplo control de acceso, evaluación de desempeño, supervisión y auditoría.
 - Requisitos y procedimientos de gestión de incidentes.
 - Requisitos de capacitación y sensibilización para los procesos asociados a la seguridad, como por ejemplo gestión de incidentes y procedimientos de autorización.
 - Normas y controles para la subcontratación en caso de que apliquen.
 - Requisitos de selección del personal del proveedor en caso de que apliquen, incluyendo los procedimientos de notificación.
 - La implementación de procesos para la gestión de la información y el ciclo de vida de los componentes de tecnología y los riesgos de seguridad asociados, incluyendo la gestión de los riesgos de componentes obsoletos debido a los avances tecnológicos o cambios en los proveedores.
 - Controles para propagar y hacer un seguimiento adecuado de las prácticas y requisitos de seguridad de la información en la cadena de suministro en caso de que aplique.

- Garantías de que la información entregada y los productos de tecnología funcionan tal como se esperaba desde el punto de vista de la seguridad de la información.
 - El derecho a auditar los procesos y controles de los proveedores relacionados con el acuerdo.
 - Mecanismos de resolución de defectos y posibles conflictos.
 - Las obligaciones del proveedor de cumplir con las políticas y requisitos de seguridad de la información de Centro Ceibal.
- Realizar el seguimiento, revisar y auditar regularmente la prestación de servicios del proveedor, verificando el cumplimiento de los acuerdos acordados y los requisitos de seguridad de la información de Centro Ceibal.
 - Establecer el nivel de resiliencia y si es necesario, los acuerdos de recuperación y contingencia para asegurar la disponibilidad de la información y los procesos que garantizan la seguridad de la información.
 - Gestionar los cambios a la prestación de servicios de los proveedores teniendo en cuenta la criticidad de la información, sistemas y procesos de negocios involucrados y la reevaluación de riesgos.
 - Gestionar adecuadamente las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otro componente que sea necesario mover, de manera de garantizar que la seguridad de la información se mantiene durante todo el período de transición.
 - Cumplir con la normativa interna y de los organismos reguladores y de control.

Política de control de acceso

Esta política establece los criterios generales para el control de acceso a los activos de información, aplicaciones y demás componentes, basado en los objetivos de negocio de Centro Ceibal y en la seguridad de la información, de manera de velar por la confidencialidad, integridad y disponibilidad de los activos.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Establecer los estándares y los controles de acceso (tanto físicos como lógicos) de la información, en función de los requisitos de seguridad de las aplicaciones, la clasificación de la información y la gestión de riesgos.
- Gestionar los derechos de acceso en un entorno distribuido y de redes que reconozca todos los tipos de conexión disponibles.
- Separar los distintos roles de control de acceso, de manera de gestionar adecuadamente los riesgos.
- Establecer los procedimientos para las autorizaciones formales de pedidos de acceso y gestionar las altas, bajas y modificaciones de usuarios de los sistemas.
- Restringir el acceso a la información y funciones de las aplicaciones siguiendo las pautas establecidas en los roles de los usuarios.
- Establecer los métodos de autenticación de acuerdo a la criticidad de la información y los riesgos asociados, fijando las directivas que salvaguarden la confidencialidad, integridad y disponibilidad de la información.
- Registrar todos los eventos relevantes relativos al uso y gestión de las identidades de usuario y la información de autenticación.
- Restringir y monitorear los roles de acceso privilegiados.
- Restringir y controlar el uso de programas utilitarios privilegiados.
- Revisar periódicamente los derechos de acceso de los usuarios.
- Restringir y controlar el acceso al código fuente de las aplicaciones de manera de garantizar un desarrollo seguro, siguiendo lo establecido en la Política de desarrollo seguro.
- Capacitar y concientizar a los usuarios en el uso responsable de la información de autenticación.
- Asegurar la confidencialidad y privacidad de la información cumpliendo con la normativa vigente y las obligaciones contractuales, limitando de manera adecuada el acceso a la información y los servicios.
- Cumplir con la normativa interna y de los organismos reguladores y de control.

Política sobre el uso de controles criptográficos

Esta política establece los criterios generales para el uso de controles criptográficos para la protección de la confidencialidad, integridad y disponibilidad de la información.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Establecer las características y los requisitos que deben cumplir los controles criptográficos en Centro Ceibal, que incluyan los algoritmos de cifrado, su utilización y uso seguro, longitud de las claves y demás definiciones técnicas relacionadas en función de diversos escenarios y ámbitos de uso, riesgos asociados y la información a proteger.
- Establecer los responsables del diseño, implementación, gestión y disposición de los controles criptográficos en Centro Ceibal.
- Establecer las condiciones y requisitos mínimos que deben cumplir los proveedores y agentes externos en sus propios mecanismos criptográficos y en los productos y servicios que ofrecen en función de los estándares establecidos por Centro Ceibal.
- Establecer los procedimientos para auditar y registrar las actividades relacionadas con los controles criptográficos de forma de asegurar que se cumpla con las dimensiones de la seguridad mencionadas en el enunciado de la presente política y con las definiciones de los dos primeros párrafos.
- Considerar y respetar las regulaciones y restricciones nacionales e internacionales que aplican al uso de controles criptográficos.

