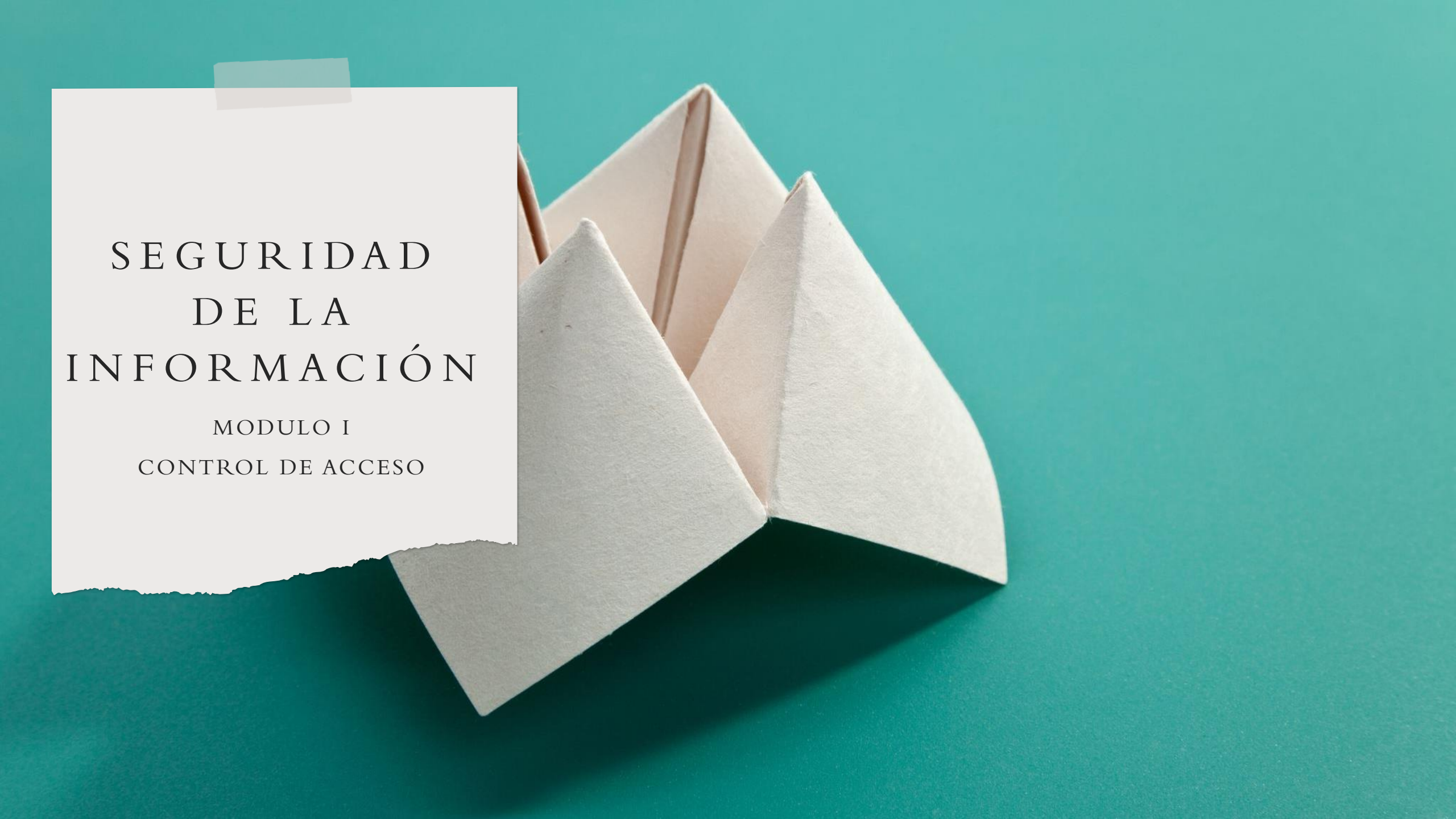
SEGURIDAD DE LA INFORMACIÓN

MODULO I

CONTROL DE ACCESO



OBJETIVOS

GENERAL

- Adquirir, comprender y/o consolidar las competencias relacionadas a la capacidad de entender en forma básica, la razón de la existencia y del funcionamiento de los ataques cibernéticos, dentro del marco del ciudadano digital, desde donde se genera la necesidad de las medidas de protección para garantizar la convivencia armoniosa de las actividades digitales cotidianas.

ESPECÍFICOS

- Comprender los Riesgos y cuidados para la gestión de credenciales.
- Comprender los Peligros y los tipos de Protección en el uso del Correo Electrónico.
- Conocer y poner en práctica las medidas de protección ante las diferentes técnicas de Ingeniería Social.
- Conocer buenas prácticas para la Navegación segura por Internet.
- Conocer las buenas prácticas la protección contra amenazas a los equipos.
- Comprender la necesidad de la protección de datos e información

OBJETIVOS

- Saber los riesgos de ciberseguridad
- Adquirir los conocimientos básicos de seguridad para mitigar los riesgos

MODULO I

Control de Acceso - Credenciales

¿QUÉ ES LA AUTENTICACIÓN?

- Es el proceso por el cual se identifica a un usuario, proceso o dispositivo para permitir acceder a recursos dentro de un sistema de información.

