14 de agosto de 2020

CINDE-DCI-OF-017-2020

Estimados señores
Unidad de Servicios Tecnológicos.
MICITT

Considerando lo estipulado en la **ADENDA N°2- CONTRATO N° MICITT-PINN-CON-636-2019** que señala lo siguiente: "*CINDE deberá informar mediante nota formal dirigida al Departamento de Respuesta a incidente de Seguridad Informática del MICITT, el cumplimiento de los requerimientos técnicos enumerados en el plazo de tres días hábiles a partir de la entrada en vigencia de la presente adenda."* Se adjunta la siguiente información:

EVALUACIÓN DE ASPECTOS DE SEGURIDAD:

1. Medidas de seguridad en la cuenta de Survey Monkey.

• Administración consolidada, mediante cuenta corporativa. Lo que garantiza la propiedad y el control de todas las encuestas y los datos.

• Se establece doble factor de autenticación. Al ingresar a la cuenta (se envía un código de seguridad al correo de la cuenta registrada)

• Las contraseñas se rigen bajo los principios de mínimo 8 caracteres números, letras en mayúscula y minúscula, y también caracteres especiales.

• Norma ISO 27001 (Seguridad de la información).

En caso requerir un mayor detalle en aspectos tales como:

- Seguridad física
- Cumplimiento
- Control de acceso

- Políticas de Seguridad
- Personal
- Personal de seguridad especializado
- Gestión de la vulnerabilidad y pruebas de penetración
- Codificación
- Desarrollo
- Gestión de activos
- Gestión de incidentes de seguridad de la información.

Refiérase al siguiente enlace:
https://es.surveymonkey.com/mp/legal/security/

2. Medidas de seguridad en los correos que utilizan de CINDE.

• La infraestructura de correos de CINDE se basa sobre el servicio en la nube de Microsoft 365 y Kaspersky. Por consiguiente, todas las medidas de seguridad acá descritas son propias de nuestros proveedores de servicio.

- Como primera capa de seguridad contamos con Kaspersky Security for Microsoft Office 365 el cual detecta si un mensaje de correo contiene malware, ciertos archivos adjuntos, signos de correo masivo o signos de suplantación de identidad.
- El servicio nativo de Microsoft 365 Business incluye la protección contra amenazas avanzada (ATP) de Office 365, un servicio de filtrado de correo electrónico basado en la nube que protege de spam, phish, malware, ransomware, vínculos nocivos.
- Las contraseñas se rigen bajo los principios de mínimo 8 caracteres números, letras en mayúscula y minúscula, y también caracteres especiales.
- Cambio de contraseña cada 3 meses.
- Cuentas de alto riesgo en la organización establecen la autenticación multifactor (MFA) o verificación en dos pasos mediante el uso de su contraseña y un código de comprobación. Esta medida se estará implementado al 100% de la organización durante Julio 2020.
- El cifrado de mensajes de Office 365 combina capacidades de cifrado y derechos de acceso para garantizar que solo los destinatarios previstos puedan ver el contenido del mensaje.

Para un mayor detalle, refiérase al siguiente enlace: https://support.microsoft.com/es-es/office/informaci%C3%B3n-general-sobre-la-seguridad-de-microsoft-365-para-empresas-3274b159-a825-46d7-9421-7d6e209389d1#ID0EAABAAA=Setup

3. Medidas de seguridad en Dropbox.

• Administración consolidada, mediante cuenta corporativa. Lo que garantiza la propiedad y el control de los datos.

• Seguimiento de los datos que se comparten con miembros de la organización y personas externas mediante registros de auditoría exhaustivos.

• Las contraseñas se rigen bajo los principios de mínimo 8 caracteres números, letras en mayúscula y minúscula, y también caracteres especiales.

• Cambio de contraseña cada 3 meses.

• Borrado de contenido permanente, únicamente por el administrador del sistema.

• Borrado remoto, cuando los empleados abandonan el equipo o extravían un dispositivo, los administradores pueden eliminar de forma remota los datos de Dropbox y las copias locales de los archivos.

• Transferencia de cuenta, después de la desactivación de un usuario los administradores pueden transferir archivos desde la cuenta de ese usuario a otro usuario del equipo.

• Estado de usuario suspendido, los administradores tienen la posibilidad de inhabilitar el acceso de un usuario a su cuenta mientras conservan sus datos y relaciones de uso compartido para mantener protegida la información de la compañía.

• Control de eventos individuales de archivos y carpetas.

- Se agregó un archivo a Dropbox
- Se creó una carpeta

- Se mostró un archivo
- Se editó un archivo
- Se descargó un archivo
- Se copió un archivo o carpeta
- Se movió un archivo o carpeta
- Se cambió el nombre de un archivo o carpeta
- Se revirtió un archivo a una versión anterior
- Se revirtieron los cambios en archivos
- Se restauró un archivo eliminado
- Se eliminó un archivo o carpeta
- Se eliminó de manera permanente un archivo o carpeta

• Recuperación y control de versiones, todos los clientes de Dropbox Business tienen la capacidad de restaurar archivos borrados y documentos, así como de recuperar versiones anteriores de archivos y documentos, lo que asegura la posibilidad de rastrear y recuperar los cambios realizados en datos importantes.