Política de gestión de claves de cifrado y certificados SSL

Esta política establece los criterios generales para el uso, protección y duración de las claves criptográficas a través de su ciclo de vida, así como de los certificados SSL.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Establecer los procedimientos para realizar una adecuada gestión de las claves criptográficas incluyendo su generación, almacenamiento, archivo, respaldo, recuperación, distribución, retiro, revocación y destrucción, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información.

- Establecer los procedimientos para auditar y registrar las actividades relacionadas con la gestión de las claves, para asegurar que se cumpla con las dimensiones de la seguridad mencionadas en el párrafo anterior.
- Establecer los procedimientos para realizar una adecuada gestión de los certificados SSL, que incluya su correcta adquisición, almacenamiento, respaldo, recuperación, retiro, revocación y vencimiento, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información.
- Establecer los procedimientos para auditar y registrar las actividades relacionadas con la gestión de las claves y los certificados SSL para asegurar que se cumpla con las dimensiones de la seguridad mencionadas en los párrafos anteriores.
- Establecer los procedimientos, los requisitos y las condiciones adecuadas para el caso de tener que compartir las claves o certificados SSL con proveedores o agentes externos a Centro Ceibal.
- Establecer los estándares y acuerdos contractuales respecto al servicio que deben cumplir los proveedores de certificados externos.
- Cumplir con la normativa interna y de los organismos reguladores y de control relativa a este tema.

Política de intercambio de información

Esta política establece los criterios generales para mantener la seguridad de la información, ya sea internamente o con cualquier entidad externa, de manera de garantizar la confidencialidad, integridad y disponibilidad de la información transferida.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Establecer y comunicar los estándares, criterios de seguridad y calidad en el intercambio de información a través de cualquier medio de comunicación, con la finalidad de proteger la transferencia de información de su interceptación, copiado, modificación, desviación y destrucción.
- Establecer acuerdos sobre la transferencia de información con cualquier entidad externa que incluyan:
 - Responsabilidades y compromisos de las distintas partes intervinientes.
 - Procedimientos para asegurar la trazabilidad, el no repudio y niveles aceptables del control de acceso.
 - Aseguramiento de la cadena de custodia mientras la información se encuentra en tránsito.
 - Normas técnicas para el empaquetado, grabación, lectura y escritura de la información.
- Establecer las responsabilidades de los/as funcionarios/as, terceras partes y cualquier otro/a usuario/a de manera de asegurar la confidencialidad, integridad y disponibilidad de la información en tránsito.
- Usar las técnicas criptográficas adecuadas para asegurar la confidencialidad, integridad y disponibilidad de la información, siguiendo lo establecido en la Política de controles criptográficos.
- Elaborar y actualizar los acuerdos de confidencialidad con funcionarios/as y partes externas que incluyan:
 - Alcance de la información a ser protegida.
 - Duración del acuerdo y acciones requeridas al finalizarlo.
 - Responsabilidades por parte de las partes intervinientes.
 - Acciones a tomar en caso de incumplimiento.
 - El uso permitido respecto a la información y los derechos de las partes intervinientes.
 - Requerimientos de auditoría y trazabilidad.
- Establecer los controles necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información transmitida a través de mensajería electrónica, que incluyan:
 - El correcto direccionamiento y transporte de los mensajes.
 - Establecer y asegurar la confiabilidad, disponibilidad y niveles de autenticación necesarios de acuerdo al nivel de seguridad de la red y servicios usados.
 - Aprobaciones necesarias al usar servicios tercerizados y consideraciones legales pertinentes.
- Establecer los controles necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información transmitida a través de medios físicos, que incluyan:
 - Establecer y mantener el inventario de mensajeros y transportes autorizados.
 - Establecer los mecanismos de protección de la información a transportar, como por ejemplo: embalajes, registros, identificaciones, protecciones térmicas y aislaciones correspondientes.
- Cumplir con la normativa interna y de los organismos reguladores y de control.

Política de desarrollo seguro

Esta política establece los criterios generales para el desarrollo seguro del software de Centro Ceibal, ya sea interno o externo a través de la contratación de proveedores, de manera de garantizar la confidencialidad, integridad y disponibilidad de la información.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Establecer los estándares, criterios de seguridad y calidad en el desarrollo del software.
- Establecer la infraestructura de soporte de operaciones para asegurar el desarrollo seguro y correcto del software a través de una separación de ambientes de desarrollo y pruebas que permita la incorporación de modificaciones y/o actualizaciones con una adecuada gestión de los riesgos.
- Establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad, siguiendo las pautas publicadas por los organismos especializados (CVE, OWASP) o detectadas por cualquier usuario y proponiendo las medidas de remediación necesarias.

