DIAN®

POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

El emprendimiento es de todos

Minhacienda

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Elaborado por
Operador Económico Autorizado

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad de la Red

Proteger la red de ataques. Defender el perimetro de la red, filtrar el acceso no autorizado y el contenido no autorizado. Monitorear y probar los controles de seguridad.

Educación y conciencia del usuario

Producir políticas de seguridad de usuario que cubran el uso aceptable y seguro de los sistemas. Incluirlo en las capacitaciones. Mantener conciencia de los riesgos ciberneticos.

Prevención de Malware

Producir políticas relevantes y establecer defensas anti-malware en toda la organización.

Controles de medios extraíbles

Producir una politica para controlar todo el acceso a los medios extraíbles. Limitar los tipos de medios extraíbles y su uso. escanear todos los medios en busca de malware antes de importarlos al sistema corporativo.

Configuración segura

Aplicar parches de seguridad y garantizar que se mantenga la configuración segura de todo los sistemas. Crear un inventario del sistema y definir una compilación de referencia para todos los dispositivos.

Configurar un Régimen de Gestión de Riesgos

Evalúar el riesgo para la informacion y los sistemas de la organización con el mismo interés que se haría para, los riesgos legales, regulatorios, financeros u operativos. Para lograr esto, incluir un régimen de gestion de riegos en toda la organización, con el apoyo de la junta y los altos directivos.

Gestión de privilegios de usuario

Establecer procesos de gestión efectivos y limitar el numero de cuentas privilegiadas. Limitar los privilegios del usuario y monitorear su actividad. Controlar el acceso a la actividad y auditar logs.

Gestión de incidentes

Establecer una respuesta a incidentes y capacidad de rescuperación ante desastres. Probar los planes de gestión de incidentes. Proporcionar formación especializada. Reportar incidents criminales a la policía.

Monitoreo

Establecer una estrategia de monitoreo y producir políticas de apoyo. Monitorear continuamente los sistemas y redes. Analizar los logs en búsqueda de actividad inusual que pueda indicar un ataque.

Trabajo en casa y móvil

Desarrollar una politica de trabajo móvil y capacitar al personal para cumplirla. Aplicar una línea base segura para todos los dispositivos. Proteger los datos en transito y en reposo.

DIAN®
POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Pedir a su personal que trabaje desde casa

Es posible que haya más personas trabajando desde casa que de costumbre, y algunas de ellas puede que no lo hayan hecho antes, por lo tanto es importante tener en cuenta varios aspectos que garanticen la seguridad de la información de la organización, que se esta manejando.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Configurar nuevas cuentas y accesos

El aumento en el uso de contraseñas se debe principalmente a la oleada de servicios en línea, incluidos los proporcionados por el gobierno y el sector público en general, y el crecimiento masivo en el uso de computadoras personales, teléfonos inteligentes y tabletas.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Interceptación
Las contraseñas pueden ser interceptadas mientras viajan por la red.

Fuerza Bruta
Busqueda automatica de billones de contraseñas hasta que se encuentra la correcta.

Key logging
Instalar un keylogger para interceptar las contraseñas cuando son ingresadas.

Busqueda Manual
Detalles tales como fechas de cumpleaños o nombres de mascotas se pueden usar para adivinar las contraseñas.

Shoulder surfing
Observar a alguien escribir su contraseña.

Robar contraseñas
Las contraseñas almacenadas sin seguridad puede ser robadas, tales como las guardadas en notas en su escritorio.

Robar hashes
Robar archivos hash que pueden romperse para mostrar la contraseña.

Filtración de Datos
Usar contraseñas filtradas de un sistema para atacar otros sistemas.

Password spraying
Probar un número pequeño de contraseñas comunmente usadas para acceder a un gran numero de cuentas.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Seguridad en Tecnología de la Información

Operador Económico Autorizado

Reduzca su dependencia de las contraseñas.

1. Solo use contraseñas donde se necesiten y sean apropiadas.
2. Considere alternativas a las contraseñas tales como SSO, tokens de serguridad y soluciones biométricas.
3. Use MFA para todas las cuentas importantes y los sistemas conectados a internet.

Implementar soluciones técnicas

1. El bloqueo de contraseñas puede defender contra ataques de fuerza bruta.
2. Para bloquear, permitir entre 5-10 intentos de ingreso antes de bloquearse.
3. Considere usar monitoreo de seguridad para defendernos contra ataques de fuerza bruta.
4. Listas negras de contraseñas previene que se usen contraseñas comunes.