The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Source(s):

NIST SP 1800-27B under Authentication from FIPS 200

NIST SP 1800-27C under Authentication from FIPS 200

MÉTODOS MÁS UTILIZADOS

- El método más utilizado es de NOMBRE DE USUARIO y CONTRASEÑA, luego siguen otras
- Acceso biométrico
- Envío de enlace a través de correo electrónico
- Generación de código aleatorio y envío a dispositivo (SMS, MAIL)

BUENAS PRÁCTICAS DE CONTRASEÑAS

BUENAS PRÁCTICAS EN CONTRASEÑAS

Se deben tener unas consideraciones para la generación o elección de contraseñas independientes de la robustez de la misma contraseña, entre ellas figuran:

- No utilizar las mismas contraseñas para distintos sistemas
- No guardar las contraseñas en un post-it y pegarlo en el monitor
- No compartir las contraseñas
- No utilizar fechas, ni nombres de personas relacionadas a usted
- Siempre y cuando el sistema te lo permita utilizar autenticación de doble factor

CONTRASEÑAS ROBUSTAS

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

CONTRASEÑAS ROBUSTAS

Recomendaciones al momento de elegir o generar una contraseña

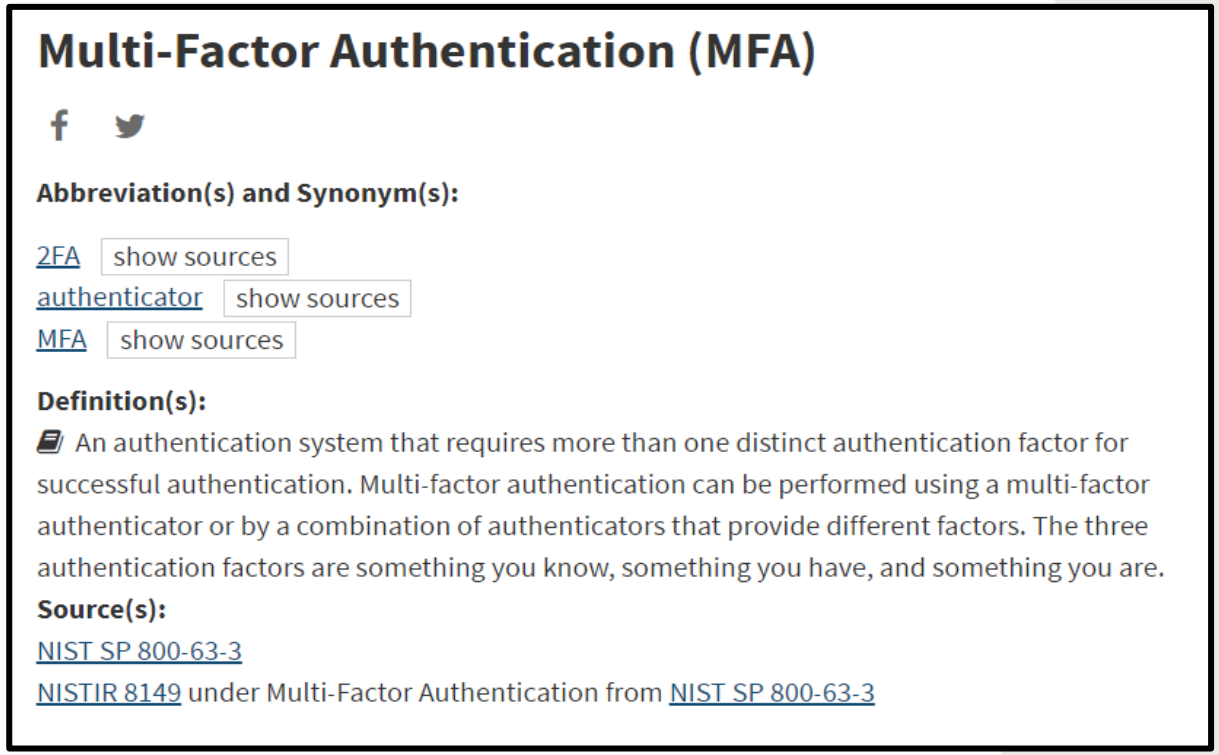
- Longitud de mínimo 8 caracteres
- Combinación de caracteres: Mayúsculas, minúsculas, números y símbolos
- Consejo: Se pueden usar frases para un mejor recordamiento, ejemplo “la muerte Abel Antonio, en mi tierra la sintieron los muchachos”

Hay empresas que se dedican a hacer un “chequeo” de las contraseñas más comunes y más vulnerables, se puede ver https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

AUTENTICACIÓN DE DOBLE FACTOR

Como lo indica el nombre, requiere más de una forma de autenticación para acceder al un sistema de información, las combinaciones más comunes son:

- Usuario – contraseña – Código de verificación (via mail o sms)
- Usuario – contraseña – autorización remota
- Usuario – contraseña – enlace de verificación
- Usuario – contraseña – biométrico / facial



Multi-Factor Authentication (MFA)

Abbreviation(s) and Synonym(s):

2FA show sources
authenticator show sources
MFA show sources

Definition(s):

An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Source(s):

NIST SP 800-63-3
NISTIR 8149 under Multi-Factor Authentication from NIST SP 800-63-3

GESTORES DE CONTRASEÑAS

- Hay aplicaciones para móviles que te permiten gestionar y guardar contraseñas, opciones hay muchas y ninguna mejor que la otra; solamente deben seguir unos requerimientos
- Deben ser seguros, fácil de usar, organizado, permitir contraseñas seguras