- Desarrollar un plan de actualizaciones para el software desarrollado, asegurando que queden instaladas las últimas versiones y parches más recientes, con el fin de evitar la explotación de vulnerabilidades.
- Establecer los estándares y procedimientos necesarios para una adecuada documentación del software. La documentación deberá, entre otras características, ser generada durante el ciclo de vida de desarrollo, ser actualizada frente a cambios, ser revisada por usuarios finales y ser almacenada y difundida adecuadamente.
- Incluir la seguridad en la planificación y diseño de los proyectos, como parte integral de los requerimientos de desarrollo.
- Establecer los requerimientos de seguridad de los distintos componentes de los proyectos de desarrollo, tomando en cuenta la criticidad de los activos y la información involucrada. Para preservar la confidencialidad, integridad y disponibilidad de la información de acuerdo a la criticidad definida, se deberán establecer las métricas y los controles adecuados, como por ejemplo, los definidos en la Política de controles criptográficos.
- Establecer los estándares de codificación segura que deben regir el desarrollo del software, siguiendo las buenas prácticas recomendadas a nivel internacional (por ejemplo OWASP).
- Establecer los estándares técnicos y de procesos que componen los sets de pruebas del desarrollo de software, siguiendo las metodologías y estándares recomendados por los organismos especializados (ej. ISO 29119, ISTQB). Las pruebas deberán verificar los requerimientos de seguridad del software y ser lo más automatizadas y completas posible.
- Establecer los procedimientos y normas de seguridad que permitan auditar, medir y revisar los controles de seguridad definidos en la etapa de diseño, manteniendo un registro de los resultados y acciones tomadas.
- Establecer los estándares, requisitos, certificaciones y otras características que deben cumplir los proveedores externos para cumplir con las exigencias de la presente política y la Política de gestión de proveedores, de manera de asegurar la confidencialidad, integridad y disponibilidad de la información.
- Cumplir con la normativa interna y de los organismos reguladores y de control.

Política de gestión de software de base y aplicaciones

Esta política establece los criterios generales para que los procesos de adquisición, desarrollo, instalación, configuración, actualización y mantenimiento de sistemas informáticos de Centro Ceibal (software de base y aplicaciones), garanticen la confidencialidad, integridad y disponibilidad de la información que contienen.

Las acciones necesarias para la correcta implementación de la política incluyen:

- Establecer y comunicar los estándares, requisitos, certificaciones y otras características que deben cumplir los proveedores externos para poder participar en los procesos de adquisición y mantenimiento de sistemas informáticos.
- Establecer y comunicar los estándares, requisitos, certificaciones y otras características que deben cumplir los proveedores externos para poder participar en los procesos de instalación, configuración y actualización de sistemas informáticos.
- Regular la relación con proveedores externos de sistemas informáticos, estableciendo las responsabilidades y actividades necesarias para poder cumplir con un nivel de servicio aceptable de acuerdo a los criterios establecidos por Centro Ceibal.
- Establecer y comunicar los estándares, requisitos, certificaciones, actualizaciones y otras características que deben cumplir los sistemas informáticos internos y externos de Centro Ceibal.
- Establecer y comunicar los estándares, requisitos, certificaciones y otras características que deben cumplir los dispositivos informáticos para conectarse e intercambiar información con los sistemas de Centro Ceibal.
- Implementar los procesos necesarios para que las comunicaciones de Centro Ceibal cumplan con los criterios de confidencialidad, integridad y disponibilidad de la información.
- Establecer y comunicar los estándares técnicos y de procesos que debe cumplir el desarrollo interno y externo de aplicaciones de acuerdo a la Política de desarrollo seguro.
- Cumplir con la normativa interna y de los organismos reguladores y de control.

Política de clasificación de activos de información

Esta política establece los criterios de clasificación de los activos de información. Los activos de información tienen distintos niveles de confidencialidad de acuerdo a quienes pueden crear, consultar, modificar y eliminarlos. El nivel de confidencialidad es uno de los factores determinantes de la criticidad de los activos y en consecuencia sobre los controles de acceso y las medidas de resguardo y gestión de riesgos que sobre los mismos se deben establecer.

Para el **uso interno** de los activos de información, Centro Ceibal establece criterios de clasificación de la información de acuerdo al nivel de confidencialidad requerido.

Respecto a la transparencia y publicidad de la información (**uso externo**) Centro Ceibal cumple con toda la normativa vigente establecida en relación al acceso de la información pública, de manera de promover la transparencia estatal y garantizar el derecho de acceso de todas las personas. Para cumplir con estos requerimientos Centro Ceibal clasifica la información siguiendo las pautas establecidas en la normativa vigente:

- **Información pública:** Toda la información es por defecto pública, salvo que se trate de información secreta, reservada o confidencial, de acuerdo con lo dispuesto en la Ley N° 18.381.
- **Información reservada:** Se considera como reservada toda información que:
 - a. comprometa la seguridad pública o la defensa nacional,
 - b. menoscabe la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de reservado a Estado uruguayo.
 - c. dañe la estabilidad financiera, económica o monetaria del país,
 - d. ponga en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona,
 - e. suponga una pérdida de ventajas competitivas para Centro Ceibal o pueda dañar su proceso de producción,

- f. desproteja descubrimientos científicos, tecnológicos o culturales desarrollados o en poder de Centro Ceibal,
- g. afecte la provisión libre y franca de asesoramientos, opiniones o recomendaciones que formen parte del proceso deliberativo de Centro Ceibal hasta que sea adoptada la decisión respectiva, la cual deberá ser documentada.