Proteja todas las contraseñas

1. Asegurese que las aplicaciones web corporativas que requieran autenticación usen HTTPS.
2. Proteja cualquier sistema de administración de acceso.
3. Escoja productos y servicios que protejan las contraseñas usando estandares tales como SHA-256.
4. Proteja el acceso a las bases de datos de los usuarios.
5. Dele prioridad a las cuentas de administradores, cuentas en la nube y usuarios remotos.

Ayudar a los usuarios a crear mejores contraseñas

1. Tenga en cuenta los diferentes métodos de generación de contraseñas.
2. Use generadores de contraseñas incorporados cuando use administradores de contraseñas.
3. No use requisitos de complejidad.
4. Evite crear contraseñas que sean demasiado cortas.
5. No imponga limites artificiales en la longitud de la contraseña.

Mensajes clave para la capacitación del personal

1. Enfatizar en los riesgos de reutilizar las contraseñas en cuentas de la casa y el trabajo.
2. Ayudar a los usuarios a elegir contraseñas que sean difíciles de adivinar.
3. Ayudar a los usuarios a priorizar sus cuentas de alto valor.
4. Considere hacer que la capacitación sea aplicable a la vida personal de los usuarios.

Ayude a los usuarios a hacer frente a la sobrecarga de contraseñas

1. Permitir a los usuarios almacenar de forma segura sus contraseñas, incluyendo el uso de administradores de contraseñas.
2. No expirar automaticamente las contraseñas. Solo pídale a los usuarios que cambien sus contraseñas por indicación o por compromiso.
3. Usar herramientas de delegación en lugar de compartir contraseñas. Si existe un requisito comercial urgente para compartir contraseñas, use controles adicionales para proporcionar la supervisión requerida.

DIAN®
POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Preparando a su personal para trabajar desde casa

Software como servicio (SaaS)

- ✓ Basecamp
- ✓ Confluence
- ✓ G Suite
- ✓ Jira
- ✓ MailChimp
- ✓ Office 365
- ✓ Slack
- ✓ Smartsheet
- ✓ Stride
- ✓ Trello
- ✓ Yammer
- ✓ Zendesk

- ✓ Protección de datos en tránsito entre los clientes y el servicio.
- ✓ Configuración de certificados internos y externos de buenas prácticas de la industria.
- ✓ Autenticación y protección de API.
- ✓ Separación de privilegios.
- ✓ Autenticación multifactor.
- ✓ Registro y recopilación de eventos.
- ✓ Disponibilidad de logs.
- ✓ Respuesta clara ante incidentes a problemas de seguridad y parches.

DIAN®
POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Preparando a su personal para trabajar desde casa

Recomendaciones generales para apoyar el trabajo seguro en casa.

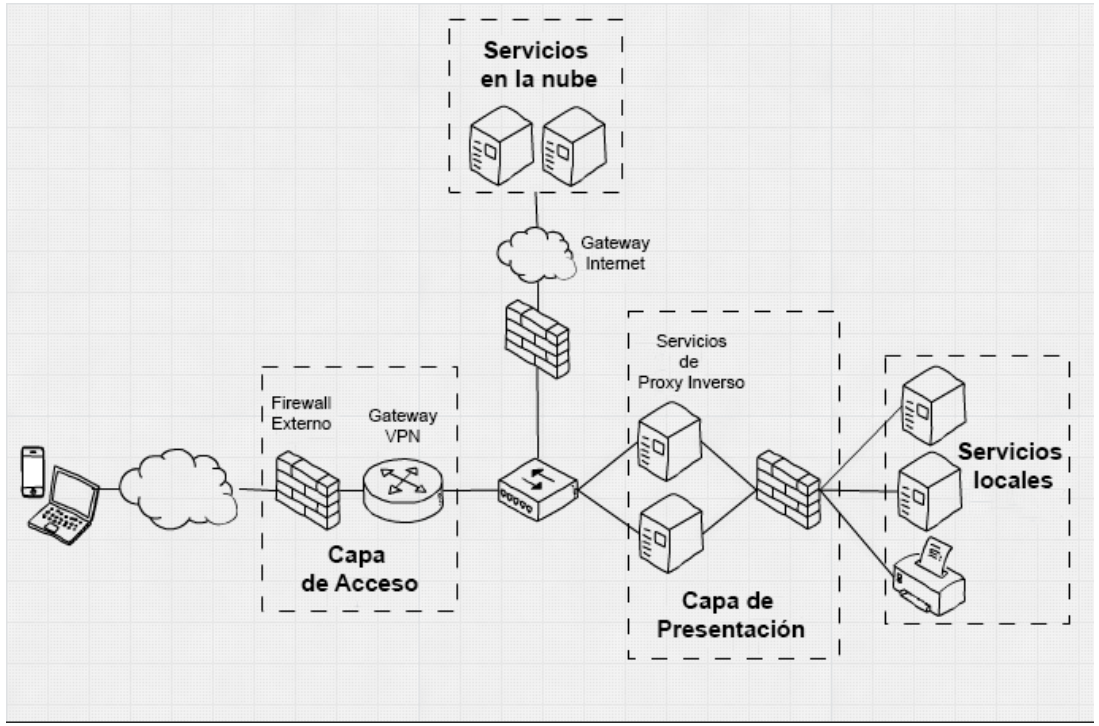
- ✓ Producir guías escritas con las características del software, que indiquen como funciona.
- ✓ Considerar producir una serie de ¿Cómo se hago?
- ✓ Verificar cómo se están adaptando el personal para tener que trabajar de diferentes maneras.
- ✓ Asegúrese de que los dispositivos cifran los datos mientras están en reposo, lo que protegerá los datos del dispositivo.
- ✓ Usar el software de administración de dispositivos móviles para configurar dispositivos con una configuración estándar.
- ✓ Asegurarse que el personal sepa cómo informar cualquier problema técnico.
- ✓ Trabajar temas de seguridad informática y boletines regulares de seguridad.

