LA SEGURIDAD

no es un sprint, es un maratón

Instructor de Capacitación:

Carlos Alfredo Hdz

Equipo de SI:

Tawny Valdivieso
Jazmín Dominguez

Educación
Secretaría de Educación Pública

CONADE
COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE

tobb

CONTENIDO

1. EQUIPO Y SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se puede definir como la prevención de la **confidencialidad, integridad y disponibilidad** de la información, independientemente del formato que tenga: impresa, digital, video, etc.

2. ACTIVOS DE INFORMACIÓN

Los activos de información son todos aquellos elementos que tienen valor para una organización y que, por lo tanto, deben ser protegidos (procesamiento, transporte, almacenamiento)

3. ISO 27001/2022

La norma internacional ISO/IEC 27001:2022 establece las mejores prácticas para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

EQUIPO

DPTI

Promover la integración en la sociedad del conocimiento en materia de cultura física y deporte, así como implementar un esquema de organización en la CONADE, basado en una planeación estratégica; instrumentar el uso eficiente de las tecnologías de información, comunicaciones y seguridad de la información, con el fin de elevar la eficiencia operativa gubernamental, transformando, modernizando y facilitando el acceso de trámites y servicios al ciudadano; asimismo, supervisar el cumplimiento de las obligaciones de transparencia y acceso a la información pública.

Carlos García
Director de Planeación y Tecnologías de Información

Rafael Rueda
Jefe de Departamento de Soporte Técnico

Emmanuel Tahuilan
Jefe de Departamento de Desarrollo de Sistemas

Ana Chacón
Jefa de Departamento de Redes y Comunicaciónes

EQUIPO

Administraciones KASAI

Garantizar la operación oportuna y adecuada de la CONADE, para el cumplimiento de los objetivos y metas institucionales a través de la prestación de los "Servicios Informáticos Integrales del Centro de Atención Tecnológica para la CONADE 2025"

Luis Vera
Director de Tecnologías Administraciones KASAI

Víctor Carreola
Administrador General del CAT

Tawny Alexis Valdivieso
Administrador de SI

Jazmín Dominguez
Ingeniero en Seguridad Perimetral

Luis Alberto Ramirez
Ingeniero en Sitio Redes

Juan Manuel Hernández
Ingeniero en sitio - Centro de Datos

Carlos Alfredo Hernandez
Transferencia del Conocimiento

Educación
Secretaría de Educación Pública

CONADE
COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE

tobb

PRINCIPIOS DE SI

Confidencialidad

Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.
Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información.