Dicha información, permanecerá con tal carácter hasta un período de quince años desde su clasificación. Además, su carácter pasará ser público cuando se extingan las causas que dieron lugar a su clasificación. Sólo se ampliará el periodo de Reserva sobre cierta documentación cuando permanezcan y se justifiquen las causas que le dieron origen.

- **Información confidencial:** Se considera como confidencial toda información que:
 - a. Sea entregada en tal carácter a los sujetos obligados, siempre que:
 - Refiera al patrimonio de la persona,
 - Comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica, que pudiera ser útil para un competidor,
 - Esté amparada por una cláusula contractual de confidencialidad;
 - b. Los datos personales que requieran previo consentimiento informado.

Los documentos o secciones de documentos que contengan estos datos. La documentación clasificada como información confidencial o reservada deberá tener incorporada una leyenda indicativa de su carácter confidencial o reservada.

- **Información secreta:** Es aquella que las diferentes leyes han indicado como secreta. En este caso es el legislador quien lo ha definido así; por lo tanto, no se debe clasificar la información como secreta, aunque sí es conveniente rotular los documentos que contienen información secreta.

Sin perjuicio de la clasificación anterior, a los efectos del acceso y utilización de la información por parte de personal vinculado a Centro Ceibal (empleados/as dependientes o personas físicas prestadoras de servicios personales: consultores/as, asesores/as; en adelante, “personal”), la información se cataloga de acuerdo a los siguientes criterios:

- **Información accesible a todo el personal:** Información de acceso y utilización por todo el personal de Centro Ceibal. Se trata de toda aquella información que no es clasificada en alguna de las restantes dos categorías.
- **Información de uso interno de cada proceso:** Toda información que se dispone en cada uno de los procesos. Esta categoría incluye los datos que solo pueden ser entendidos y operados por el personal que los genera, los gestiona y participa del proceso. No puede ser compartida con otras áreas ajenas al proceso, salvo autorización del responsable del proceso.
- **Información restringida:** Es la información que solo puede ser accedida y gestionada por el Consejo de Dirección, Gerencia General y quien estos dispongan. Esta categoría incluye información estratégica para la toma de decisiones institucionales o información que por su grado de privacidad requiere que esté disponible solo para el Consejo de Dirección y Gerencia General y quienes estos dispongan en cada caso.

El personal de Centro Ceibal deberá ajustarse a lo aquí establecido, así como a lo dispuesto en el punto 2.4. Confidencialidad del Código de Ética: “Los integrantes de Centro Ceibal están obligados a la discreción y a la confidencialidad, no pudiendo manifestarse en nombre de Centro Ceibal, ni difundir o utilizar con ningún motivo, en su beneficio propio o en el de terceros, la información confidencial, inédita o privilegiada obtenida en el ejercicio de sus funciones, tanto sobre hechos, datos o actividades de la organización como de sus beneficiarios, a menos que sea autorizado expresamente por el Consejo Directivo. El conocimiento, las tecnologías y metodologías generadas u obtenidas en la institución son propiedad intelectual de Centro Ceibal. Hasta no ser del dominio público, no deberán usarse o traspasarse para fines particulares o en provecho propio tecnologías, metodologías, know-how u otras informaciones de propiedad de Centro Ceibal o por ella desarrolladas u obtenidas, sin autorización expresa del Consejo Directivo. El incumplimiento de la obligación de confidencialidad determinará el despido por notoria mala conducta, sin derecho a indemnización por despido y aginaldo”.

Política de gestión de incidentes

Esta política establece los lineamientos generales para gestionar adecuadamente los eventos e incidentes de seguridad de la información e incluye el reporte oportuno de los usuarios y el análisis de la información para reducir los riesgos asociados, con el fin de prevenir y limitar su impacto.

Las acciones necesarias para una adecuada gestión y resolución de los incidentes de seguridad involucran:

- Adoptar medidas para la detección de eventos de seguridad de la información.
- Implementar canales para la recepción de reportes de eventos de seguridad de la información.
- Analizar los eventos de seguridad de la información para determinar si se trata de un incidente de seguridad de la información.
- Clasificar y priorizar los incidentes de seguridad de la información.
- Implementar procedimientos de reporte y respuesta a incidentes y eventos para contenerlos y mitigarlos. La gestión de cada incidente debe contemplar todas las etapas de su ciclo: reporte, asignación, tratamiento, respuesta y cierre.
- Explicitar de manera clara y sin ambigüedades los mecanismos y métodos para realizar los reportes de incidentes de seguridad, así como también la información mínima a proporcionar, manteniendo el anonimato de quien reporte.
- Informar a quien corresponda de acuerdo a la normativa vigente en la materia.
- Velar por la integridad, confidencialidad y disponibilidad de la información generada en el contexto de un evento o incidente, preservando adecuadamente las evidencias correspondientes con el fin de mantener la trazabilidad y auditabilidad de las acciones.
- Resolver las consecuencias de los incidentes de seguridad de la información.
- Investigar los incidentes de seguridad de la información.

- Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.
- Aprender de los incidentes de seguridad de la información para prevenir nuevas ocurrencias y aplicar acciones posincidente, tales como mejorar los procesos operativos de gestión de incidentes de seguridad de la información o asegurar la retención de evidencias.
- Cumplir con la normativa interna vigente y de los organismos reguladores y de control.

Política de continuidad del negocio y recuperación ante desastres

Esta política establece las pautas para la prevención ante la ocurrencia de una interrupción del funcionamiento de Centro Ceibal y la puesta en práctica de las respuestas adecuadas y oportunas con el objetivo de minimizar los posibles impactos adversos. Las posibles y múltiples causas pueden tener origen en factores tecnológicos, humanos y/o naturales que puedan afectar los procesos del negocio y sus activos asociados.

En tal sentido, la continuidad del negocio requiere: identificar los servicios críticos, establecer estrategias y protocolos, determinar los insumos necesarios para el desarrollo de las actividades en un entorno seguro y definir responsabilidades y funciones, en cumplimiento con la normativa aplicable.

El diseño del Plan de Continuidad del Negocio de Centro Ceibal se sustenta en acciones de carácter estratégico, como:

- Definir los procesos críticos del negocio y sus activos asociados.
- Identificar y valorar los riesgos a los que están expuestos los procesos críticos del negocio y sus activos asociados, así como establecer aquellos eventos que puedan causar interrupciones en la operativa normal, resultado de las vulnerabilidades y materialización de amenazas.
- Efectuar un análisis de impacto ante la eventualidad de una interrupción operativa, que permita determinar prioridades y criticidad en la recuperación, los tiempos tolerables y las necesidades mínimas de recursos y equipos críticos.
- Implantar controles preventivos y medidas de mitigación de riesgos, que permitan ajustar la exposición a niveles tolerables e identificar las vulnerabilidades existentes, así como cualquier amenaza potencial para Centro Ceibal.
- Definir criterios, formalizar acuerdos de servicios con terceros que permitan la continuidad de las funciones críticas provistas y evaluar la capacidad de los proveedores de cumplir con dichos acuerdos.
- Formular y documentar el Plan de Continuidad del Negocio para prevenir y dar respuestas adecuadas ante posibles interrupciones, estableciendo roles y responsabilidades con el objetivo de mantener las operaciones en niveles de servicios aceptables y actualizándolo en forma permanente.
- Formular y documentar el Plan de Recuperación ante Desastres que establezca la estrategia de recuperación de las operaciones del negocio en niveles de servicios tolerables previamente definidos, actualizándolo en forma permanente.
- Evaluar y probar periódicamente el Plan de Continuidad del Negocio y el Plan de Recuperación ante Desastres de Centro Ceibal, de acuerdo con la criticidad de los procesos de negocio y con los requerimientos establecidos por los organismos reguladores.
- Documentar e informar los resultados de las pruebas realizadas a la Alta Gerencia y Comités involucrados.
- Difundir el Plan de Continuidad del Negocio y capacitar al personal involucrado en su aplicación.
- Cumplir con la regulación normativa interna y de los organismos reguladores y de control.

Política de respaldos

Esta política establece los criterios generales que aseguran una correcta ejecución, control, resguardo y disposición de los respaldos de la información, para garantizar su confidencialidad, integridad y disponibilidad.

Dentro de las acciones necesarias para el correcto desarrollo se encuentran:

- Mantener actualizado un inventario de infraestructura de TI con clasificación de criticidad. A partir de este, establecer un registro de todos los activos que se respaldan detallando características unívocas de estos, así como contenido respaldado, frecuencia, ciclo de vida y retención de la información. Como mínimo, toda infraestructura que Centro Ceibal defina como crítica deberá estar contemplada dentro del procedimiento de respaldo, así como todo otro activo que por su importancia requiera estar considerado.
- Establecer y documentar los procedimientos de respaldo y recuperación de la información, así como la forma de control necesaria para validar la ejecución periódica y el correcto funcionamiento de los respaldos por parte de los operadores responsables. Especificar los formatos en los que se realizan los respaldos de modo de poder accederlos cuando se quieran restaurar.
- Generar y documentar un procedimiento de controles de prueba con una frecuencia adecuada a definir, para validar el correcto funcionamiento de la rutina de respaldos, así como la correcta recuperación de la información. Establecer, además, un procedimiento de validación y control de aquellos medios de respaldo que se vayan a almacenar por un período superior a un año, para asegurar la correcta recuperación de la información contenida en ellos.
- Documentar de forma adecuada el registro de recuperaciones y controles de la información de respaldo.
- Realizar la gestión y el tránsito adecuado de los medios de respaldo, así como de la información contenida en estos, y velar por su seguridad lógica, física y ambiental de manera que se cumpla con la confidencialidad, integridad y disponibilidad de la información.
- Establecer los procedimientos de destrucción segura de información y medios de respaldo.
- Cumplir con la normativa interna y de los organismos reguladores y de control.

Política de gestión de ambientes

Esta política establece los criterios generales que permiten un uso correcto y seguro de los distintos ambientes para el despliegue de aplicaciones. El objetivo es minimizar los riesgos de accesos no autorizados en particular a los ambientes productivos.

