UNIVERSIDAD NACIONAL
RAÚL SCALABRINI ORTIZ
SAN ISIDRO

Tecnicatura en Ciberseguridad

FUNDAMENTOS DE CIBERSEGURIDAD Y PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Actividad Grupal N° 1

Integrantes: Bressán Esteban
Bustos Mauro R.
Carini Alfredo
Carmona Krechov Facundo
Castro Mónica

COMISIÓN 2

Profesor: Eduardo Winkler

Fecha Entrega: 11/9/2022

Consigna:

Considerando que Ud. es el Responsable de Seguridad Informática de la Entidad Alfa, diseñe una Política de Seguridad para el control de acceso remoto de proveedores.

Recuerde qué generalmente una política incluye:

1- Objetivos
2- Alcance
3- Documentos relacionados
4- Definiciones y abreviaturas
5- Versionado y control de cambios
    -Sobre el acceso remoto y proveedores

6- Asignación (criterios)
    -Nomenclatura
7- Tiempo de vida
8- Acceso a recursos
9- Perfiles
10- Responsables
11- Auditoría

Documento: Politica de VPN		Código: PSAVpn_007
Generado por: Responsable Del Área de Informática	Versión: 3.0	Calificación interna: 100
Revisado por: Comité de Seguridad Informática		
Aprobado por: Directorio	Próxima Revisión: 11/9/2023	

SOBRE LA POLÍTICA DE SEGURIDAD

1. Objetivo de la Política

El objetivo de esta política de seguridad es mantener un control de acceso, sobre los activos críticos de información de la organización y que el servicio externo solo tenga acceso a aquellos datos que les son de necesidad y de mantener la confidencialidad de aquella información que no le es relevante para cumplir con sus tareas.

Para que la misma cumpla correctamente su función, el servicio externo sólo debe poder hacer uso de la información que la organización considere necesaria para que estos puedan cumplir con su función y que, toda la información permanezca íntegra, confiable y disponible, cada acceso interno o externo debe ser registrado.

Esta protección debe contemplarse antes, durante y a la finalización del servicio contratado.

2. Alcance:

Esta política alcanza a todos los proveedores que hayan sido contratados por ALFA y terceras partes vinculadas, y a acuerdos de confidencialidad establecidos entre las partes que necesiten acceder de manera remota a servicios, equipos, información o cualquier otro activo digital propiedad de ALFA o sus clientes para brindar servicios relacionados al almacenamiento, infraestructura, plataforma o software que sean entregados a ALFA en modalidad de servicio y / o provisión de productos.

3. Documentos Relacionados

ISO/IEC – 27001: Sistema de Gestión de Seguridad de la Información publicado por La Organización Internacional de Normalización (ISO) y en especial su dominio “A.9 Control de Accesos”, “A.15.Relación con los proveedores”.

ISO/IEC – 27032: estándar de Ciberseguridad publicado por La Organización Internacional de Normalización (ISO). Ofrece orientación para fortalecer el estado de la ciberseguridad en la organización, utilizando los puntos técnicos y estratégicos más importantes para esa actividad.

ISO/IEC – 27036: Seguridad de la información en las relaciones con los proveedores – Parte 1: Visión general y conceptos; Parte 2: Requisitos; Parte 3: Directrices para la seguridad en la cadena de suministro de las tecnologías de la información y la comunicación

Ley 25326 De Protección de Datos Personales

Acuerdos de Confidencialidad entre las partes.

4. Definiciones y abreviaturas

VLAN: Área de red Local Virtual

VPN: Red privada virtual

LAN: Red de área local

Intranet: Servicio corporativo Interno.

VCS: Sistema de Control de Versiones

Token: Código de seguridad cifrado para acceso remoto.

5. Versionado y control de cambios

Se debe implementar una política que registre históricamente las versiones y cambios realizados en los repositorios a los que se accede de forma remota.

Asimismo se debe implementar un registro de versión y control de cambios sobre la presente política de seguridad.

SOBRE LOS ACCESOS REMOTO Y PROVEEDORES

6. Asignación (criterios)

Los proveedores deberán acceder de forma remota a los activos de información a través de herramientas tales como VPN y/o cualquier otro que ALFA defina cuando fuere necesario para el cumplimiento de las obligaciones. En caso contrario, se deberá solicitar una autorización especial al propietario de la información, quien analizará los motivos del requerimiento y definirá si se otorga o deniega la solicitud.

Los proveedores deberán definir e informar de manera fehaciente a ALFA quienes serán las personas responsables de la información de las terceras partes que podrían acceder.

7. Tiempo de vida

El acceso remoto a los activos de información, los repositorios, cualquier recurso o servicio previamente definido, estará limitado a por un período de tiempo por cada conexión remota definida por Alfa en función de los requerimientos presentados por el proveedor. Asimismo, las credenciales de acceso que serán definidas por Alfa contarán con una caducidad en cuanto al tiempo de validez de dichas credenciales.

8. Acceso a recursos

Las políticas de acceso a los recursos por parte de terceros serán definidos por Alfa en función de los requerimientos y actividades a desarrollar con la información o repositorios siguiendo el concepto de mínimo privilegio pudiendo escalarlos en caso de ser necesario con previa autorización.

En todos los casos los accesos remotos, previamente autorizados deberán realizarse mediante combinación de usuario y contraseña con la robustez suficiente y autenticación de doble factor, quedando a criterio de Alfa la metodología de implementación del mismo.

9. Perfiles

Se definirán los perfiles de acceso a la información o recursos, en función de los siguientes privilegios, sólo lectura, consulta, modificación y control total estructurado de acuerdo a lo establecido en la política de acceso a recursos, y de acuerdo a los roles y funciones que cada agente externo deba desempeñar.

Bajo ninguna circunstancia se brindará acceso a otros activos que por su naturaleza y/o función Alfa considere que excedan la incumbencia de agentes externos.

10. Responsables

Alfa designará un comité de Seguridad que será el responsable de impulsar, implementar y gestionar la presente política de seguridad.

Dicho comité tendrá como función principal corroborar el cumplimiento, mantenimiento y modificaciones que correspondan a la presente política de acuerdo al tiempo de revisión designado, o a cualquier incidencia previa que lo amerite.

El comité también deberá difundir dichas políticas dentro de todas las áreas de la organización y velar por el compromiso del cumplimiento de las mismas.

11. Auditoría

Alfa deberá asegurar que los proveedores prestadores de servicios cumplan con estándares del negocio en materia de seguridad, Alfa se reserva el derecho de solicitar evidencia de la ejecución de auditorías independientes relacionadas al riesgo tecnológico, control interno, o auditorías de certificación relacionados con dicha materia, los cuales deben ser facilitados de manera confidencial y con el objeto de revisar el alcance del trabajo realizado y el detalle de los resultados obtenidos.