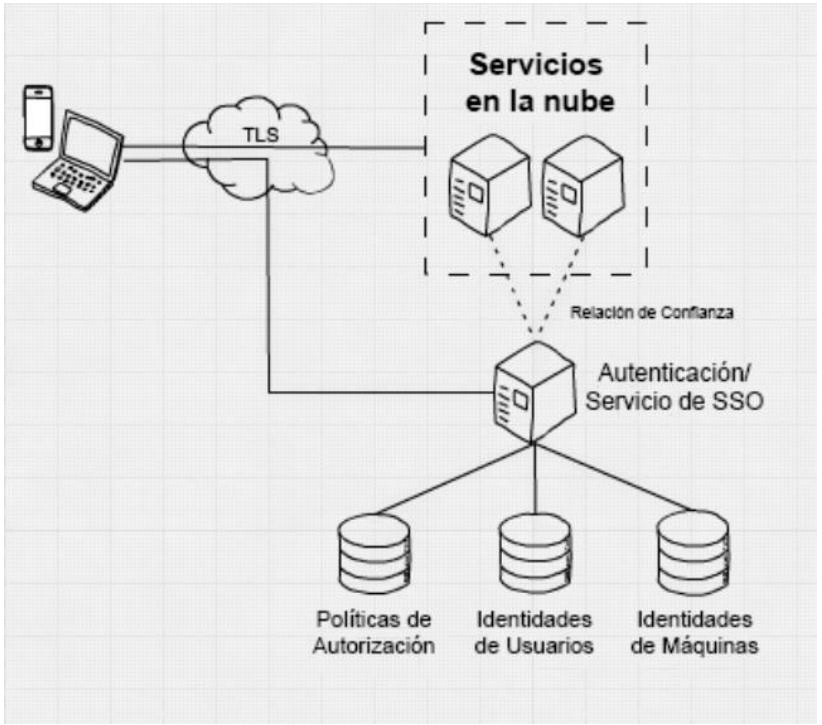
DIAN®
POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Controlar el acceso a los sistemas corporativos.





Si tiene recursos locales, el uso de una arquitectura de acceso remoto basada en **VPN** tradicional es una forma de equilibrar la facilidad de uso remota con el riesgo de compromiso.

Si tiene pocos o ningún servicio local, la arquitectura **Zero Trust** puede ser muy eficaz.