Dentro de las acciones necesarias para el correcto desarrollo se encuentran:

- Definir los diferentes ambientes que son utilizados en Ceibal. Las buenas prácticas establecen la creación mínima de 4 ambientes por solución aplicativa: desarrollo, testing, preproducción y producción. En caso de utilizar menos ambientes deberá justificarse adecuadamente la decisión. Podrán incluso ser necesarios mayor cantidad de ambientes para soluciones con necesidades particulares como por ejemplo: capacitación, migraciones y procesos de extracción, transformación y carga..
- Establecer los procedimientos que rigen la creación de cada uno de éstos ambientes de acuerdo a los objetivos y requisitos particulares de las partes interesadas y la organización.
- Establecer los roles y responsabilidades de gestión de cada uno de estos ambientes de acuerdo a los requerimientos y necesidades de las partes interesadas teniendo particular cuidado en velar por la confidencialidad, integridad y disponibilidad de la información.
- Establecer los procedimientos de pasajes entre ambientes de manera de asegurar un despliegue seguro. Se deberá tener especial cuidado en el pasaje a producción, estableciendo claramente las autorizaciones, controles, niveles de aceptación/rechazo, gestión de riesgos, calidad, contingencias y rollbacks necesarios para un despliegue seguro. Esto deberá estar alineado con lo establecido en la política de gestión de cambios de Ceibal.
- Documentar y establecer claramente la trazabilidad en los pasajes entre ambientes de manera que puedan ser correctamente auditados.
- Establecer claramente los procedimientos de accesos y permisos para cada tipo de ambiente, asegurando el control del acceso tanto físico como lógico y verificando los procesos de autenticación y autorización adecuados que garanticen la seguridad de la información.
- Establecer los procedimientos de monitoreo y auditoría que permitan asegurar la confidencialidad, integridad y disponibilidad de la información gestionada en los distintos ambientes.

Política de seguridad en la nube

Esta política establece los criterios generales que permiten un uso correcto y seguro de las soluciones, bases de datos, APIs y demás componentes tecnológicos que se encuentran alojados en nubes públicas y privadas en distintas modalidades (BaaS, SaaS, IaaS, PaaS y otros). Es importante tener en cuenta que en general aplica el modelo de responsabilidad compartida y es fundamental definir y hacer cumplir las responsabilidades que recaen en los proveedores y aquellas que son de Ceibal.

Para un apropiado desarrollo de la política, se debe:

- Definir adecuadamente los perfiles, grupos, roles y usuarios siguiendo los criterios de mínimos privilegios y gestionando medidas que aseguren la confidencialidad de la información.
- Identificar, inventariar y clasificar según su criticidad todos los activos alojados en la nube.
- Implementar los controles necesarios para garantizar un acceso seguro a la información como, por ejemplo, implementar doble factor de autenticación, teniendo especial cuidado en la gestión de las cuentas privilegiadas.
- Implementar las configuraciones adecuadas de seguridad recomendadas por los proveedores de servicios en la nube aplicando los controles necesarios.
- Monitorear y auditar los componentes tecnológicos alojados en nubes a través de los servicios ofrecidos por los proveedores y los controles tecnológicos que se consideren adecuados a la criticidad de los activos e información almacenados. El objetivo es detectar las vulnerabilidades y riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de los sistemas en cuestión.
- Definir los procesos asociados a la gestión de la seguridad en las nubes documentando los procedimientos, instructivos y demás componentes de la gestión documental.
- Generar una respuesta adecuada frente a posibles incidentes de seguridad de la información en las nubes, recuperando los activos de información que puedan ponerse en riesgo. Esto implica entre otras medidas la implementación de los respaldos correspondientes y el plan de contingencia necesario para la recuperación.
- Exigir y conocer de los proveedores de las nubes los acuerdos de nivel de servicio, acuerdos de no divulgación de información, certificaciones y otros componentes contractuales que sean necesarios para garantizar la seguridad de la información y el cumplimiento normativo analizando si se adecuan a las necesidades de Ceibal. Esto podrá incluir las penalizaciones que se consideren necesarias frente a incumplimientos por parte de los proveedores.
- Considerar los aspectos de privacidad y protección de datos personales, verificando el cumplimiento de la normativa vigente que pueda aplicar como ser la territorialidad del almacenamiento de los datos, las certificaciones exigidas y los contratos necesarios para mantener la seguridad de la información.
- Divulgar y concientizar entre el personal los servicios que están habilitados para ser contratados en la nube y los controles necesarios para el uso adecuado de la información por ejemplo si es necesario cifrar la información en reposo y tránsito.
- Cumplir los requisitos del ciclo de vida de los datos almacenados en la nube, incluyendo el borrado de los mismos de manera segura.
- Conocer las políticas de seguridad de los proveedores de nubes a contratar analizando si se adecúan a las necesidades de Ceibal.

Política de destrucción de la información

El propósito de esta política de destrucción de la información es establecer los criterios principales para la destrucción segura y efectiva de la información, tanto en formato físico como digital, con el fin de proteger la confidencialidad de los datos.