Integridad

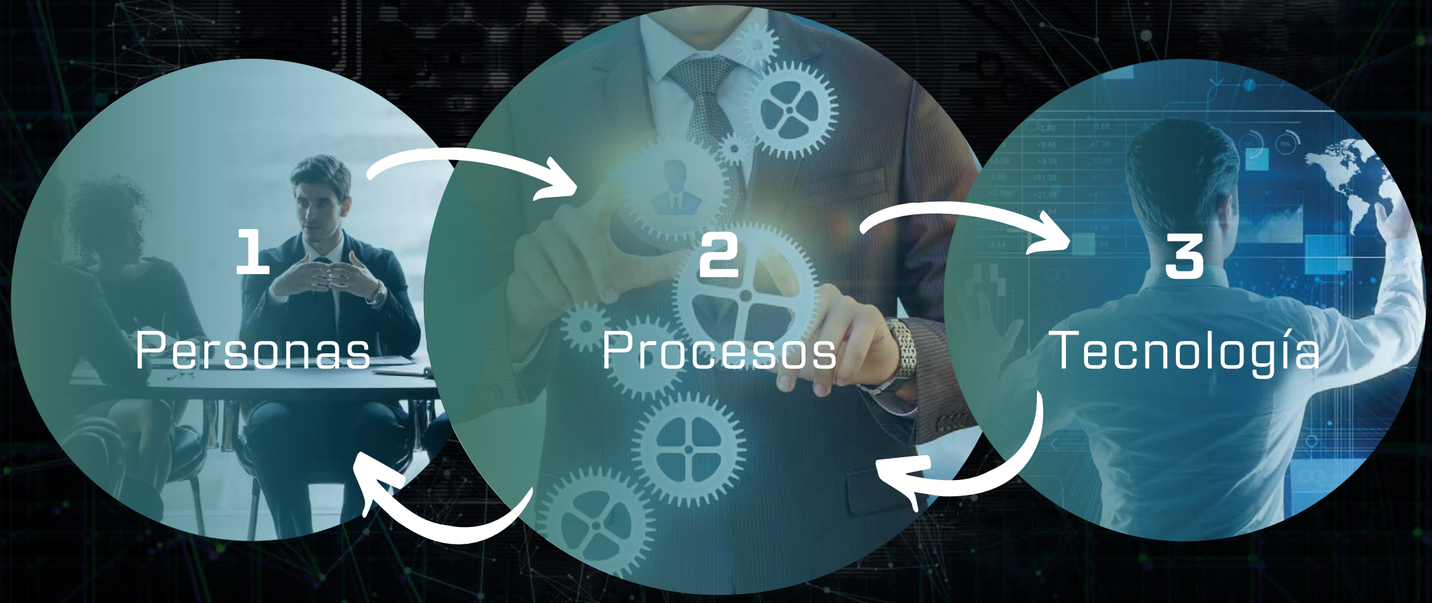
Es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Disponibilidad

La información debe ser almacenada de manera segura y disponible para las y los usuarios cuando la necesiten. Así mismo debe ser mantenida y utilizada de tal forma que su integridad no se vea comprometida, cuando dicha información sea sensible

ELEMENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

La SI se engrana a partir de 3 elementos escenciales:



ACTIVOS DE INFORMACIÓN

Información que maneja

Hardware

Software

Servicios

Procesos

Personas

ACTIVO DE INFORMACIÓN

¿cómo lo analizamos y protegemos?

ACTIVO DE INFORMACIÓN

¿Quién protege?

Custodio de Activo

Tratamiento

Clasificación

CLASIFICACIÓN DE LA INFORMACIÓN

En la CONADE la información se Clasifica en:

RESERVADA

Información que, si se divulga, puede **comprometer la seguridad nacional, la seguridad pública o afectar procesos gubernamentales.**

CONFIDENCIAL

Información que contiene **datos personales** o sensibles cuya divulgación podría vulnerar la privacidad de las personas.

PÚBLICA

Información que puede ser **consultada libremente** por cualquier persona, sin restricción alguna.

ACTIVIDAD

¿Tú cómo clasificas tu información?

Información sobre Juicios en curso

Datos personales de Atletas

Avisos de Privacidad

Marcos Normativos

Información bancaria

Presupuestos públicos

Nóminas de Servidores Públicos

Datos personales de Usuarios

Políticas de Seguridad de la Información

Historiales médicos

Estrategias de Seguridad

RESERVADA	CONFIDENCIAL	PÚBLICA

Educación
Secretaría de Educación Pública

CONADE
COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE

tobb

RESERVADA

Información sobre Juicios en curso

Políticas de Seguridad de la Información

Estrategias de Seguridad

CONFIDENCIAL

Datos personales de Atletas

Información bancaria

Datos personales de Usuarios

Historiales médicos

PÚBLICA

Avisos de Privacidad

Marcos Normativos

Nóminas de Servidores Públicos

Presupuestos públicos

CLASIFICACIÓN DE LA INFORMACIÓN EN LA CONADE

Lo que sí se debe hacer

- Identifica la información que manejas: ¿Es confidencial, reservada o pública?
- Consulta con el responsable del área si tienes dudas sobre la clasificación.
- Etiqueta correctamente los documentos electrónicos y físicos.
- Comparte la información solo con personas autorizadas en la CONADE.
- Aplica las medidas de seguridad correspondientes al nivel de clasificación (contraseñas, cifrado, almacenamiento).
- Actualiza la clasificación si la información cambia de contexto o uso.
- Utilizar la leyenda de aviso de confidencialidad dentro del correo institucional.