• Cifrado, para proteger los datos en tránsito entre las aplicaciones de Dropbox y nuestros servidores, Dropbox aplica el protocolo de capa de sockets seguros (SSL)/seguridad de la capa de transporte (TLS) para la transferencia de datos, lo que crea un túnel seguro protegido por el estándar de cifrado avanzado (AES) de 128 bits o superior.

• Normas ISO 27001 (Seguridad de la información), ISO 27017 (Seguridad en la nube), ISO 27018 (Privacidad en la nube y protección de los datos) y ISO 22301 (Continuidad de las operaciones).

Para un mayor detalle, refiérase al siguiente enlace:
https://www.dropbox.com/business/trust/security

4. Medidas de respaldo que realicen de la información.

• Para todos los efectos se mantiene una copia local de los datos en los equipos del grupo de trabajo.

5. Medidas de seudonimización y de cifrado de datos personales.

• SurveyMonkey: codifican sus datos en tránsito mediante protocolos criptográficos Transport Layer Security seguros. Los datos de SurveyMonkey también se codifican cuando están almacenados.

• Dropbox: aplica el protocolo de capa de sockets seguros (SSL)/seguridad de la capa de transporte (TLS) para la transferencia de datos, lo que crea un túnel seguro protegido por el estándar de cifrado avanzado (AES) de 128 bits o superior.

• Exchange Online (correo) usa TLS (Seguridad de la capa de transporte). Son protocolos criptográficos que protegen la comunicación por red con certificados de seguridad que cifran una conexión entre equipos.

6. Cualquier otra medida que estén teniendo para garantizar la confidencialidad, integridad, disponibilidad.

• Establecemos nuestra confianza en los proveedores de servicios, los cuales se rigen bajo normas ISO y los más altos estándares internacionales para mantener la confidencialidad, integridad y disponibilidad de la información.

7. La capacidad de restaurar la disponibilidad y el acceso a los datos personales si algo les ocurriera.

• Nuestra capacidad de recuperación de desastres está supeditada a los términos establecidos por nuestros proveedores de servicio. Importante resaltar Dropbox, Microsoft y SurveyMonkey cuentan con diversos centros de datos a nivel global.

8. Políticas de seguridad del manejo de información con el personal que tratará la información, por ejemplo, medidas de acceso a las cuentas de datos personales, políticas de contraseñas, actualización de contraseñas.

• Se establece cambios de contraseña cada 3 meses y doble factor de autenticación.

• Las contraseñas se rigen bajo los principios de mínimo 8 caracteres números, letras en mayúscula y minúscula, y también caracteres especiales.

• Se generan reportes de auditoria en relación con el manejo de documentos.

9. Medidas técnicas de mantenimiento y soporte de los equipos que utilizarán, por ejemplo, tienen antivirus, antimalware, actualizaciones del software de los equipos, entre otras.

• Se establece una capa super de protección de correo ante ataques de spam, phish, malware, ransomware, vínculos nocivos y virus con dos proveedores online Microsoft y Kaspersky.

• Se mantiene la última versión de Office y Windows 10 en la totalidad de los equipos de la organización.

• Cada equipo cuenta con Nod32, como Antivirus.

• Se establecen mantenimientos periódicos cada 3 meses a los equipos.

• Nuestro modelo de gestión software se da bajo el concepto Software as a service (SaaS).

Aviso

Confidencialidad de la información

por escrito de CINDE. La información en este documento es considera privilegiada y confidencial. Por lo tanto, es la posición de CINDE que está prohibido el uso, divulgación o publicación de la información contenida en este documento. La información contenida en este documento no se considera sujeta a divulgar bajo la Ley de Libertad de Información. Si usted tiene algún comentario, duda, pregunta, o bien, si requiere alguna aclaración por favor póngase en contacto con:

Nombre: Erick Castro Área:
Coordinador TIC
Teléfono: +506 2201-2809 / +506 2201-2800
E-Mail: ecastro@cinde.org

Atentamente:

Vanessa Gibson

Digitally signed by Vanessa Gibson
DN: cn=Vanessa Gibson, o=CINDE, ou=Investment Client Director, email=vgibson@cinde.org, c=CR
Date: 2020.08.14 09:48:32 -06'00'

Vanessa Gibson Forbes
Directora de Clima de Inversión
CINDE

cc. Despacho Ministerio de Ciencia, Tecnología y Telecomunicaciones.

cc. Despacho Viceministerio de Ciencia y Tecnología.

cc. PINN

cc. Archivo.