Dentro de las acciones necesarias para el correcto desarrollo de la política se encuentran:

- Establecer los lineamientos y procedimientos que rigen la vida útil de los dispositivos, la obsolescencia tecnológica, el alcance del beneficio y los productos y servicios que brinda Ceibal, de manera que se pueda determinar de manera correcta el ciclo de vida de la información y dispositivos para proceder a su correcta disposición
- Establecer los roles y responsabilidades en gestión de cada tipo de destrucción de información de acuerdo a los requerimientos y necesidades de las partes interesadas teniendo particular cuidado en velar por la confidencialidad de la información.
- Establecer los procedimientos que rigen el momento y los mecanismos de destrucción de la información de acuerdo a los objetivos y requisitos particulares de las partes interesadas y la organización. Los mismos deben garantizar que la información sea eliminada de manera segura y no pueda ser recuperada o accedida de ninguna manera si se considera necesario. Esto puede llegar a incluir junto con la información original, todas sus copias y respaldos.

- Documentar y establecer claramente la trazabilidad en los procesos de destrucción de la información de manera que puedan ser correctamente auditados, incluido lo que por alguna razón no se pueda destruir. Esto incluye las acciones necesarias para verificar el cumplimiento de los procedimientos de destrucción, y actualizar los procesos conforme a las mejores prácticas y cambios regulatorios.
- Cumplir con los plazos legales para la destrucción de la información, así como con la normativa vigente en la materia.
- Capacitar a los usuarios, proveedores y demás partes interesadas sobre la importancia y los procedimientos de destrucción segura de la información.

Política de escritorio y pantallas limpias

El propósito de esta política es establecer los lineamientos y promover conductas que colaboren con la reducción de los riesgos de acceso no autorizado, pérdida o alteración de la información cumpliendo con los cometidos de asegurar la confidencialidad, integridad y disponibilidad de la información de Ceibal.

Dentro de las acciones necesarias para el correcto desarrollo de la política se encuentran:

- Establecer los lineamientos y procedimientos que rigen el uso correcto de los dispositivos asegurando la confidencialidad de la información en los entornos de trabajo tomando en cuenta las medidas de seguridad necesarias para que otros usuarios no puedan acceder a la información sensible o crítica.
- Establecer los procedimientos para que la información en formato físico o digital no quede a disposición de usuarios que no deberían tener acceso a la misma.
- Establecer las buenas prácticas y procedimientos a tener en cuenta en el uso de escritorios, pantallas y demás recursos físicos de la organización para asegurar la confidencialidad de la información que permanece en los mismos.
- Establecer las configuraciones de seguridad necesarias para brindar un soporte adecuado al usuario que le permita asegurar la confidencialidad de la información que procesa.
- Establecer los procedimientos para reportar la información que se encuentra abandonada o no está alojada de manera segura cumpliendo con los requisitos de seguridad necesarios.
- Documentar y establecer claramente los procedimientos que permitan monitorear, auditar y verificar que se cumpla con lo establecido en la presente política.
- Capacitar y concientizar a los usuarios, proveedores y demás partes interesadas sobre la importancia y los procedimientos para mantener la información confidencial de manera segura.

Glosario y abreviaturas

Activo: ítem, objeto o entidad que tiene valor real o potencial para una organización (UNIT-ISO 55000 – Cap.3 Términos y definiciones).

Activo crítico: activo que tiene potencial para impactar significativamente en el logro de los objetivos de la organización (UNIT-ISO 55000 – Cap.3 Términos y definiciones).

Activos de información: datos o información que tienen valor para una organización (Decreto Presidencial N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones).

Análisis de Impacto: el análisis de impacto al negocio (Business Impact Analysis o BIA por sus siglas en inglés) es una herramienta de evaluación orientada a conocer cómo podría verse afectada una organización y las consecuencias sobre los procesos de negocio como resultado de la ocurrencia de algún incidente o un desastre. Permite estimar la magnitud del impacto operacional y financiero asociado a una interrupción.

Autenticación: asegurar que una supuesta característica de una entidad es correcta (UNIT-ISO 27000 – Cap.2 Términos y definiciones).

Código de uso de sistemas informáticos: documento en el cual se establecen las normas que deben regir el uso de cualquier sistema informático.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados (UNIT-ISO 27000 – Cap.2 Términos y definiciones).

Control: medida que modifica el riesgo (UNIT-ISO 27000 – Cap.2 Términos y definiciones).

CSI: Comité de Seguridad de la Información

Disponibilidad: propiedad ser accesible y utilizable por solicitud de una entidad autorizada (UNIT-ISO 27000 – Cap.2 Términos y definiciones).

Evento de seguridad de la información: ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad (UNIT-ISO/IEC 27035).

GTSI: Grupo de Trabajo de Seguridad de la Información

Incidente de seguridad de la información: es indicado por un único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información (UNIT-ISO/IEC 27035).

Integridad: propiedad de exactitud y completitud (UNIT-ISO 27000 – Cap.2 Términos y definiciones).

Plan de Continuidad del Negocio: conjunto de documentos que establecen las estrategias, protocolos, servicios, responsabilidades, funciones e insumos necesarios para que, en la eventualidad de una interrupción imprevisible del funcionamiento operativo de Centro Ceibal, éste quede habilitado para reestablecer sus actividades operacionales básicas, en particular la atención a los beneficiarios.