Lo que no debes hacer

- Asumir que toda la información es pública por defecto.
- Compartir documentos por correo o medios externos sin verificar su clasificación.
- Compartir contraseñas.
- Guardar documentos sensibles en USB sin protección.
- Dejar información impresa en escritorios o espacios comunes.
- Enviar información confidencial por WhatsApp u otras apps sin autorización.
- Descuidar la información porque “ya todos la conocen” o “no es tan importante”.

LEYENDA DE CONFIDENCIALIDAD

AVISO DE CONFIDENCIALIDAD

De conformidad con lo establecido en el inciso a del artículo 57 del “Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal”, se informa que este mensaje y los datos adjuntos son para uso exclusivo de la persona o entidad a la que expresamente ha sido enviada, el cual puede contener información que por su naturaleza deba ser considerada como CONFIDENCIAL o RESERVADA, en términos de lo dispuesto por las Leyes General y Federal de Transparencia y Acceso a la Información Pública y General de Protección de Datos Personales en Posesión de Sujetos Obligados. Si por error ha recibido esta comunicación: 1) queda estrictamente prohibido la revelación, retransmisión, difusión o el uso de la información contenida; 2) notifíquelo al remitente; y 3) bórrelo de inmediato y en forma permanente, junto con cualquier copia digital o impresa, así como cualquier archivo anexo al mismo.

RIESGOS Y AMENAZAS

Los riesgos de seguridad de la información están asociados a la probabilidad de que las amenazas se materialicen sobre los activos informáticos, causando un daño a la organización.

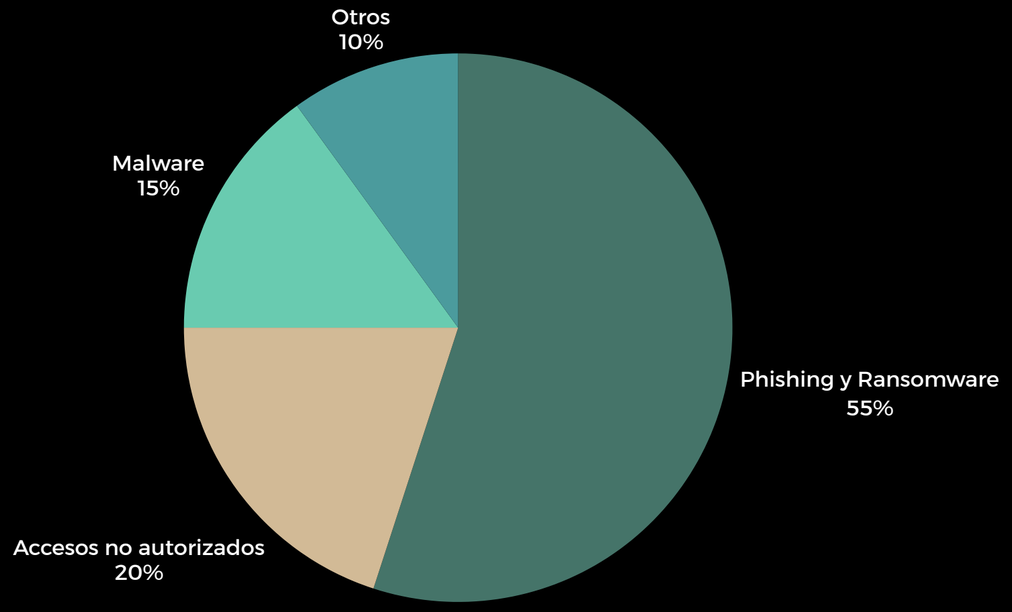
Los riesgos tienen que ver además con el grado de confidencialidad de la información, así como hardware, software, servicios, entre otros.

Por otro lado, el incremento de las amenazas a los sistemas de información es directamente proporcional al crecimiento de la virtualidad y el uso de nuevas tecnologías.