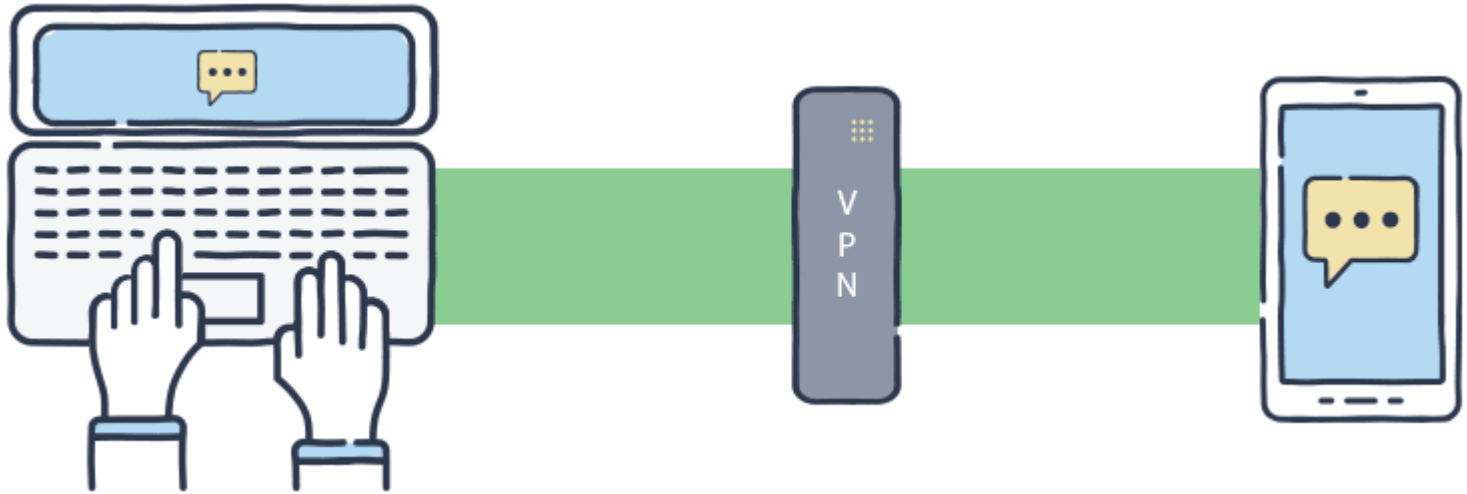
DIAN
POR UNA COLOMBIA MÁS HONESTA

Operador Económico Autorizado

Controlar el acceso a los sistemas corporativos.

Redes privadas virtuales (VPN)

Las redes privadas virtuales (VPN) permiten a las organizaciones proporcionar conectividad segura entre dispositivos en ubicaciones físicamente separadas.



Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado **Controlar el acceso a los sistemas corporativos.**

Consideraciones de Ciberseguridad en las VPN

- ✓ A medida que las organizaciones utilizan VPN para el teletrabajo, se están encontrando más vulnerabilidades y están siendo blanco de actores cibernéticos malintencionados.
- ✓ Como las VPN son 24/7, las organizaciones son menos propensas a mantenerlas actualizadas con las últimas actualizaciones y parches de seguridad.
- ✓ Los actores cibernéticos malintencionados pueden aumentar los correos electrónicos de phishing dirigidos a los teletrabajadores para robar sus nombres de usuario y contraseñas.
- ✓ Las organizaciones que no utilizan la autenticación multifactor (MFA) para el acceso remoto son más susceptibles a los ataques de phishing.
- ✓ Las organizaciones pueden tener un número limitado de conexiones VPN, después de lo cual ningún otro empleado puede teletrabajar. Con la menor disponibilidad, las operaciones empresariales críticas pueden verse afectadas, incluida la capacidad del personal de seguridad de TI para realizar tareas de ciberseguridad.

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Controlar el acceso a los sistemas corporativos.

Mitigaciones

- ✓ Actualizar las VPN, los dispositivos de infraestructura de red y los dispositivos que se utilizan para conectarse de forma remota a entornos de trabajo con las últimas revisiones de software y configuraciones de seguridad.
- ✓ Alertar a los empleados sobre un aumento esperado en los intentos de phishing.
- ✓ Asegurarse de que el personal de seguridad de TI esté preparado para aumentar las siguientes tareas de ciberseguridad de acceso remoto: revisión de logs, detección de ataques y respuesta y recuperación de incidentes.
- ✓ Implemente MFA en todas las conexiones VPN para aumentar la seguridad. Si MFA no se implementa, requiere que los trabajadores de teletrabajadores usen contraseñas seguras.
- ✓ Asegúrese de que el personal de seguridad de TI pruebe las limitaciones de VPN para prepararse para el uso masivo y, si es posible, implemente modificaciones, como la limitación de velocidad, para dar prioridad a los usuarios que requerirán anchos de banda más altos.
- ✓ Informar de incidentes, phishing, malware y otros problemas de ciberseguridad a las autoridades pertinentes.

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Ayudar al personal a cuidar los dispositivos.

Pérdida, daños o robo

Ya sea que usen su propio dispositivo o el de la organización, aliente al personal a bloquear sus pantallas si no lo atienden, especialmente si hay niños o compañeros de casa presentes. Cuando no se usa el dispositivo, el personal debe mantenerlo en un lugar seguro.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Operador Económico Autorizado

Medio Extraíbles.

- ✓ Deshabilitar los medios extraíbles mediante la configuración de los dispositivos.
- ✓ Utilizar herramientas antivirus cuando sea apropiado.
- ✓ Sólo permitir el uso de productos suministrados por la organización
- ✓ proteger los datos en reposo (cifrar) en medios extraíbles.

DIAN
POR UNA COLOMBIA MÁS HONESTA

Ciberseguridad OEA durante el estado de emergencia económica, social y ecológica

Elaborado por
Operador Económico Autorizado

GRACIAS

El emprendimiento es de todos | Minhacienda

DIAN
POR UNA COLOMBIA MÁS HONESTA