INSTRUCCIÓN

UNA-R-DISC-009-2024

UNA-DTIC-DISC-002-2024

PARA: COMUNIDAD UNIVERSITARIA

DE: RECTORÍA Y DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

ASUNTO: USO OBLIGATORIO DEL DOBLE FACTOR DE AUTENTICACIÓN EN EL CORREO ELECTRÓNICO INSTITUCIONAL.

FECHA: 26 DE JULIO DEL 2024

Estimados (as) compañeros (as):

PRIMERO: MARCO JURÍDICO

1. Marco de Gobierno y Gestión de TI de las Universidades Públicas y CONARE, aprobado mediante acuerdo CNR-307-2021, y aprobado por el Consejo Universitario de la UNA mediante acuerdo UNA-SCU-ACUE-240-2023, publicado en gaceta UNA-GACETA N.° 09-2023
2. Circular UNA-CGT-CIRC-016-2024 - SEGUNDO FACTOR DE AUTENTICACIÓN (2FA).
3. Circular UNA-CGT-CIRC-009-2024 - SEGUNDO FACTOR DE AUTENTICACIÓN (2FA)
4. Circular UNA-CGT-CIRC-012-2024 - ACCIONES DE CIBERSEGURIDAD REQUERIDAS A LA POBLACIÓN UNIVERSITARIA

SEGUNDO: INSTRUCCIONES

Como parte de las acciones vinculadas con las metas estratégicas vinculadas a la Transformación Digital, establecido en el PMPI 2023-2027 (metas 1.5.1, 1.5.2 y 1.5.3), así como con el proceso de implementación del nuevo Marco de Gobierno y Gestión de TI de las Universidades Públicas y CONARE, aprobado por CONARE mediante acuerdo CNR-307-2021, y por el Consejo Universitario de la UNA mediante acuerdo UNA-SCU-ACUE-240-2023, publicado en gaceta UNA-GACETA N.° 09-2023 del 06 de noviembre de 2023, **se instruye a todas las personas funcionarias a activar el mecanismos de doble factor de autenticación (2FA) en sus cuentas de correo electrónico institucional**, este mecanismo también es conocido como múltiple factor de autenticación (MFA).

Este mecanismo constituye un nivel adicional de seguridad para el uso del correo institucional y progresivamente también será implementado en otras plataformas tecnológicas de la institución que lo soportan. El doble factor de autenticación consiste básicamente en utilizar un mecanismo de confirmación adicional al usuario y la contraseña para ingresar a la plataforma de correo, estos mecanismos pueden ser, una **aplicación** (App) instalada en el teléfono, un **mensaje de texto** (SMS) o una **llamada telefónica** en la que se proporciona un código de acceso.

La implementación de múltiples factores de autenticación en las plataformas institucionales tiene como objetivo proteger la información institucional y reducir las posibilidades de hackeos o estafas utilizando técnicas de “phishing” a través del correo institucional.

Este mecanismo será implementado de manera obligatoria a partir del **próximo 30 de setiembre de 2024**, por lo que invitamos a los miembros de la comunidad universitaria que requieran capacitación o apoyo en la implementación de esta configuración en sus correos, a participar en alguna de las charlas virtuales que se brindarán con este propósito en las siguientes fechas:

Capacitación	Fecha	Hora
Capítulo Ciberseguridad 2FA - 1	Martes 6 de agosto	1:30 pm a 2:30 pm
Capítulo Ciberseguridad 2FA - 2	Jueves 8 de agosto	1:30 pm a 2:30 pm
Capítulo Ciberseguridad 2FA - 3	Lunes 12 de agosto	10:00 am a 11:00 am
Capítulo Ciberseguridad 2FA - 4	Miércoles 14 de agosto	08:30 am a 09:30 am
Capítulo Ciberseguridad 2FA - 5	Martes 20 de agosto	10:00 am a 11:00 am
Capítulo Ciberseguridad 2FA - 6	Jueves 22 de agosto	10:00 am a 11:00 am
Capítulo Ciberseguridad 2FA - 7	Lunes 26 de agosto	1:30 pm a 2:30 pm
Capítulo Ciberseguridad 2FA - 8	Miércoles 28 de agosto	1:30 pm a 2:30 pm
Capítulo Ciberseguridad 2FA - 9	Martes 3 de septiembre	1:30 pm a 2:30 pm
Capítulo Ciberseguridad 2FA - 10	Jueves 5 de septiembre	1:30 pm a 2:30 pm
Capítulo Ciberseguridad 2FA - 11	Lunes 9 de septiembre	10:00 am a 11:00 am
Capítulo Ciberseguridad 2FA - 12	Miércoles 11 de septiembre	10:00 am a 11:00 am
Capítulo Ciberseguridad 2FA - 13	Martes 17 de septiembre	10:00 am a 11:00 am
Capítulo Ciberseguridad 2FA - 14	Jueves 19 de septiembre	10:00 am a 11:00 am
Capítulo Ciberseguridad 2FA - 15	Lunes 23 de septiembre	1:30 pm a 2:30 pm
Capítulo Ciberseguridad 2FA - 16	Miércoles 25 de septiembre	1:30 pm a 2:30 pm

El registro deben realizarlo mediante el siguiente formulario, y se les hará llegar el enlace de la reunión.

Adicionalmente el personal de la DTIC estará atendiendo de manera presencial en las instalaciones de la DTIC los días jueves de los meses de agosto y setiembre, para brindar atención personalizada y apoyar en la configuración del doble factor de autenticación. Mediante el siguiente formulario puede solicitar una cita en los horarios habilitados para este propósito.

Fecha	Hora
Jueves 8 de agosto	08:30 am a 11:30 am
Jueves 15 de agosto	1:30 pm a 4:30 pm
Jueves 22 de agosto	1:30 pm a 4:30 pm
Jueves 29 de agosto	08:30 am a 11:30 am
Jueves 5 de septiembre	08:30 am a 11:30 am
Jueves 12 de septiembre	08:30 am a 11:30

	am
Jueves 19 de septiembre	10:00 am a 11:00 am
Jueves 26 de septiembre	1:30 pm a 4:30 pm

Para poder atender de manera ágil y eficiente a la mayor cantidad de funcionarios en estos espacios, se solicita conocer de previo la clave de acceso (contraseña) de la cuenta de correo que desean configurar (no se realizarán procesos de recuperación de claves en estos espacios).

Es importante indicar que las cuentas de correo electrónico que no son de uso personal, vinculadas a una dependencia académica o administrativa (como por ejemplo dtic@una.cr o rectoria@una.cr) también deben ser configuradas con el doble factor de autenticación, por lo que es importante conocer el procedimiento para los casos donde ese tipo de cuentas son gestionadas por diferentes personas de la instancia.

Como parte de los esfuerzos por facilitar la implementación de esta mejora de seguridad, la DTIC también pone a disposición los siguientes materiales de referencia, los cuales los puede encontrar en la dirección:
https://documentos.una.ac.cr/handle/unadocs/16270

Lista de guías o manuales para activar 2FA:

- Video Configuración 2FA - Gmail.mp4
- Manual Configuración 2FA - Gmail.pdf
- Video Configuración 2FA - Microsoft 365.mp4
- Manual Configuración 2FA - Microsoft 365.pdf
- Video Configuración 2FA cuentas compartidas - Gmail.mp4
- Manual Configuración 2FA cuentas compartidas - Gmail.pdf

Atentamente,

AXEL ARMANDO HERNANDEZ VARGAS (FIRMA)
PERSONA FISICA, CPF-01-0968-0694.
Fecha declarada: 29/07/2024 09:28:17 AM
Razón: Universidad Nacional
Lugar: DTIC

FRANCISCO JOSE GONZALEZ ALVARADO (FIRMA)
PERSONA FISICA, CPF-02-0451-0487.
Fecha declarada: 29/07/2024 01:49:17 PM
Razón: Presidente
Lugar: Consejo Rectoria - UNA

M.Sc. Axel Hernández Vargas
Director General

MEd. Francisco González Alvarado
Rector

AHV/YFC

Publicada en: Correo Institucional
Entra en Vigencia: A partir de su publicación.
Conservación en: Adge (expediente de disposiciones normativas)