¿PROTEGERTE?

Los ciberataques no distinguen fronteras. Cada segundo, en algún lugar del mundo, una organización enfrenta un intento de vulnerar su información. Entender las cifras globales y nacionales es el primer paso para dimensionar los riesgos.

Distribución de los tipos de ataques más comunes en México:



75%

- En 2024, las organizaciones enfrentaron en promedio 1,876 ataques cibernéticos semanales — un incremento del 75% respecto al año anterior.

(Fuente: IBM / Varonis)

- El costo promedio de una brecha de datos en el mundo alcanzó los $4.88 millones de dólares por incidente.

(Fuentes: National University / TechTarget)

ISO 27001/2022

NORMA INTERNACIONAL

PREVENCIÓN

PROTECCIÓN DE DATOS

Cada organización debe contar con personal capacitado y responsable de asegurar la protección de la información, infraestructura y servicios en temas de Ciberseguridad.

POLÍTICAS Y PROCESOS

Cada organización es responsable de cumplir con los lineamientos de Seguridad de la Información y asegurar que todos los Empleados cumplan con los lineamientos mínimos necesarios en tema de Ciberseguridad y Protección de Datos.

MEJORA CONTINUA

Cada organización debe cumplir con los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

MGSI

Marco de Gestión de Seguridad de la Información es un acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

Establece como directriz que las Instituciones de la Administración Pública Federal deberán contar con un Marco de Gestión de Seguridad de la Información (MGSI), alineado a la política general de Seguridad de la Información, que cada Institución establezca de conformidad con sus objetivos y dimensionamiento.

¿Cómo me ayuda a mí?

- Identificación de Riesgos
- Protección de Datos
- Cumplimiento Normativo
- Conciencia y Capacitación
- Mejora Continua
- Objetivos Constitucionales

Artículo 75

Norma Técnica de Seguridad de la Información

MSGI EN LA CONADE

89 % CUMPLIMIENTO

COMPROMISO CON LA SEGURIDAD DE LA INFORMACIÓN

Educación
Secretaría de Educación Pública

CONADE
COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE

tobb

ELEMENTOS DEL MGSI

1. REDES
2. CENTRO DE DATOS
3. ACTIVOS DE INFORMACIÓN
4. INCIDENTES DE SI
5. CONTINUIDAD Y DRP
6. CONCIENTIZACIÓN Y CAPACITACIÓN
7. RECURSOS HUMANOS
8. DESARROLLO SEGURO

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Educación
Secretaría de Educación Pública

CONADE
COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE

tecnm

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

No dejes desatendido tu equipo de cómputo ¡Bloquéalo!

Mantendrás tu escritorio (físico y virtual) limpio

Resguarda la Información reservada o confidencial en sitios seguros

Alerta a la MSC cualquier sospecha de Phishing y Malware

Mantén seguras y actualizadas tus contraseñas

Haz uso de las herramientas de trabajo proporcionadas

Navega en páginas seguras y permitidas

No compartas las redes institucionales a personal externo de la CONADE

Educación
Secretaría de Educación Pública

CONADE
COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE

tobb

INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. INCIDENTES

Cada incidente, grande o pequeño, importa. Resolverlos a tiempo evita riesgos, protege las operaciones y refleja nuestro compromiso con la excelencia.

2. CLAVES PARA EL ÉXITO

1. Prioriza cada solicitud: No subestimes ningún incidente.
2. Resuelve con calidad: Una solución efectiva asegura continuidad.
3. Actúa rápido: Cada minuto cuenta para minimizar el impacto.

3. BENENFICIOS

- Operaciones estables
- Reconocimiento del equipo
- Resultados con éxito

Priorizar y resolver incidentes a tiempo garantiza el éxito de nuestras operaciones.