Plan de Recuperación ante Desastres: conjunto de políticas, procedimientos y herramientas que permiten la recuperación de infraestructura y sistemas de información definidos como críticos ante la ocurrencia de un desastre, sea natural o provocado por el hombre.

Proceso crítico: según el Plan de Continuidad del Negocio, son aquellos fundamentales para el negocio, su interrupción potencial puede impactar en el logro de los objetivos.

Seguridad física: preservación de la confidencialidad, integridad y disponibilidad física de los activos de información.

Seguridad lógica: preservación de la confidencialidad, integridad y disponibilidad de los activos de información almacenados en sistemas informáticos.

Sistema de información: aplicaciones, servicios, activos de tecnología de la información o cualquier otro componente que maneje información (UNIT-ISO/IEC 27000).

Software de base: es aquel sobre el que se desarrollan o implantan programas informáticos de usuario final. Esto incluye, entre otros, sistemas operativos, software de servidor web, motores de bases de datos, librerías.

Usuario de un activo de información: quien accede de manera autorizada a la información contenida en los activos, independientemente de las posibilidades de consulta o modificación.

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas (UNIT-ISO 27000 – Cap.2 Términos y definiciones).

Vigencia

Actualizaciones del Manual de Políticas de Seguridad de la Información

Este Manual de Políticas será revisado de manera anual por el CSI.

Centro Ceibal se reserva el derecho de realizar cualquier cambio y/o corrección a este Manual de Políticas sin que ello requiera aviso o requisito alguno. Es responsabilidad de los Usuarios remitirse con cierta frecuencia a estos documentos para verificar las actualizaciones subsiguientes.

Cómo se realiza la regulación

Jurisdicción y Ley aplicables

Esta Manual de Políticas de Seguridad de la Información se encuentra regido, sin excepción y en todas sus cláusulas, por las leyes de la República Oriental del Uruguay y será interpretada de acuerdo a ellas. Cualquier controversia derivada de este documento relativa a su existencia, validez, interpretación, alcance o cumplimiento será sometida a los tribunales de Montevideo, renunciándose en forma expresa a cualquier otro fuero o jurisdicción.

Obtenido de «https://wiki.ceibal.edu.uy/index.php?title=Manual_de_políticas_de_seguridad_de_la_información&oldid=98106»

Categoría: Normativa interna

-
- Esta página fue modificada por última vez el 18 dic 2024 a las 13:57.

Especificación de la política de contraseñas

De Wiki Ceibal

COPIA NO CONTROLADA

Cualquier copia impresa de este documento se considera **no controlada**, por lo que está prohibida la reproducción total o parcial sin la autorización del Responsable de Calidad.

Datos SGC	
Código	62385
Tipo	Especificaciones (ES)
Nombre	Especificación de la política de contraseñas
Revisión	97100 (2024-10) -
	Ubicación
Proceso	Gestión de la Seguridad de la Información
Subproceso	/ Soporte de Infraestructura

Contenido

- 1 Objetivo
- 2 Alcance
- 3 **DEFINICIÓN DE REGLAS PARA LA GENERACIÓN DE CONTRASEÑAS**

Objetivo

Establecer los criterios de complejidad para la gestión de contraseñas en Ceibal.

Alcance

Contraseñas de todos los sistemas pertenecientes a Ceibal

DEFINICIÓN DE REGLAS PARA LA GENERACIÓN DE CONTRASEÑAS

Este documento explica en detalle los criterios de complejidad a tener en cuenta a la hora de cambiar o crear contraseñas para todos los sistemas pertenecientes a Ceibal. Se divide en 3 niveles de complejidad según el rol:

BÁSICO

- Mínimo: 4 caracteres
- Caracteres alfanuméricos inclusive espacios
- Cambio: No
- Posibles roles: Estudiantes, jubilados y Biblioteca país.
- Solicitar actualización de al menos uno de los datos de contacto (mail o cel).

INTERMEDIO

- Mínimo: 8 caracteres
- Mayúsculas y minúsculas
- Números
- Cambio: No
- Posibles roles: Docentes
- Solicitar actualización de al menos uno de los datos de contacto (mail o cel).

AVANZADO

- Mínimo: 8 caracteres
- Letras y números
- Mayúsculas y minúsculas
- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos
- Intentos mínimos antes del bloqueo: 10
- Cambio: No
- Posibles roles: Funcionarios de Ceibal.
- Solicitar actualización de al menos uno de los datos de contacto (mail o cel).

CUENTAS PRIVILEGIADAS

- Mínimo: 10 caracteres
- Letras y números
- Mayúsculas y minúsculas
- Al menos un carácter no alfanumérico (por ejemplo, !, \$, #, %)
- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos
- MFA activado
- Cambio: Cada 6 meses
- Intentos mínimos antes del bloqueo: 5
- Posibles roles: Jefes y Gerentes de Ceibal - Cuentas privilegiadas

Obtenido de «https://wiki.ceibal.edu.uy/index.php?title=Especificación_de_la_política_de_contraseñas&oldid=97100»

Categoría: Especificaciones

-
- Esta página fue modificada por última vez el 30 oct 2024 a las 11:38.