ERISC

Equipo de Respuesta a Incidentes de SI

Equipo dedicado a la gestión y resolución de incidentes de seguridad. Conformado por personal de la DPTI -CONADE, así como de Administraciones Kasai (proveedor de servicio de administración de seguridad de la información)

Educación
Secretaría de Educación Pública

CONADE
COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE

tobb

INCIDENTES

¿Quién me ayuda?

MSC

MESA DE SERVICIO CALIFICADA

55 5927 5200 ext. 1101

mesadeservicio@conade.gob.mx

Portal de la MSC

https://mesadeservicio.conade.gob.mx/WOListView.do

Educación
Secretaría de Educación Pública

CONADE
COMISIÓN NACIONAL DE CULTURA FÍSICA Y DEPORTE

tobb

PLAN DE CONTINUIDAD DEL NEGOCIO

¿Qué es un BCP?

Un Plan de Continuidad del Negocio (BCP, por sus siglas en inglés) es una estrategia que permite a las organizaciones mantener sus operaciones durante y después de una interrupción inesperada.

¿Por qué es importante?

- Evita interrupciones graves en la operación
- Salvaguarda la información y los activos críticos
- Mantiene la confianza de clientes y socios
- Reduce la improvisación en momentos de crisis

¿Cómo funciona?

Un BCP ayuda a una institución a estar preparada ante cualquier crisis. Para lograrlo, se basa en 3 pilares fundamentales:

1. Identificar riesgos y puntos débiles
2. Definir estrategias para mantener la operación
3. Preparar y capacitar al equipo

PLAN DE RECUPERACIÓN ANTE DESASTRES

¿QUÉ ES UN DRP?

Un Plan de Recuperación ante Desastres es una estrategia diseñada para restaurar sistemas tecnológicos y datos críticos después de un evento inesperado, como ciberataques, fallas en servidores, errores humanos o desastres naturales. Su objetivo principal es reducir el tiempo de inactividad y recuperar la infraestructura lo más rápido posible.

¿POR QUÉ ES IMPORTANTE?

En la era digital, la información y los sistemas tecnológicos son el corazón de cualquier empresa. Un DRP es crucial porque:

- Protege la continuidad del negocio
- Previene la pérdida de información valiosa
- Reduce el tiempo de respuesta ante incidentes
- Asegura el cumplimiento de normativas

¿CÓMO SE ACTIVA?

Un DRP sigue 3 pasos clave para garantizar que la institución pueda recuperar su infraestructura tecnológica sin grandes afectaciones:

1. Evaluar los riesgos y sistemas críticos
2. Establecer procedimientos de respaldo y restauración
3. Probar y actualizar el plan regularmente

CAMPAÑAS DE CONCIENCIACIÓN

RESUMEN

01 La Seguridad de la Información protege los activos valiosos de la organización, asegurando su confidencialidad, integridad y disponibilidad.

02 Los activos de información pueden ser datos, hardware, software, servicios, personas y más. Son analizados a través de sus vulnerabilidades, amenazas, valor, procesos y propiedad.

03 El propietario del activo es quien debe asegurar su correcto tratamiento y clasificación, de acuerdo a si la información es pública, privada o confidencial.

04 Clasificar la información en la CONADE permite proteger datos sensibles, cumplir con normativas y evitar incidentes. Existen prácticas clave que deben seguirse y otras que deben evitarse

05 Los riesgos y amenazas en el entorno digital aumentan globalmente y en México, con ciberataques en crecimiento. La protección de datos es una prioridad.

06 La ISO/IEC 27001:2022 proporciona el marco internacional para implementar políticas, procesos y controles que protejan la información y fomenten la mejora continua.

07 El Marco de Gestión de Seguridad de la Información (MGSI) de la CONADE abarca elementos clave como redes, centros de datos, continuidad, capacitación, desarrollo seguro y recursos humanos.

08 Las Políticas Internas de Seguridad y procesos definen cómo actuar ante incidentes, quién debe intervenir y cuáles son las mejores prácticas.

09 El Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP) aseguran que la CONADE pueda responder, recuperarse y seguir operando tras una crisis.

¿DUDAS?

GRACIAS